Chambers

GLOBAL PRACTICE GUIDES

Definitive global law guides offering
comparative analysis from top-ranked lawyers

Trade Secrets

Contributing Editors
Claudia Ray and Joseph Loy
Kirkland & Ellis LLP

practiceguides.chambers.com

2021

Chambers

Global Practice Guides

Trade Secrets

Contributing Editors

Claudia Ray and Joseph Loy

Kirkland & Ellis LLP

2021

Chambers Global Practice Guides

For more than 20 years, Chambers Global Guides have ranked lawyers and law firms across the world. Chambers now offer clients a new series of Global Practice Guides, which contain practical guidance on doing legal business in key jurisdictions. We use our knowledge of the world's best lawyers to select leading law firms in each jurisdiction to write the 'Law & Practice' sections. In addition, the 'Trends & Developments' sections analyse trends and developments in local legal markets.

GPG Director Katie Burrington
Product Manager Emily Kyriacou
Managing Editor Claire Oxborrow
Deputy Editor Philip Myers
Copy Editors Shelagh Onn, Kevan Johnson, Sally McGonigal, Ethne Withers, Jonathan Mendelowitz, Nancy Laidler
Editorial Assistants Daniella Lowe, Carla Cagnina, Rose Walker
Production Manager Jasper John
Production Coordinator Genevieve Sibayan

Published by
Chambers and Partners
No.3 Waterhouse Square
138 Holborn, London
EC1N 2SW
Tel +44 20 7606 8844
Fax +44 20 7831 5662
Web www.chambers.com

CONTENTS

INTRODUCTION

Contributed by: *Claudia Ray and Joseph Loy,* ***Kirkland & Ellis LLP***

Trade Secrets: Trends and Developments

As businesses around the world evaluate their options for protecting valuable intellectual property in today's context of a dynamic technological environment and a highly mobile labour force, trade secret protection can be an essential complement to patent, copyright and trade mark protections. This is particularly true in the United States in light of recent developments in the patent system – including shifting judicial standards for patent-eligible subject matter and the increased availability of post-grant challenges at the Patent Office – that have increased the importance of trade secret protection as an alternative vehicle for protecting intellectual property. Moreover, as the developed world continues its shift from a manufacturing economy to a knowledge-based economy, where the most rapidly growing sectors offer software and services, trade secret laws are more relevant than ever.

This edition focuses on best practices for protecting trade secrets and avoiding the pitfalls of encroaching on others' trade secret rights. A key area to which trade secret owners must remain alert is the use of technological and other protections to protect their valuable intellectual property. Recent decades have seen a sea change in the way employers recruit and maintain their workforce, including hiring a substantial number of remote employees, increased use of independent contractors, and the rise of the "gig" economy in which an ever-rotating cast of independent workers may have access to the company's confidential information.

On top of these existing trends, the global COVID-19 pandemic forced many sectors to rapidly shift from traditional workplace practices to ad hoc work-from-home policies. Whether this unexpected crisis ultimately sparks a push to fully remote work remains to be seen, but it is clear that successfully navigating the modern workplace will require balancing agility and innovation with appropriate confidentiality controls. The increased focus on remote work, born out of necessity but likely to remain to some degree, underscores the need to create sophisticated confidentiality measures to protect trade secrets without impairing the ready interchange of ideas and information and collaborative work environments that may be necessary to promote the very innovation that generates trade secrets. The days when a company could simply lock its crown jewels in a vault and rest easy knowing its trade secrets were safe has passed.

At the same time, as an increasingly mobile workforce chooses to pursue new opportunities and leverage experiences from prior companies, the risk of misappropriation grows. Employees may feel incentivised to use knowledge and insight gained at prior employers to differentiate themselves in a new job, and without adequate training and precautions the line between acquired skills and acquired confidential information could become blurred. New employers (whether leanly staffed start-ups or global heavyweights) should implement stringent procedures for insulating themselves from others' confidential information. And former employers must remain vigilant in safeguarding the improper use of their hard-earned property or risk losing it to competitors.

Because disputes over trade secrets arise even when such precautions are taken, we explore the latest trends in trade secret litigation and alternative dispute resolution (ADR) proceedings. Given the high stakes for both sides in a trade secret dispute, it will be important for

INTRODUCTION

Contributed by: *Claudia Ray and Joseph Loy,* ***Kirkland & Ellis LLP***

counsel to consider the full spectrum of offensive and defensive resources that may be available under statutory and common law misappropriation laws and advise clients accordingly – whether that entails implementing procedures for effectively maintaining the confidentiality of trade secrets or minimising the risk of coming into the possession of or using a competitor's trade secrets.

Increasing Prevalence of DTSA Lawsuits

In the United States, just as the Uniform Trade Secret Act displaced nearly all state-specific common law misappropriation schemes, providing a theoretically uniform body of law across the many states, Congress enacted the Defend Trade Secrets Act (DTSA) in 2016, building on earlier federal economic espionage statutes, to create a federal system of trade secret law. Now that the first wave of DTSA cases has made its way through the federal courts, we are beginning to see greater uniformity and certainty on key issues. As explored in this practice guide, a robust body of case law is developing on such topics as pleading requirements, the required particularity for descriptions of trade secrets in discovery, liability based on conduct predating the enactment of the DTSA, and allowable measures of damages. The enactment of the DTSA, not surprisingly, has resulted in a significant uptick of federal filings, as trade secret owners seek to benefit from the perceived uniformity and predictability of the federal courts. Moving forward, counsel should keep up to date with the latest developments in DTSA litigation, which is proving to be an indispensable part of every trade secret owner's toolkit.

International Considerations

Protecting trade secrets internationally continues to be dynamic and unpredictable. Courts in the United States are just beginning to grapple with issues of liability and damages based on conduct occurring overseas. And many foreign jurisdictions are themselves still developing their trade secret jurisprudence. Global businesses must navigate the laws of each country and territory on a case-by-case basis and make informed decisions about how to safeguard trade secrets locally as well as centrally, to ensure that they do not inadvertently lose global protection for failure to comply with a single foreign law.

Trade secret owners conducting business in the United States should also not forget that the United States International Trade Commission (ITC) can conduct investigations and recommend prohibitions against importing articles based on the theft of trade secrets. Although there had been a long lull in such investigations, there has been a surge in investigations and enforcement actions at the ITC in recent years. As a result, companies doing business globally should stay apprised of the latest developments in litigation involving international parties, whether in the federal court system, at the ITC or globally. That part, we assure you, is not a secret.

INTRODUCTION

Contributed by: *Claudia Ray and Joseph Loy,* ***Kirkland & Ellis LLP***

Kirkland & Ellis LLP is an international law firm with 2,700 attorneys across the United States, Europe and Asia. Kirkland's trade secrets litigation practice includes approximately 75 attorneys with years of experience in representing both plaintiffs and defendants in trade secrets matters in diverse industries. Kirkland's trade secrets attorneys have litigated the broad spectrum of trade secret disputes, ranging from outright theft to violation of various agreements, including employment, R&D, joint development, and technology transfer and know-how agreements. Significant victories have been won for clients in these matters in UK courts, US federal and state courts, and in arbitrations, and the firm has worked collaboratively with law enforcement agencies to protect clients' intellectual property. The practice's success is grounded in extensive jury and bench trial experience, and it has a sophisticated appellate practice to protect clients' successes at the trial level.

CONTRIBUTING EDITORS

Claudia Ray is a partner in Kirkland's intellectual property practice group. She represents clients in litigation, arbitration and administrative proceedings involving trade secret, copyright, trade mark, internet and contact/licensing issues across a wide range of industries. Her trade secret practice includes litigation and counselling relating to software, technology, financial services and consumer products. Claudia also serves on the Intellectual Property and Technology Advisory Committee of the American Arbitration Association and the US Amicus Subcommittee of the International Trademark Association, and is the chair of the Copyright Law Committee of the Association of the Bar of the City of New York.

Joseph Loy is a partner in Kirkland's intellectual property practice group. His practice focuses on trade secret and patent infringement disputes before federal trial and appellate courts nationwide. His trade secret work includes both offensive and defensive litigation and corporate counselling. Joe has represented clients in cases involving a wide range of industries, including medical devices, pharmaceuticals, biotechnology, wireless telecommunications, petrochemicals, cruise ships, digital photography, smartphones and computer software. He is a frequent commentator on trade secret issues before intellectual property Bar associations and law school communities.

Kirkland & Ellis LLP

601 Lexington Avenue
New York
NY 10022

Tel: 212 446 4800
Fax: 212 446 4900
Email: claudia.ray@kirkland.com
Web: www.kirkland.com

KIRKLAND & ELLIS

CHINA

Law and Practice

Contributed by:
Yi Xue
Zhong Lun Law Firm see p.29

CONTENTS

1. LEGAL FRAMEWORK

1.1 Sources of Legal Protection for Trade Secrets

China does not have a unified trade secret law, but the rules governing civil, administrative and criminal enforcement routes are scattered among a series of laws and regulations. The Anti-Unfair Competition Law (2019 revised, AUCL) is the principal law regarding trade secrets, which defines and regulates what is a trade secret, the misappropriation of trade secrets and the corresponding legal liabilities, etc. Although China follows the civil law system, judicial interpretations issued by the Supreme People's Court are binding on the courts. The Judicial Interpretation on Unfair Competition (2020 revised) and the Judicial Interpretation on Trade Secrets (2020) play significant roles in the judicial practice of trade secret protection.

Other civil laws relevant to trade secrets protection include the Civil Code, the Company Law, the Labour Law and the Labour Contract Law. The Civil Code, in the Part III Contracts, provides the general obligation of trade secret protection in contract negotiations and the rules related to technology licence contracts that may involve technical secrets. The Company Law provides the trade secret protection obligations for senior management, prohibiting directors or managers of a company from illegally disclosing the company's trade secrets. The Labour Law and Labour Contract Law regulate the employees' obligation to protect the trade secrets of their employers under labour contract and non-compete agreements.

Trade secrets can also be protected through administrative enforcement. The State Administration of Industry and Commerce's Provisions Regarding the Prohibition of Trade Secret Infringement provides administrative procedures for handling trade secrets cases. Now this authority of the State Administration of Industry and Commerce is succeeded by the State Administration for Market Regulation (SAMR).

The Criminal Law (2020 revised) and the Judicial Interpretation (III) Concerning the Application of Law in the Handling of Criminal Cases for the Infringement upon Intellectual Property Rights regulate the acts that seriously infringe upon trade secrets as the crime of infringing upon trade secrets.

1.2 What Is Protectable as a Trade Secret

The AUCL defines a trade secret as technical, operational or other commercial information unknown to the public that is of commercial value and for which the owner has taken corresponding confidentiality measures.

Technical information generally refers to technical solutions obtained by way of scientific and technological knowledge, information and experience, while business information generally refers to various types of business information that can bring competitive advantage to rightholders other than technical information.

1.3 Examples of Trade Secrets

The Judicial Interpretation on Trade Secret has addressed the typical categories of information qualified as trade secrets, covering a wide spectrum of business and technical information, giving concrete examples to illustrate the types of information that courts have found are protectable under the AUCL.

Technical information that can be protected as trade secrets mainly includes structure, raw materials, components, formulas, materials, samples, patterns, propagating materials of new plant varieties, techniques, method or its steps, algorithms, data and computer programs. Business information subject to trade secret protec-

tion mainly includes original ideas, management, sales, finance affairs, plans, samples, bidding materials, customer information and data.

1.4 Elements of Trade Secret Protection

Under the AUCL, information is entitled to trade secret protection if three elements are met:

- the relevant information should be confidential, which means that it should be unknown to, and be difficult to be obtained by, the relevant personnel in the relevant field;
- the relevant information should have actual or potential commercial value and can bring competitive advantage for the owner; and
- the relevant information shall be protected by the owner by adopting proper secret-protection measures suitable for the commercial value or other specific situation.

1.5 Reasonable Measures

The owner of a trade secret is required to show that it took reasonable measures to protect the trade secret. According to the Judicial Interpretation on Trade Secret, when determining whether the owner has adopted reasonable confidentiality measures, the courts usually consider the following factors:

- the features of the trade secret and its carrier;
- the commercial value of the trade secret;
- the identifiability degree of the confidentiality measures;
- the degree of correspondence between confidentiality measures and the trade secret; and
- the intention of the owner to keep it confidential and other factors.

Under any of the following circumstances, where it is sufficient to prevent disclosure of a trade secret under normal conditions, the owner will be found to have adopted reasonable confidentiality measures in:

- signing a confidentiality agreement or stipulating the obligation of confidentiality in a contract;
- putting forward the confidentiality requirements to employees, former employees, suppliers, clients and visitors, etc, who may have access to, or obtain, the trade secret in such ways as articles of association, training, rules and systems, and written notification;
- limiting visitors to, or conducting differentiated management on, the classified factory buildings, workshops or other production places;
- differentiating and managing the trade secret and its carriers by such means as marking, classification, isolation, encryption, sealing up for safekeeping and limiting the scope of persons who may have access to, or obtain, such secret;
- taking measures such as prohibiting or restricting the use of, visiting, storing or reproducing computer equipment, electronic equipment, network equipment, storage equipment and software, etc, that can be used to access or obtain the trade secret;
- requiring resigned employees to register, return, clear away or destroy the trade secret they have accessed or obtained as well as the carriers thereof, and to continue to assume the obligation of confidentiality; or
- taking other reasonable confidentiality measures.

It should be noted that the following circumstances may not be deemed as proper confidentiality measures for trade secrets in judicial practice:

- collateral obligation of secret protection in a contract does not reflect the subjective desire and objective measures of the owner of trade secrets to take confidentiality measures and thus the existence of collateral obligation

alone is not enough to establish reasonable measures;
- only imposing competition restrictions on employees in labour contracts or confidentiality agreements without specifying the scope of trade secrets does not qualify as reasonable measures; and
- labour contracts or the internal rules unilaterally issued by the company fail to clearly define the specific contents and the scope of trade secrets.

1.6 Disclosure to Employees

As one of the three constituent elements for a trade secret, the nature of confidentiality requires that trade secrets must be unknown to the public. However, "unknown to the public", with the characteristic of relativity, only requires trade secrets not to be generally known to, or easily available to, the relevant personnel in the relevant technology or business field rather than anyone other than the owner. In other words, the right-holder disclosing a trade secret to those who need to know it will not affect the secrecy of such trade secret if confidentiality measures have been taken. Therefore, if necessary, the right-holder may disclose a trade secret to its employees, which will not affect the availability of the legal protection for the trade secret. But the right-holder should also take strict confidentiality measures upon such disclosure.

1.7 Independent Discovery

According to Article 14 of the Judicial Interpretation on Trade Secret, the trade secrets obtained through independent research and development or reverse engineering shall not be affirmed as a misappropriation of trade secrets stipulated in the AUCL. However, if any party has obtained the trade secret of someone else by unjustifiable means and then claims no infringement upon the trade secret on the ground of reverse engineering, it shall not be supported.

1.8 Computer Software and Technology

Apart from claiming for protection under the Copyright Law or the provisions under a licence agreement, computer software owners may also protect their information under the AUCL. The courts have held that computer programs and related documents can constitute protectable trade secrets if certain requirements are met. As with other types of information, when determining the availability of the trade secret protection, the focus will be the three constitutive elements of "unknown to the public", "being of commercial value" and "confidentiality measures having been taken", and there are no laws or regulations regarding trade secret protection unique to computer software.

Although the protection provided by trade secrets laws and regulations goes beyond the scope of copyright protection, which only protects the expression of computer programs and related documents of a software, it is not enough to demonstrate that trade secrets exist by referring to a broad scope of software technology. The trade secret owner should identify the specific lines of computer source code or the concrete software features of the software sought for protection.

1.9 Duration of Protection for Trade Secrets

The current laws and regulations in China have no limit on the duration of protection for trade secrets. In principle, as long as the relevant information remains to meet the three constituent elements of a trade secret, the owner is entitled to protection for trade secrets. If a trade secret is publicly disclosed, whether it is disclosed by the owner intentionally or accidentally, the requirement of "unknown to the public" will no longer be met so that it cannot be protected legally as a trade secret. Although disclosure to the persons on a need-to-know basis will not affect the existence of a trade secret, proper secrecy-keeping

measures such as concluding a non-disclosure agreement (NDA) with the persons having access to the trade secret should be adopted.

1.10 Licensing

As with other intangible properties, a trade secret can be licensed to any third party, whereby the right-holder can convert it into real benefits. In practice, both technological secrets and business secrets can be licensed by concluding relevant contracts. The Civil Code, in Chapter XX, specifically addressed certain rules on technology contracts as they are the most common form of trade secret licence.

In general, the trade secret owner is entitled to a licensing fee or royalty from the licensee for exploiting the trade secrets licensed. The trade secret owner may flexibly agree on specific licensing terms and conditions by concluding a licence contract with the licensee. In practice, there are three types of trade secret licence:

- sole licence, under which the owner licenses a trade secret to only one licensee for using, and the owner is also prohibited from using such trade secret;
- exclusive licence, under which the owner licenses a trade secret to only one licensee for using, but the owner is allowed to use such trade secret; and
- non-exclusive licence, under which the owner is entitled to license a trade secret to more than one party, and the owner is also allowed to use such trade secret.

When entering into a contract for the licence for the using of trade secrets, the owner should prudently agree on the key terms of such licence, such as the using scope, duration, geographical scope, method, licence fee, the licensee's confidentiality obligations and liabilities for breach of the licence contract. For a technology licence, it is also advisable to specify in advance the issues, such as whether the licensee is allowed to reverse engineer, and who will own trade secrets generated from additional research and development undertaken by either party after the licence has been granted. During the performance of the licence contract, the owner should also closely monitor the use of the trade secret by the licensee. Once the owner learns any violations, the owner should immediately take actions.

1.11 What Differentiates Trade Secrets from Other IP Rights

Compared with other intellectual property rights, the protection of trade secrets has its own particularities, with the following characteristics:

- trade secrets can be protected indefinitely – patents, trade marks and copyrights are protected by law only within a certain period and conditions; while the legal protection for trade secrets can be indefinite as long as such trade secrets meet the three constituent elements of trade secrets;
- protection for trade secrets is relative – trade secrets are generated by "taking certain confidentiality measures", which determines that trade secret right is relative to specific subjects within the scope of confidentiality and cannot be used against those who obtain such trade secrets by proper ways, such as independent development or reverse engineering;
- the target object of trade secret protection is different – laws and regulations related to trade secrets aim to protect non-public information, which requires that the target object must be unknown to the public; while the target objects of other intellectual property rights are public;
- trade secret rights are obtained in different ways – subject to administrative review and approval, both patent right and trade mark right are the rights granted by rel-

evant administrative authorities; copyright is obtained automatically by the owner from the time when the work is completed, while trade secret right, as long as it meets the three elements as a trade secret, will be obtained by the right-holder through lawful labour or other legitimate means; and
- the cost of protecting trade secrets is different – since administrative review and approval are not required, there is no need to pay the fees for approval, authorisation, registration or maintenance to relevant administrative authorities for the protection of trade secrets.

1.12 Overlapping IP Rights

The protection of trade secrets may, in some cases, overlap with the protection of other intellectual property rights, especially the copyright. For instance, an internal Equipment Maintenance Manual of an equipment manufacturer on the one hand can be protected as a work under the Copyright Law if it meets the originality standard. On the other hand, the technology information included in the Equipment Maintenance Manual can also constitute trade secrets if such information satisfies the three constitutive elements of a trade secret. In judicial practice, the plaintiff may claim both secret protection and copyright protection in the same case and the court may hold in favour of both claims depending on the specific situation of the case.

1.13 Other Legal Theories

In addition to the infringement lawsuits based on the legal theory of misappropriation according to the AUCL, it is also possible to sue the counterparty for breach of confidentiality obligations based on the contractual stipulations. For instance, the trade secret owner may bring a civil lawsuit for breach of confidentiality obligations under a licence agreement, joint venture agreement or service agreement against the counterparty to such agreements.

In addition to the infringement lawsuits based on the legal theory of misappropriation according to the AUCL, it is also possible to sue the counterparty for breach of confidentiality obligations based on the contractual stipulations. Even though there is no clear contractual stipulation, according to the Judicial Interpretation on Trade Secret, the confidentiality obligation of the alleged infringer may also be derived from the collateral obligation based on the principle of good faith. Especially for the case where an employee is sued for infringement upon trade secrets, in judicial practice, some courts state that once a labour agreement has been reached, the employee will bear the collateral obligation of loyalty to the employer, the content of which may include keeping trade secrets for the employer. Therefore, when an employee who did not sign any confidentiality agreement with the employer commits an infringement upon the trade secrets learned from work, the employer may also claim for his breach of collateral obligation to keep trade secrets based on the labour contract.

With regard to the tortious interference with contractual confidentiality obligation, the AUCL identifies tempting a person in acquiring, disclosing, using, using or allowing any other person to use the trade secret of the right-holder in violation of his or her confidentiality obligation as one of the misappropriations upon trade secrets. Therefore, the right-holder may bring a claim for infringement upon trade secrets against a defendant where it has induced an employee to breach a contractual confidentiality obligation to the owner/employer.

1.14 Criminal Liability

The Criminal Law, in Article 219, regulates the acts that seriously infringe upon trade secrets as the crime of infringing upon trade secrets. According to this article, whoever commits any of the following conducts to infringe upon a trade secret shall, if the circumstances are seri-

ous, be sentenced to fixed-term imprisonment of not more than three years and a fine or be sentenced to a fine only; or if the circumstances are especially serious, be sentenced to fixed-term imprisonment of not less than three years nor more than ten years and shall also be fined:

- obtaining a right-holder's trade secret by theft, bribery, fraud, coercion, electronic intrusion, or any other illicit means;
- disclosing, using, or allowing any other person to use a trade secret obtained from a right-holder by any means as specified in the preceding subparagraph;
- disclosing, using, or allowing any other person to use a trade secret in its possession, in violation of its confidentiality obligation or the requirements of the right-holder for keeping the trade secret confidential;
- whoever knows any conduct set forth in the preceding paragraph but still obtains, discloses, uses, or allows any other person to use the trade secret shall be punished for the crime of infringing upon trade secrets.

In addition to the above provisions, the Criminal Law also provides that whoever steals, pries into, buys, or illegally provides any trade secret for any overseas institution, organisation or individual shall be sentenced to fixed-term imprisonment of not more than five years and a fine or be sentenced to a fine only; or if the circumstances are serious, be sentenced to fixed-term imprisonment of not less than five years and a fine.

When serious infringement upon trade secrets occurs, the right-holder may pursue both civil and criminal claims against the alleged infringer and the infringer may bear both the civil tort damages liability and the criminal liability. The civil proceeding and the criminal proceeding are independent of each other; however, it should be noted that, in general terms, the principle of "criminal priority" can be applicable to the cases regarding both criminal and civil liability, which means that the criminal case will be handled first and the civil proceedings will proceed after the criminal proceedings conclude.

1.15 Extraterritoriality

No information is available in this jurisdiction.

2. MISAPPROPRIATION OF TRADE SECRETS

2.1 The Definition of Misappropriation

Article 9 of the AUCL defines misappropriation as follows:

- acquiring a trade secret from the right-holder by theft, bribery, fraud, coercion, electronic intrusion, or any other illicit means;
- disclosing, using, or allowing another person to use a trade secret acquired from the right-holder by any means as specified in the preceding subparagraph;
- disclosing, using, or allowing another person to use a trade secret in its possession, in violation of its confidentiality obligation or the requirements of the right-holder for keeping the trade secret confidential; and
- abetting a person, or tempting or aiding a person into or in acquiring, disclosing, using or allowing another person to use the trade secret of the right-holder in violation of his or her non-disclosure obligation or the requirements of the right-holder for keeping the trade secret confidential.

Where a third party knows or should have known that an employee or a former employee of the right-holder of a trade secret or any other entity or individual has committed an illegal act as specified above but still acquires, discloses, uses or allows another person to use the trade

secret, the third party shall be deemed to have infringed upon the trade secret.

According to the Judicial Interpretation on Unfair Competition, the requisite elements to establish a trade secret misappropriation claim include:

- the trade secret at issue satisfies the statutory requirements;
- the information held by the alleged infringer is the same or substantially the same as the owner's trade secret; and
- the alleged infringer has adopted improper means to acquire the trade secret.

However, as mentioned in the first paragraph, the 2019 revised AUCL broadens the scope of misappropriation and therefore the third requisite element above may not be limited to "adopting improper means to acquire the trade secret" but the specific conducts, such as "disclosing" and "allowing another person to use" in violation of its confidentiality obligation.

2.2 Employee Relationships

There are no laws or regulations that specifically concern infringement acts committed by employees and thus the case where the misappropriation involves an employee of the owner should apply the same constitutive elements of trade secret misappropriation as other cases.

The employee may also have a collateral obligation to keep trade secrets that he or she learned from work for the employer based on the labour contract even though the employer did not sign any confidentiality agreement or terms with the employee. In judicial practice, some courts state that once an employee establishes a labour relationship with the employer, he or she has an obligation to be loyal to the employer based on the principle of good faith. Therefore, when an employee who did not sign any confidentiality agreement or terms with the employer commits an infringement upon the trade secrets learned from work, the employer may also claim for his or her breach of collateral obligation to keep trade secrets based on the labour contract.

2.3 Joint Ventures

There are no specific provisions on the confidentiality obligations with respect to trade secrets between joint venturers in the Chinese legal system. The secret-protection obligations between the joint venturers largely depend on the terms of the joint venture agreement or separate confidentiality agreement. However, as a general rule under the Contracts Part of the Civil Code, any party to a contract is obliged to keep trade secrets for the other party based on the principle of good faith. To be specific, the parties shall not disclose or improperly use the trade secret learned in concluding a contract, no matter whether the contract is established or not.

If any party discloses or improperly uses such trade secret and thus causes loss to the other party, it shall be liable for damages. Therefore, any party to a joint venture agreement shall be liable to keep the trade secrets it learns from the other party.

2.4 Industrial Espionage

In China, there are no laws and regulations specifically regulating industrial espionage currently. However, if any industrial espionage involves trade secrets, it can be regulated by other relevant laws. For example, the "other illicit means" stipulated in Article 9 of the AUCL should include the use of industrial espionage. Therefore, if any party infringes upon trade secrets by way of espionage, the right-holder can claim infringement liabilities against the infringer according to the AUCL. Besides, the right-holder may also pursue an SAMR proceeding or bring a criminal charge if the infringement is serious.

3. PREVENTING TRADE SECRET MISAPPROPRIATION

3.1 Best Practices for Safeguarding Trade Secrets

The steps recognised as helpful to safeguard trade secrets can generally be divided into two categories.

Establish a Trade Secret Protection Policy

The first step to protect trade secrets is to have a written trade secret protection policy. An effective trade secret protection policy should include at least the following:

- identify what information should be regarded as a trade secret;
- make clear how to manage and use the confidential information; and
- clearly state the consequences of any violations – such as unauthorised, improper use, or disclosure of confidential information – including employment termination, civil legal action or even criminal prosecution.

Implement the Trade Secret Protection Policy

It is advisable to implement the general secret protection policy in the following three key areas.

Establish trade secret protection rules in employment management

- It is recommended for companies to require all key personnel who have access to trade secrets to sign confidentiality agreements in which the scope of trade secrets should be specified. In addition, the requirement that the ownership of any intellectual property including trade secrets created by the employee during his or her employment shall be automatically assigned to the company should be incorporated into the employment contract or adopted as a company policy.
- Companies should implement a system to educate employees and prevent an employee's wilful or negligent wrongdoings, including ensuring that the trade secret protection policy is reflected in the employees' handbooks or similar manuals and all employees have been fully informed of such policy, and providing regular training on confidentiality requirements.
- Companies should also pay attention to new hired employees and departing employees and take necessary measures such as conducting background due diligence when hiring new employees and holding exit interviews with employees leaving the company.

Take precautions for dealings with third parties

As with employees, when dealing with third parties such as outside vendors, independent contractors and joint venturers, it is necessary to sign confidentiality agreements in conformity with the corporate confidentiality policy.

Adopt proper security measures to protect trade secrets

The primary principle is to limit access to confidential information on a need-to-know basis. To this end, various general security measures should be implemented, including:

- safeguarding and monitoring hard and electronic copies of the information;
- marking confidential information;
- maintaining computer security; and
- restricting public access to the company's facilities.

3.2 Exit Interviews

Employers will conduct exit interviews for departing employees to ensure that all trade secret information has been registered, returned, cleared or destroyed and to remind them of their confidentiality obligations. In practice, employ-

ers will usually take the following actions in the process of an exit interview:

- provide a reminder regarding the obligations of confidentiality and non-compete (if any); and
- require the departing employees to sign a written acknowledgment certifying they have returned all documents and company property and promising that nothing is saved on a personal computer or storage devices.

For those who have access to significant trade secrets of the company, employers may further require the departing employee to provide written acknowledgment indicating that they had access to certain confidential information and specifying such information. In addition, employers will try to enquire where the employee will go (although an employee without a non-compete obligation is not obliged to disclose his or her new employer). If necessary, employers will notify the new employer of the employee's ongoing confidentiality obligations.

4. SAFEGUARDING AGAINST ALLEGATIONS OF TRADE SECRET MISAPPROPRIATION

4.1 Pre-existing Skills and Expertise

The courts, in principle, recognise a distinction between an employee's general knowledge and skills and protectable trade secrets.

The Supreme People's Court stated in a working paper that knowledge, experience and skills mastered and accumulated by employees in the process of work shall constitute part of the personal characters of employees, and employees have autonomy to use them after quitting a job, except the trade secrets of their employers.

A ruling made by the Supreme People's Court in a retrial case reflects a similar position. As labourers who have the ability to learn, employees are bound to master and accumulate the knowledge, experience and skills related to the work they perform during the employment. Except in the case of trade secrets belonging to the employer, the knowledge, experience and skills constitute a part of the employee's personality and are the basis of their viability and labour capacity. After employees leave, they have the freedom to use their own knowledge, experience and skills to win the trust of customers and thus form a competitive advantage, which does not violate the principles of good faith and generally accepted business ethics.

In China, there is no "inevitable disclosure" doctrine, nor a clear-cut line between an employee's general skills and experience versus expertise derived through exposure to the employer's trade secrets. Employers should bear the burden to specify the scope of the trade secret, thereby distinguishing the trade secrets they claimed from an employee's general knowledge and skills.

4.2 New Employees

New employees holding trade secret information from their past may subject the new employer to third-party misappropriation liability. Employers should check and verify the new employee's obligation of non-compete and confidentiality, including the scope and term effectiveness of such obligation. Employers should discuss trade secret protection with employees before they are hired. At pre-employment interviews, new employees should be given a copy of the Trade Secret Protection Policy and be required to provide a written commitment acknowledging having read and understood it and promising that new employees are not bringing trade secrets or disclosing the trade secrets when performing the new job.

5. TRADE SECRET LITIGATION

5.1 Prerequisites to Filing a Lawsuit

In terms of procedure requirements, there is no prerequisite that a trade owner must satisfy before filing a lawsuit based on the legal theory of trade secret misappropriation. However, in the case that an employee steals a trade secret and the owner claims its right on the ground of breach of labour contract or non-compete obligation, the dispute would be identified as a labour dispute and therefore application for arbitration would be a prerequisite before initiating a civil litigation.

5.2 Limitations Period

The general statutory limitation of three years provided in the Civil Code applies to trade secret claims. The statutory limitation is calculated from the date on which the right-holder knows or ought to be aware of the damage to the rights and the exact offending party, and can be suspended or interrupted.

In addition, if a trade secret claim is filed as a labour dispute, then according to the Law on Labour-dispute Mediation and Arbitration, the limitation period for application for arbitration of a labour dispute is one year, which shall be calculated from the date on which a party knows or ought to be aware of the infringement of its rights, and such limitation period can be suspended or interrupted. Where a party has objection to the arbitral award of a labour dispute case, it may initiate a litigation to a people's court within 15 days from the date it receives the award.

5.3 Initiating a Lawsuit

To initiate a trade secret lawsuit, the plaintiff should submit a complaint with specific claim(s), facts and reasons, preliminary evidence for infringement and necessary identity documents, such as a business licence or power of attorney to persons being entrusted as an agent in the lawsuit, to the court having jurisdiction over the case. In addition, the plaintiff should pre-pay the court fees.

5.4 Jurisdiction of the Courts

Territorial Jurisdiction

As there is no special provision on the jurisdiction of a trade secret claim, the general provisions of the Civil Procedure Law should apply.

If a trade secret claim is filed as a tort lawsuit, according to Article 28 of the Civil Procedure Law, it should be under the jurisdiction of the people's court at the place where the tort occurs or at the domicile of the defendant. The aforesaid "place where the tort occurs" includes the place where the tort is committed and the place where the result of the tort occurs. For a trade secret lawsuit, the "place where the tort is committed" is the place where the defendant is accused of committing the infringement, which includes the place where the trade secret is obtained, the place where the trade secret is disclosed and the place where the trade secret is used; the "place where the result of infringement occurs" shall be interpreted as the place where the direct result of infringement occurs. Notably, the plaintiff's domicile cannot be simply deemed as the place where the result of infringement occurs.

If a trade secret claim is filed as a contract dispute case, according to Article 23 of the Civil Procedure Law, it should be under the jurisdiction of the people's court at the domicile of the defendant or at the place where the contract is performed.

Hierarchical Jurisdiction

The hierarchical jurisdiction varies depending on the amount of the case and the type of the trade secret in dispute.

Due to the professional nature and complexity of trade secret cases, trade secret cases should, in principle, be under the jurisdiction of intermediate people's courts. The primary people's courts approved by the Supreme People's Court can also accept and hear civil tort cases related to business secrets of first instance subject to the amount in dispute of the case. For cases concerning technology secrets, only intermediate people's courts or above have the jurisdiction over cases of first instance.

There are three specialised courts – ie, the Beijing IP Court, the Shanghai IP Court and the Guangzhou IP Court – that have the same hierarchical jurisdiction as the local intermediate people's court. Those three specialised IP courts have jurisdiction over all the first-instance technology secret cases and the business secret cases whose amount in dispute exceeds a certain amount in their respective regions.

The high people's courts and even the Supreme People's Court may also have jurisdiction over first-instance trade secret cases. Such cases heard by the high people's court or the Supreme People's Court shall have a significant impact or have a dispute of huge amount (at least RMB5 billion).

5.5 Initial Pleading Standards

A trade secrets plaintiff will not face different pleading standards as compared with other types of cases. An eligible pleading should satisfy the following criteria:

- the plaintiff has a direct stake in the case;
- there is/are specific defendant(s);
- there is/are specific claim(s), fact(s) and reason(s); and
- the court has jurisdiction over the case.

Accordingly, the plaintiff needs to provide necessary identity information for both the plaintiff and the defendant, a pleading with statements of claims and supporting evidential materials in a preliminary level for filing to the court that has proper jurisdiction.

To fulfil the above initial pleading standards, the plaintiff is generally required to provide supporting evidential materials that could preliminarily prove the existence of the asserted trade secret, the plaintiff's legal right over such trade secret and the infringement of the defendant. Thus, the plaintiff is not required to produce hard evidence to support the claims and facts stated in the complaint at the pleading stage.

5.6 Seizure Mechanisms

In China, civil seizure is available as a measure of property preservation that is served as an interim relief to the claimant before a final judgment in the case. For a case in which the claimant may suffer losses or a future ruling on the case would become difficult to enforce, the court may, pursuant to an application by the claimant or its own discretion before or during a litigation, rule on property preservation measures.

Property preservation measures including seizure, detainment and freezing of assets could be applied for a trade secret case as with other types of cases. Notably, the seizure as a measure of property preservation is not limited to the accused products containing the trade secret at issue but to a broader scope, which aims to guarantee effective enforcement of the ruling if the claimant wins.

For a property preservation application made before the litigation, the applicant shall provide a bond equivalent to the preservation amount it requested. Under special circumstances, the court may exercise its own discretion in determining the magnitude of the bond.

For a property preservation application made during the litigation, a bond is also necessary in general, except in certain specific cases. To illustrate, under the circumstances where the trade secret case is already crystal clear and the preservation order is unlikely to be misused, or where the claimant is a financial institution with independent solvency established with approval from the financial regulatory authorities, the bond may be exempted by the court.

In addition to the property preservation mentioned above, where an evidence may be lost or difficult to obtain in future, the court may, pursuant to an application by the claimant or its own discretion during the litigation, adopt preservation measures on such evidence.

5.7 Obtaining Information and Evidence

In China, the discovery mechanism is not available for a party to obtain relevant information and evidence from the other party in the pre-trial phase of a lawsuit as practised in common law jurisdictions. As the plaintiff bears the burden of producing evidence, in principle, the owner of a trade secret has to collect evidence independently.

Notwithstanding the above general rule, where a trade secret owner encounters difficulties in collecting evidence, the owner can seek judicial assistance. According to Article 64 of the Civil Procedural Law as well as the Provisions of the Supreme People's Court on Evidence in Civil Procedures, the party, on objective grounds, who is unable to gather evidence independently may apply for investigation and evidence collection by the people's court. Besides, the Judicial Interpretation on Trade Secret also stipulates that the right-holder may apply to the people's court for the investigation and collection of the evidence related to the claimed infringement that is kept by a public security organ, procuratorial organ or other court, if it fails to collect such evidence by itself due to objective reasons.

According to the Civil Procedure Law, a trade secret owner can obtain the following types of evidence:

- statements of litigants;
- documentary evidence;
- physical evidence;
- audio-visual materials;
- electronic data;
- witness testimony;
- appraisal opinion; and
- investigation records.

Apart from other types of evidence, appraisal opinions are commonly used in a trade secret lawsuit, especially for cases involving technology secrets.

The time period for producing evidences may be agreed upon by the parties subject to approval of the people's court. Generally, the parties should submit evidence to the court within such period.

5.8 Maintaining Secrecy While Litigating

In order to maintain the secrecy of trade secrets in litigation, China has made clear provisions on the confidentiality measures applicable to lawsuits in various laws, judicial interpretations and judicial policy documents. The basic rules to maintain secrecy include the following:

- the court should hold a non-public hearing upon application;
- the parties should not present the evidences that involve the trade secrets in public when presenting such evidence in the courtroom; and
- the parties should not cross-examine the written evidences that involve the trade secrets in public.

In practice, the court may further take the following measures to keep trade secrets confidential:

- restrict or prohibit the reproduction of confidential evidence;
- display confidential evidence only to the attorney; and/or
- order the signing of a confidentiality undertaking, etc.

5.9 Defending against Allegations of Misappropriation

The main defences against misappropriation that can be used by the defendant in a trade secret litigation include the following:

- the "trade secret" claimed by the plaintiff does not meet the statutory requirements of a trade secret;
- the plaintiff is not a proper right-holder of the "trade secret";
- the plaintiff fails to take reasonable measures to maintain secrecy;
- the information used by the defendant is not the same or similar to the "trade secrets" claimed by the plaintiff, or materially different from such "trade secrets"; and
- the defendant did not access or use the information at issue through an improper way; eg, relevant information can be easily obtained through public channels without paying a certain price; the defendant obtained the relevant information through independent development or reverse engineering; the defendant has lawful right to use the relevant information, such as lawful purchase, lawful acceptance of the licence and acquisition in good faith; the defendant did not know that the source of the relevant information was illegal; and there was no intentional infringement of the right-holder's trade secrets.

In addition, the defendant can also defend against the damages claimed by the plaintiff by rebutting the causation between the damage and the misappropriation, as well as the calculation method and composition of the damages.

5.10 Dispositive Motions

In China, there is no equivalent practice for "dispositive motions" as in common law jurisdictions. A court trial cannot be avoided unless the court finds that the case does not fulfil the requirements for filing a litigation as provided in the Civil Procedure Law after accepting the case. The court will dismiss a case where:

- the plaintiff does not have a direct interest in the case;
- there is no identifiable defendant;
- the pleading fails to provide specific claims and facts and reasons; and
- the court does not have jurisdiction over the case.

5.11 Cost of Litigation

The costs that the parties to a trade secret litigation may expect to incur mainly include:

- attorney fees;
- the costs for producing evidence, such as notarisation fees and investigation fees; and
- the court fees calculated based on the damages claimed by the plaintiff.

Where the case involves complicated technology information, it is common for the parties to engage an appraisal agency or an expert witness to identify the critical matters in a trade secret case, such as the non-public nature of the trade secret at issue, and the similarity between the plaintiff's trade secret and the information held by the defendant, which may incur additional costs for producing evidence.

In China, a contingency fee arrangement is allowed if the following requirements provided in

the Administrative Measures on Fees for Lawyer Services are satisfied:

- the case should be a civil case involving a property relationship; and
- the client has been clearly informed of the government-guided prices for legal services but still insists on being charged a contingency fee.

The PRC legislature or the administration authorities have not released any laws or regulations on litigation financing. As reported, some litigation financing service platforms have been established in recent years. Although litigation financing services have been available in China, such market is still underdeveloped.

6. TRIAL

6.1 Bench or Jury Trial

In China, a trade secret case is tried and decided by a collegial bench consisting of judges or both judges and people's jurors. A collegial bench normally consists of three members designated by the court. The parties do not have the right to decide the composition of a collegial bench.

Notably, the role of people jurors in a collegial bench is different from the jurors under the jury system in common law jurisdictions. Such people jurors enjoy the same authorities and bear the same obligations as judges, responsible for both factual and legal issues, and each of them has one vote in the decision-making process.

6.2 Trial Process

Generally, trade secret cases follow the general civil procedures like other types of cases. A complete trial process of civil litigation normally includes the following stages:

- pre-hearing preparation;
- announcement of disciplines of the court hearing, and rights and obligations of the parties;
- opening statements by the parties;
- court investigations focusing on evidence presentation and examination (including hearing testimony from live witnesses, if any);
- court debate; and
- closing statements by the parties.

At the end of the trial proceeding, the court may seek the parties' opinion on whether they accept mediation. If either party refuses mediation, the court will adjourn the hearing. Then the court will conduct internal deliberation and will render the judgment in due course.

The time required for a trade secret trial depends on the complexity of the case. The trial generally lasts from several hours to several days.

6.3 Use of Expert Witnesses

Chinese law does not set out special provisions on expert witnesses or identify expert witness testimony as an independent type of evidence. The so-called expert witness may present his or her opinions on certain issues to the court according to the following rules.

- Appraisal opinions issued by a qualified appraisal agency are recognised as a statutory type of evidence under the Civil Procedure Law, which, to some extent, could be deemed as opinions of experts. The parties to a trade secret case may apply for appraisal on complicated issues such as the scope of the trade secret at issue and the similarity comparison between the trade secret at issue and the information held by the defendant. The court may also decide to engage an appraisal agency to issue appraisal opinions on its own initiative depending on the needs of a case.

- The Civil Procedure Law also established the "expert auxiliary system", which allows the parties to apply to the court for having a person with special expertise present before the court to provide opinions regarding the appraisal opinion or to explain specialised issues such as technical matters to the court. The opinions given by such person with specialised expertise are deemed as statements of the parties, which is subject to examination of the court and the other party.
- The court may assign technical investigation officers to participate in litigation activities when adjudicating IP cases that are highly specialised, such as patents, technical secrets and computer software. The opinions of the technical investigation can be used as a reference for the technical facts of the collegiate bench.

7. REMEDIES

7.1 Preliminary Injunctive Relief

The Civil Procedure Law has established a behaviour preservation system that is functionally similar to a preliminary injunction. Such behaviour preservation may be granted by the court according to the claimant's application or ordered directly by the court even without the claimant's application.

Notably, the Judicial Interpretation on Trade Secret also stipulates a special provision for the behaviour preservation applicable to trade secret cases. Where the alleged infringer attempts to obtain, disclose, use or allow others to use the claimed trade secret by improper means, or has done so, and if the failure to take preservation measures will make a future ruling on the case difficult to enforce or cause irreparable damage to the right-holder, the court may render a ruling to take preservation measures.

The duration for behaviour preservation shall be reasonably determined by the court based on the claimant's request. Generally, an order to suspend infringement upon a trade secret shall be upheld until the ruling for the case takes effect.

A bond is required for the behaviour preservation ordered either before or during the litigation process. The amount of such bond shall be equivalent to the loss that may be incurred by the respondent as a result of enforcement of the preservation.

7.2 Measures of Damages

According to the AUCL and the Judicial Interpretation on Trade Secret, the damages to a successful claimant may first be calculated based on the following measures:

- the losses suffered by the claimant;
- the gains obtained by the respondent; or
- a reasonable estimation based on referable royalty fees.

To prove the losses suffered by the claimant, evidences such as annual output and profit margin of the claimant, sales performance before and after the infringement in comparison and sales amount of the infringing products would be required. To prove the gains obtained by the respondent, evidences such as annual output and profit margin of the respondent and sales amount of the infringing product would be required. To employ the measure of royalty fees, a licence agreement qualified as a reasonable reference and corresponding payment documents would be required.

However, under the circumstance where the above three measures of damages are unavailable, the court may determine a compensation below RMB5 million according to the specifics of each case.

Also, it should be noted that under the circumstance where the trade secrets become known to the public due to the infringement, the amount of damages thereof may be determined based on the commercial value of the trade secrets determined on the basis of factors such as costs of research and development, the revenue derived from the implementation of such trade secrets, the potential benefits, and the period of time during which the competitive advantage might be maintained.

For general misappropriation, damages are still awarded with a principle to compensate the losses of the aggrieved party by measures as illustrated above. Therefore, a successful respondent may seek damages only when there are losses incurred in certain specific cases, such as improper application of interim relief.

However, for malicious misappropriation, punitive damages are available to a successful claimant according to the AUCL, amounting to one to five times the amount calculated based on the losses suffered by the claimant or the gains obtained by the respondent. However, it should be noted that such punitive damages shall be applied in cases with serious consequences only, the standards of which remain to be observed in future judicial practices.

7.3 Permanent Injunction

In China, permanent injunctions are awarded in the form of cessation of infringement, exclusion of hindrance, elimination of risks and/or specific performance based on establishment of infringement.

Among the permanent reliefs, cessation of infringement is a typical remedy applied in a trade secret case. The duration of such relief shall generally expire when the trade secret is known to the public. However, if such duration is obviously unreasonable, a judgment may be made to limit a certain duration or scope.

Chinese law does not offer the remedy of recalling the product that is the subject of the accusation to the claimant in a trade secret misappropriation case.

In addition, limiting an employee's subsequent employment is not an applicable permanent relief either since the principle of inevitable disclosure has not yet been applied and the free flow of talent is highly valued in China. However, if there is a proper non-competition agreement ahead, which is commonly used in China, the claim to limit an employee's subsequent employment for not more than two years may be supported in a labour dispute case.

7.4 Attorneys' Fees

A successful plaintiff could recover its attorneys' fees in a trade secret litigation. According to the AUCL, the compensation amount shall also include reasonable expenses paid by the plaintiff to stop the infringement. In judicial practices, such reasonable expenses also include the attorneys' fees subject to the precondition that the plaintiff has clearly claimed the attorneys' fees in the pleadings and the attorneys' fees claimed by the plaintiff are within reasonable limits.

On the other hand, a successful defendant is, in principle, not entitled to attorneys' fees, except that:

- in false litigation and malicious lawsuits that result in direct damages to the defendant, the court may, on the basis of specific circumstances, support the reasonable compensation for attorneys' fees and other valid claims proposed by the non-fault defendant according to the law; and

- under the circumstance where the parties once made an agreement stating in writing that the attorneys' fees shall be borne by the party losing the lawsuit, such agreement shall be binding.

7.5 Costs

In a trade secret litigation, a successful plaintiff may recover the reasonable expenses to stop the infringement. The typical expenses that may be supported in judicial practice include the court fees, investigation and evidence collection fees (eg, notary fees, document copy fees, appraisal fees) and attorneys' fees. The plaintiff should raise a claim of recovering such fees and provide the relevant evidence. The court will assess the reasonableness of the amount and make a decision in the judgment.

A successful defendant will not be required to bear court fees. In addition, the fees for applying for judicial appraisal would usually be borne by the losing party in a trade secret case.

8. APPEAL

8.1 Appellate Procedure

As with other types of cases, against a first-instance judgment of a trade secret case, the plaintiff and the defendant shall both have the right to file an appeal with the next higher level court within 15 days after the service of the written judgment, except if it is made by the Supreme People's Court.

Most orders in a trade secret case of first instance cannot be appealed, except for orders on non-acceptance of case, objection to jurisdiction or dismissal of case. For such types of orders, parties shall appeal within ten days after their service.

Notwithstanding the foregoing, according to relevant judicial interpretation for trial of intellectual property cases, judgments and specific orders in cases of first instance concerning technical trade secrets should be directly appealed to the Supreme People's Court instead of the next higher level court from 1 January 2019.

In principle, the trial of an appeal case shall be completed within three months after the appeal is filed. Such period could be extended subject to the approval of the court.

8.2 Factual or Legal Review

The appeals courts will review both factual and legal issues. Generally, the appellant has the right to decide which issues are to be preserved or waived for appeal in its petition. And the review will focus only on the factual and legal issues related to the appeal petition, except where the judgment of first instance violates the prohibitive provisions of the law or harms national interests, public interests or the legitimate rights and interests of others.

The court of second instance shall form a panel for the appeal case and conduct a hearing to try the appeal case. However, upon examination of the case file, investigation and questioning of litigants, where there is no new fact, evidence or reason, and the panel deems that a hearing for trial is not necessary, the case may be tried without a hearing.

9. CRIMINAL OFFENCES

9.1 Prosecution Process, Penalties and Defences

The Criminal Law, in Article 219, regulates the acts that seriously infringe upon trade secrets as the crime of infringing upon trade secrets. According to this article, whoever commits any of the following conducts to infringe upon a

trade secret shall, if the circumstances are serious, be sentenced to fixed-term imprisonment of not more than three years and a fine or be sentenced to a fine only; or if the circumstances are especially serious, be sentenced to fixed-term imprisonment of not less than three years nor more than ten years and shall also be fined:

- obtaining the aggrieved party's trade secret by theft, bribery, fraud, coercion, electronic intrusion, or any other illicit means;
- disclosing, using, or allowing any other person to use a trade secret obtained from the aggrieved party by the means as specified in the preceding subparagraph;
- disclosing, using, or allowing any other person to use a trade secret in its possession, in violation of its confidentiality obligation or the requirements of the aggrieved party for keeping the trade secret confidential; or
- whoever knows any conduct set forth in the preceding paragraph but still obtains, discloses, uses, or allows any other person to use the trade secret shall also be punished for the crime of infringing upon trade secrets.

In addition to the above provisions, the Criminal Law also provides that whoever steals, pries into, buys, or illegally provides any trade secret for any overseas institution, organisation or individual shall be sentenced to fixed-term imprisonment of not more than five years and a fine or be sentenced to a fine only; or if the circumstances are serious, be sentenced to fixed-term imprisonment of not less than five years and a fine.

The criminal prosecution for trade secret theft could be made by the procuratorate or the aggrieved party itself.

Possible defences used in civil cases as illustrated in **5.9 Defending against Allegations of Misappropriation** may also be effective defences available for a criminal charge for theft of trade secrets.

Some potential defences are typical only in criminal cases, such as:

- there is no adequate criminal evidence indicating the infringement and the "access and substantial similarity" standard is not enough for criminal cases; and
- the infringement is out of negligence since the crime for trade secret misappropriation can only be an intentional crime.

In China, there is no crime of economic espionage under the Criminal Law. In the case of meeting the above-mentioned constituent requirements for the crime of infringing upon trade secrets, the economic espionage offences can be prosecuted with reference to such trade secret crime.

In the criminal prosecution proceedings for the crime of infringing upon trade secrets, the right-holder, as the usual victim, has the right and bears the obligation to co-operate and co-ordinate with the relevant public security organ or procuratorate in the investigation on trade secret misappropriation.

Firstly, the right-holder should report the misappropriation upon its trade secrets to the relevant public security organ and provide preliminary clues, so that the organ can file a case for investigation. Secondly, at the stage of investigation, the right-holder may actively provide the public security organ with substantive evidences concerning the misappropriation. According to the Criminal Procedure Law, the statement made by the victim itself can be used as important evidence to prove the facts in a trade secret infringement case. Thirdly, at the review and prosecution stage, the procuratorate shall, in accordance with the Criminal Procedure Law,

hear and record the opinions of the victim on both the factual issues and the applicable law, and the victim can also take the initiative to provide written opinions to the procuratorate.

10. ALTERNATIVE DISPUTE RESOLUTION

10.1 Dispute Resolution Mechanisms

Arbitration and mediation are common ways of alternative dispute resolution that are available for resolving trade secret disputes. For both arbitration and mediation, the clear consent of the parties is the prerequisite to trigger such proceedings; however, the parties are unlikely to reach such consent in a trade secret misappropriation dispute. Thus, arbitration and mediation are not commonly used in trade secret infringement cases.

Mediation generally includes court mediation, people's mediation and commercial mediation. Strictly speaking, court mediation is not recognised as an ADR mechanism as it forms part of litigation procedures.

People's mediation committees and commercial mediation centres have been widely established in China. The parties may voluntarily conclude mediation agreements to resolve trade secret disputes, which are legally binding upon the parties. The violation of the mediation agreements can be brought to the court for future dispute settlement.

Mediation is generally the most convenient and cost-efficient way to settle disputes. The confidentiality of trade secrets can be secured during the mediation via more flexible ways as compared with litigation proceedings. Different from arbitration, parties in the process of mediation are not entitled to apply for interim reliefs from the court, and thus mediation may not be suitable when the case is urgent, which requires interim reliefs from the court, or when the disputes are under an irreconcilable and strong conflict between the parties.

Zhong Lun Law Firm is one of the largest full-service law firms in China, with over 340 partners and over 2,200 professionals working in 18 offices in Beijing, Shanghai, Shenzhen, Guangzhou, Wuhan, Chengdu, Chongqing, Qingdao, Hangzhou, Nanjing, Haikou, Tokyo, Hong Kong, London, New York, Los Angeles, San Francisco and Almaty. Zhong Lun is capable of providing clients with high-quality legal services in more than 60 countries across a wide range of industries and sectors through its specialised expertise and close teamwork. The firm is able to assist both domestic and overseas clients in protecting their trade secrets when doing business in China through comprehensive solutions. The firm's legal services regarding trade secret protection consist of assisting clients in establishing and implementing trade secret protection rules, managing risk of trade secret leakage in dealing with business partners and resolving disputes through unfair competition and trade secret litigation.

AUTHOR

Yi Xue has been engaged in legal practice for over 20 years, and now is a partner of Zhong Lun Law Firm based in Beijing. He is one of the pioneer lawyers practising competition law in China. As his special expertise is in anti-unfair competition law, Mr Xue is capable of providing professional service on matters of trade secret protection, including assisting clients in establishing internal trade secret protection policy, preventing trade secret leakage in transactions by effective contractual arrangement, and participating in trade secret litigation. Besides, his labour law expertise also helps to assist clients in protecting trade secrets through employment management.

Zhong Lun Law Firm

23-31/F, South Tower of CP Center
20 Jin He East Avenue
Chaoyang District
Beijing 100020
P.R China

Tel: +86 10 5957 2057
Fax: +86 10 6568 1022/1838
Email: xueyi@zhonglun.com
Web: www.zhonglun.com

中倫律師事務所
ZHONG LUN LAW FIRM

DOMINICAN REPUBLIC

Law and Practice

Contributed by:
Edward Veras and Rodrigo Delgado
Delgado Malagón – Veras Vargas see p.43

CONTENTS

1. LEGAL FRAMEWORK

1.1 Sources of Legal Protection for Trade Secrets

The Dominican Republic is a country of positive, written law. The main texts of law that regulate trade secrets in this jurisdiction are:

- Law No 20-00 on industrial property;
- Law No 42-08 on the defence of competition; and
- the Labour Code (Law No 16 -92), in relation to the obviously unauthorised disclosure of commercial and industrial secrets by workers.

1.2 What Is Protectable as a Trade Secret

The text of Dominican law does not seem to be very demanding with regard to the type of information that can be protected under the legal regime of trade secrets, since it is content to establish that it can consist of "any undisclosed commercial information that a natural or legal person possesses, that can be used in any productive, industrial or commercial activity, and that is capable of being transmitted to a third party". As long as it is undisclosed information, in respect of which measures have probably been taken to keep it out of the indiscriminate reach of third parties, the text does not require per se any condition regarding the quality of the information. It mentions "any commercial information", capable of being used – without indicating what form or type of use – in a productive, industrial or commercial activity. Under this ambiguous cloak, any information could qualify. However, the majority of international authors agree on the following requirements: that they grant the owner a competitive advantage in the market and that it be treated in a way that constitutes a reasonable prevention against its disclosure to the public or to competitors.

1.3 Examples of Trade Secrets

After more than 20 years of application of current regulations, there is not a single precedent emanating from the Supreme Court of Justice which refers to trade secrets. In contractual practice, there is a tendency to confuse the instrument that supports the information protected by the trade secrets regime with the protected information itself. This occurs for strategic convenience, so that the document that establishes the obligation of confidentiality regarding the commercial secret does not refer to the protected information, which would be kept secret from whoever reads the document. Given the aforementioned flexibility of the legislation, in principle, practically any commercial information – with respect to which the measure to be kept confidential has been adopted – qualifies as a commercial secret in this jurisdiction.

1.4 Elements of Trade Secret Protection

Based on the text of the applicable law, it would be sufficient – to qualify as a commercial secret in the Dominican Republic – that the information is undisclosed (that is, secret), that it is in the possession of a natural or legal person (its owner), which may be transferable to a third party and that can be used in any productive activity, whether industrial or commercial. We reiterate that the majority of international authors are not satisfied with the criteria expressed in Dominican law, but add as requirements: that they grant the owner a competitive advantage in the market and that it be treated in a way that constitutes reasonable prevention against disclosure to the public or competitors.

1.5 Reasonable Measures

The standard for evaluating whether or not the owner of the trade secret has taken reasonable measures to protect its secret varies in taking into consideration the situation of the potential infringer of its rights. The standard for the worker in relation to the technical, commercial, or manu-

facturing secrets of his employer, is lower, since the law requires the worker not to disclose them neither for the duration of the employment contract nor after its termination. Regarding workers, the only thing then would be to determine whether or not the information constituted a technical, commercial or manufacturing secret.

That is why it is convenient, but not essential, that workers sign documents acknowledging having come into contact with certain confidential information and its support, and reiterate the obligation not to disclose it in any way or copy it. In cases of technology transfer (know-how) and licences for the use of trade secrets, it is necessary to take contractual measures so that the recipients of the secret information keep it in this way, and that all the people in their organisations access to this reserved information is also obliged to keep a reservation and not to copy it.

1.6 Disclosure to Employees

When the worker agrees to a trade secret because of the work he performs, the obligation to maintain confidentiality about the trade secret is imposed by the labour law. Different is the situation of any other worker, that is, of one who does not need to access that information to be able to fulfill his work responsibilities. Obviously, in the latter case, the protection of the trade secret is put at risk since its owner would be disclosing it to people who are not required to know it, which undermines the first condition of its legal protection regime: that the information is not within the reach of anyone.

1.7 Independent Discovery

Obviously, independent discoveries and deductions and inferences through reverse engineering – and scientific or market studies – do not infringe the rights of the owner of the secret, who lacks preventative actions aimed at preventing others from accessing the information through science or investigation. Protection is only against spurious means of obtaining information protected as a trade secret.

1.8 Computer Software and Technology

In the Dominican Republic, computer programs are normally protected by copyright (Law No 65-00). Copyright, in this jurisdiction, is inherent to protected creation – independent of its registration in a public registry. Therefore, it is perfectly possible that a computer program, whose code is protected by adopting measures to keep it as a secret, enjoy simultaneously the protection of Dominican Republic copyright laws and laws relating to intellectual property and competition.

1.9 Duration of Protection for Trade Secrets

Obviously, the protection of the trade secret will be effective as long as its owner is successful in keeping the information a secret. This implies the rigorous establishment of a protocol for the handling of information by internal collaborators and external allies. Accidental disclosure of trade secrets places them legitimately in the hands of the receiver.

If the disclosure places the trade secrets in the public domain, the protection along with the secret ends. On the other hand, the controlled disclosure – under the subscription of the appropriate documents – of the commercial secrets to a greater number of people in the organisation offers the opportunity to keep the commercial secret under control and to open up greater possibilities of approaching the justice system in search of a court order that prevents the unauthorised disclosure and use of the trade secret, which will always be possible before the information is made public.

1.10 Licensing

One way to earn money from trade secrets is their licensing, for the benefit of third parties,

in exchange for remuneration. These types of agreements tend to be limited to specific time periods and also in terms of their purposes.

1.11 What Differentiates Trade Secrets from Other IP Rights

The protection of trade secrets is quite different from the protection of other intellectual property rights. The former only enjoys protection as long as it is kept as "secret" information, whereas in the latter the registry – public – is either the starting point of protection or a suitable pre-constituted proof of the right.

1.12 Overlapping IP Rights

Normally, trade secrets and patents are mutually repelled. This is because while the trade secrets regime is based on the need to keep protected information secret, the patent responds to the opposite logic: it is the publication and registration that generates rights for the patent holder. The case of computer programs was previously mentioned which, in this jurisdiction, can be protected by both copyright and trade secrets, insofar as copyright does not arise in the Dominican Republic with the registration of the work in a public registry.

1.13 Other Legal Theories

In principle, nothing opposes the possibility of filing claims related to trade secrets which are not based on misappropriation. Additionally, nothing opposes the filing of a legal action tending to oblige an employee or a former employee to fulfill their fiduciary duties, refraining from disclosing the trade secret to which they have legally or illegally accessed. Given the nature of the action for unfair competition in the Dominican Republic – an action in civil liability in any case – it is possible to sue whoever interfered by inducing an employee to reveal a trade secret, as a co-responsible and accomplice of the violation of a contractual or legal obligation.

1.14 Criminal Liability

The penal code of 1884 makes the misappropriation of trade secrets an offence – punishable by imprisonment from three months to a year – to seize papers or letters from a person to access and disclose their secrets. The same legislation sanctions – with imprisonment from one to six months – all persons who access the secrets of others by reason of their profession or trade (this applies to workers), and who disclose them to third parties (except in cases where the law obliges them).

It is obvious that the purpose of this rule was not to prevent or dissuade people from accessing a company's trade secrets in order to benefit from them. These tools will be useful every time the secret has been revealed to third parties, but they are not applicable when the person stealing the secret uses the information for their personal gain and without disclosing it to third parties.

Both Law No 20-00 on industrial property and Law No 42-08 on the defence of competition qualify the act of accessing commercial and business secrets as one of unfair competition. This gives rise to file a legal action in civil liability for acts of unfair competition, but said norm does not contain any special criminal offence on the matter.

1.15 Extraterritoriality

Civil liability legal actions in Dominican law are personal actions. Therefore, the domicile of the defendant is that which establishes the territorial jurisdiction to hear the claim. The place wherein the event generating the damage took place is irrelevant in the hypothetical situation of the improper appropriation of a commercial secret. For the national courts to be able to hear an action in civil liability, for the commission of acts of unfair competition, it is enough that the defendant has a domicile or a branch in the Dominican Republic. If the defendant does

not have a domicile in the Dominican Republic, the Dominican courts are, in principle, unable to hear the civil action.

2. MISAPPROPRIATION OF TRADE SECRETS

2.1 The Definition of Misappropriation

In accordance with Law No 20-00: "A business secret will be considered acquired by means contrary to honest uses and practices when the acquisition results, among others, from industrial espionage, breach of a contract or other obligation, abuse of trust, infidelity, breach of a duty of loyalty or instigation to carry out any of these acts". Law No 42-08 makes it clear that the unauthorised appropriation of protected information is sufficient for a claim of trade secret misappropriation, without it being necessary to prove the use by the offender. When the infringer has had access by virtue of a contract or by their participation in a key position of the company that has allowed them to access the secret, then it is the obligation of the owner of the secret to prove the unauthorised use. When the infringing person has not had legitimate contact with the reserved information, it is sufficient to prove that said person has had access to this information – while in charge of either the person under suspicion or the defendant – to demonstrate that he has had access to the information through a lawful way.

When the infringing person has not had legitimate access to the reserved information, it is then sufficient for the plaintiff to simply prove that the defendant has had access to it. It is then the burden of the person under suspicion, or the defendant, to prove that the access they had to the protected information was lawful.

2.2 Employee Relationships

In accordance with the Labour Code, it is a duty of every worker, vis-à-vis their employer: "To rigorously keep the technical, commercial or manufacturing secrets of the products to which they directly or indirectly produce, or of which they have knowledge for good reason. Of the work they carry out, as well as of reserved administrative matters whose disclosure may cause damage to the employer, both during the duration of the employment contract and after its termination".

This duty of reserve does not usually entail a time limit, so it theoretically extends to the entire duration of the secret or the life of the worker or ex-worker. Violation of this obligation by the worker is also a cause for justified dismissal, that is, termination for just cause, based on the misappropriation by fault of the worker's.

2.3 Joint Ventures

There is expressly no provision in the Dominican commercial partnership law, nor in the civil code that refers to the obligation of a partner, not to disclose the commercial secrets of the partnership in which they are participants.

However, there are provisions in said law that prevent an administrator of a partnership from performing acts that concur with the partnership they administer. Therefore, if acts of so-called fair competition are forbidden to the director, with respect of the company they themselves manage, it is even more forbidden for them to perform acts of unfair competition, such as the disclosure of business secrets for the benefit of third parties.

Strangely, this rule only exists for the administrators, who may or may not be partners of the entity. It does not apply to the partners.

2.4 Industrial Espionage

Law No 20-00 only mentions the term "industrial espionage" once, without defining it, as an unfair means of access to a business secret. In principle, this would only give rise to a legal action of civil liability for an act of unfair competition. However, the act of espionage could also fit within those of theft and disclosure of secrets, which are foreseen and sanctioned by the penal code with a penalty of three months to one year in prison.

3. PREVENTING TRADE SECRET MISAPPROPRIATION

3.1 Best Practices for Safeguarding Trade Secrets

The influence of multinational companies and their lawyers has enriched local practice. Some of the best practices are those whose purpose is to restrict or limit the number of people with access to each trade secret by enforcing the requirement of signing a confidential information nondisclosure agreement to be able to access it. This type of document must define the instruments that contain the reserved information and prevent the latter from being copied in any way or disclosed. The establishment of manuals with restricted access – and marked as confidential – for the performance of specific operations, formulas and their mixtures, among others, tends to create a documentary trace that always helps identify who has had access, and by what means, to the whole or part of trade secrets.

In the computer programming industry, programmers must know the code, but should not have access to the ability of copying it. In the chemical industry, it is convenient to relabel the most relevant ingredients and name them in code, so that only the highest level technicians know about the use of these ingredients and their proportions in the formulas.

3.2 Exit Interviews

It is not customary in the firm's jurisdiction to conduct exit interviews with employees whose contracts have been terminated. It is, however, an increasingly widespread practice to require the signing of a confidentiality and non-competition agreement that coerce the outgoing worker into not using trade secrets for the benefit of a competitor. However, this is totally illusory when the employment contract has ended under conditions of disagreement between the parties. But, as already mentioned, the Labour Code forces the worker to respect the employer's trade secrets both during the term of the employment contract and after its termination.

4. SAFEGUARDING AGAINST ALLEGATIONS OF TRADE SECRET MISAPPROPRIATION

4.1 Pre-existing Skills and Expertise

The jurisdiction in question knows no distinction between the general knowledge and skills of the worker and a trade secret subject to protection. This does not mean, however, that doctrine and common sense do not lead us to make this distinction. The inevitable discovery is not contemplated in the law either, but all experts are aware of said doctrine and its implications. It is thus foreseeable that it will eventually be recognised by jurisprudence.

4.2 New Employees

It is clear that "the table is set" so that, in the near future, litigation based on the alleged misappropriation – through former employees – of trade secrets. However, on many occasions, previous work experience within a competing organisa-

tion constitutes one of the greatest attractions for the company that is hiring the new worker.

The disclosure by the recruited worker of their having accessed privileged information in their former job, and their duty to reserve, should be a generalised practice. This should be encouraged and promoted by the hiring company, to obtain pre-constituted proof that the recruitment does not take a view on the commercial secrets that the recruited person possesses, which must be kept under strict confidentiality.

5. TRADE SECRET LITIGATION

5.1 Prerequisites to Filing a Lawsuit

Normally, when the theft of a trade secret occurs, the firm is in the presence of a situation that generates a civil liability litigation. There is no prior, mandatory or essential procedure at the beginning of a civil liability action. This is regardless of the fact that it is possible to criminally prosecute people who by reason of their profession are depositories of other people's secrets and reveal them, as well as those who, in order to discover others' secrets, seize their papers or letters and disclose the the secrets. The Dominican Republic's legal system provides for the possibility of accessing precautionary measures aimed at stopping illicit disturbances, such as situations that endanger a trade secret.

5.2 Limitations Period

Part of the strength of the adopted solution consists of abandoning the brief statute limitation of extra contractual civil liability actions, which is normally one year, computed from the commission of the generating event. Law No 20-00 established a four-year statute of limitation period for this civil action.

5.3 Initiating a Lawsuit

Dominican law does not establish any requirements or steps prior to filing a lawsuit for the violation of trade secrets. Common sense indicates that it is convenient to collect all the available evidence on the reasonable measures adopted to guarantee that the protected information is kept secret, and also the evidence that the offender has irregularly accessed the trade secret, either for personal use or for the benefit of a third party. An intimation or prior warning would always be very convenient to demonstrate the bad faith of the person who infringes the trade secret.

5.4 Jurisdiction of the Courts

Despite the fact that Dominican law divides the court of first instance into chambers (specialised by subject), in the tradition of local judicial organisation, civil and commercial matters are heard by the same judge (the civil and commercial chamber). The establishment of independent commercial courts never happened, became a project that was continuously postponed by Congress.

Notwithstanding the foregoing, the Council of the Judiciary has established the practice – in the main judicial districts of the country – of specialising a few of the civil and commercial chambers of the court of first instance to exclusively hear matters of a commercial nature, such as, obviously, a civil liability claim for misappropriation or undue disclosure of a trade secret.

5.5 Initial Pleading Standards

In the Dominican legal system, the burden of proof is on the plaintiff. The old Roman legal adage actori incumbit probatio denies any possibility of success to a claim that is based on simple information and beliefs without solid concrete evidence. However, not all the evidence has to be available at the time the claim is filed. The production of some evidence and the performance of certain investigative measures may

be requested and ordered by the court in the course of the process.

5.6 Seizure Mechanisms

The Dominican Republic's antitrust Law No 42-08 grants the power to the National Antitrust Commission to issue precautionary measures, when these are in accordance with the law and are not likely to cause irreparable damage. However, said law does not seem very coherent. Despite contemplating the possibility of adopting precautionary measures, it only retains the ability to impose administrative sanctions against some anti-competitive practices, which does not include the inappropriate obtaining or disclosure of trade secrets.

The knowledge and decision of the judicial actions for violation of commercial secrets will be,in principle, competence of the civil and commercial chamber of the court of first instance. The president of the court also has the power to adopt precautionary measures in provisional and urgent cases, but not in accordance with the legislation specialising in trade secrets if not by the rules of common law. However, the seizure of products produced in violation of a trade secret does not appear to be supported by Dominican Republic legislation.

5.7 Obtaining Information and Evidence

With regard to the differences between civil/commercial and criminal procedures, the latter aims more to conduct inquiries that point at obtaining evidence of the violation of a trade secret, provided there is a suspicion it was carried out from the disclosure of the secret by an unauthorised person who accessed it during their professional activity, or who obtained it by stealing letters or other documents owned by the owner of the secret.

The raids, kidnappings of documents and computer equipment, smartphones and interception of communications are possible within the framework of any criminal investigation. In commercial matters, there are no equivalent mechanisms to achieve this type of measure.

5.8 Maintaining Secrecy While Litigating

The first Dominican legal provision that prohibited the protection of trade secrets in the course of litigation was the 1992 Labour Code. Both Law No 20-00 on Industrial Property and Law No 42-08 on the Defence of Competition provide mechanisms aimed at maintaining the secret nature of trade secrets during the investigation and acquiring of knowledge of a case in which this type of information is handled, in administrative headquarters, before the National Office of Industrial Property and before the National Commission of Defence of Competition.

In all three cases, the owner of the secret is required to declare that the information contained in certain evidence contains business secrets and a resolution that recognises it, adopting mechanisms so that other litigants cannot access the protected content. Outside of these three matters, Dominican Republic judicial organisation law, which dates from 1927, would seem to govern, and establishes as a rule that all judicial files are public,except those for which special laws have voted exceptions based on the preservation of interests of the family.

Although in the firm's experience there are not many cases in which the litigants have tried to make use of this power, it is plausible that the judges of the judicial order, in any matter, order the pertinent measures – the law does not define them – to avoid that an unauthorised disclosure of a commercial secret occurs during the instruction of a process. Notwithstanding the foregoing, it is worth clarifying that ultimately it is the court employees who will ensure compliance or not with the declaration of reserve made

by the judge in relation to any information that may be considered a trade secret.

5.9 Defending against Allegations of Misappropriation

Dominican Republic law does not foresee a closed catalogue of defence means for specific types of cases.

Defences are usually classified as incidental and merits of the case. Incidental defences have a procedural cut, as they tend to prevent the trial proceedings from advancing. The exception of incompetence and that of connectedness, the nullity of some specific procedural activity, the incidents regarding the evidences, among others, tend to hinder the normal course of the instance and the issuance of a sentence.

The same occurs with the means of inadmissibility, tending to establish that the plaintiff has no quality or interest to sue, that the matter is res judicata or that the matter is prescribed (statute limitation).

On the other hand, defences on the merits tend to demonstrate either that the events did not occur in the manner alleged by the plaintiff or that the legal norms invoked are not those applicable to resolve the dispute.

There are no best practices that the legal community has recognised as the best options when it comes to defending these types of lawsuits.

5.10 Dispositive Motions

Dominican Republic legislation does not provide that a plaintiff or defendant has the right to bring a dispositive motion, prior to trial, that would resolve the case if granted.

5.11 Cost of Litigation

Contingent fees are provided for in the firm's legislation, but the majority of international clients prefer to avoid this type of remuneration, just as lawyers have adopted the practice of accepting contingent remuneration only if their client makes non-refundable advances, although eventually compensable – in the case of successful litigation – with contingent fees, that no case can exceed 30% of the amount litigated.

The authors are not currently aware of any financial institution, formal or informal, that is engaged in financing litigation in the jurisdiction in question. Given the different alternative routes that the owner of a trade secret can choose when they feel that their right has been violated, the authors consider it impossible to estimate the costs of a possible litigation.

6. TRIAL

6.1 Bench or Jury Trial

There are no jury trials in the Dominican Republic. All processes are decided, in the first instance, by a single judge, with the exception of criminal cases that entail penalties of at least five years in prison, which are decided on by a court composed of three judges. Appeals are heard by the Courts of Appeal which is made up of five judges, but whose quorum is completed by three of them.

6.2 Trial Process

While criminal trials in Dominican Republic are quite similar to what is seen on television and in American movies, which feature a dynamic oral-adversarial process and where oral litigation techniques and objections are fully used, the procedure before the Commercial jurisdiction is an antiquity, where the writings prevail. The parties hardly read the request for their conclusions and present their arguments in writing.

6.3 Use of Expert Witnesses

The code of civil procedure of 1884, whose last relevant reforms on the evidence regime dates from 1978, does not foresee the figure of the expert witness. Therefore, in principle and in the framework of commercial procedures, witnesses could only testify who perceived through their senses.

7. REMEDIES

7.1 Preliminary Injunctive Relief

This jurisdiction does not present the option of preliminary precautionary measures during the process, specifically designed for the case of commercial secrets. Only the classic precautionary measures could be used: the *referimiento* – of French origin – is available for all provisional and urgent matters. The precautionary measures of common law do not require the provision of a guarantee for their execution. The judge will always be careful not to specify a conclusion of their response, limiting themselves to issuing "waiting" measures.

7.2 Measures of Damages

Contrary to what happened with other intellectual property assets whose protection is recognised by Dominican Republic legislation, in which the law offers parameters and criteria for the compensation of the owner in case of infringement of their rights, the law does not offer any parameters for the compensation that can be claimed by the victim of an unauthorised appropriation or disclosure of their trade secrets.

In terms of extra-contractual civil liability, the remuneration must be in full and is not limited to foreseeable damage. When the violation comes from a co-contracting party, except in the case of malicious acts, the compensation must be limited to the foreseeable damage, which the parties normally estimate in estimating and limiting liability clauses. In no case are there punitive damages in the legal system, which clings to the criterion that there can be no enrichment without cause, since compensation is compensation for damage – patrimonial in this case – and not a sanction.

However, the amount of damage does not imply the loss of access to the information by the victim, but rather that it goes into the hands of specific competitors or into the public domain, losing a competitive advantage.

The criteria for compensation in comparative law could eventually be upheld by local courts. In the meantime, it will be necessary to assess,as in any civil liability action, the loss of business opportunities and loss of profits that emerge, for the victim, from the violation of their trade secret.

7.3 Permanent Injunction

In the Dominican Republic, there is no permanent injunction available to a trade secret claimant. There is no specific legal provision that allows a court to order that a product be taken off the market for being produced in violation of a claimant's trade secret. Although it was previously said that the labour code obliges workers to maintain secrecy regarding trade secrets that have been revealed to them by their employers, both during the duration of the employment contract and after its termination and without a time limit, there is no ex ante solution to the possible violation of this duty by the worker. Any measure before a worker would have to be ex post, since the right to employment and salary is a fundamental human right which no judge could limit when considering potential violations of a trade secret.

7.4 Attorneys' Fees

As a general rule, each party covers the professional fees of the attorneys who have represented it. Another thing happens with the expenses of the process, which can be recovered by the

party that has obtained a profit. This is the so-called award of costs. In daily practice, lawyers request – as Dominican Republic law allows it, when they advance them – that the condemnation of costs be diverted directly to the benefit of them, and not of their clients. However, it is reasonable to assume the full costs of a process, including professional fees, as part of the harm suffered by the person whose trade secrets have been breached. Once there is a sentence on costs, either for the benefit of the anxious party or their lawyer, the settlement is carried out by presenting a state to the judge who issued the sentence. It is a simple and expeditious mechanism. The party that is not satisfied can challenge the approved state of costs, before the competent Court of Appeal, through a fairly simple procedure as well.

7.5 Costs

Contrary to what happened with other intellectual property assets whose protection is recognised by Dominican Republic legislation, in which the law offers parameters and criteria for the owner to recover the costs of the process, the law does not offer any parameter regarding the costs for the victim of an unauthorised appropriation or disclosure of trade secrets. In force, then, are the parameters of common law, according to which are the costs of the process, eg, service fees, court fees, transfers from/to the court, stationery. They can be encompassed within the category of legal costs, claiming the condemnation of the losing party for the benefit of the party that obtains a gain from the cause. This excludes, in principle, the professional fees of the lawyers of each party.

8. APPEAL

8.1 Appellate Procedure

The appeal against judgments issued in civil and commercial matters takes place, by means of the notification of a summons within a period of one month from the notification of the judgment. The most diligent party is the one that notifies the judgment in this matter. Any party that does not agree with the sentence issued in the first degree has the right to appeal it. Preparatory judgments, such as those that order investigation measures, can only be appealed together with the judgment on the merits. Interlocutory judgments and final judgments on incidents can be appealed immediately are issued. The practice of the courts, of trying to accumulate all the incidents whose appeal must be decided together with the merits, could delay the process. The process to hear the appeal could take between six months and a year.

In the case of sentences handed down in criminal matters, the appeal is also open to all parties. Appeals must be made within 20 business days from their issuance. Normally, the Courts of Appeal take around eight months to hear the appeal of a criminal sentence. In this matter, by express provision of the law, the appeal of incidental judgments prior to the issuance of the decision on the merits should, at least in theory, should not interrupt the process.

8.2 Factual or Legal Review

The Dominican legal system has, as a rule, the double degree of jurisdiction. With few exceptions, the vast majority of cases are reviewed, always both in fact and in law and in the second instance, by a Court of Appeal. In Dominican law, there are no standards for the review of first degree sentences. Questions of fact and law can be presented for the first time on appeal and without any limitation. It is even possible to call third parties into intervention, on appeal, without having brought them into action in the first degree. In commercial matters, the procedure is, as in civil matters, written. The reading of the petitions or conclusions in a public hearing is a mere formality, since the parties must present a

written statement of the grounds of their case, in fact and in law.

9. CRIMINAL OFFENCES

9.1 Prosecution Process, Penalties and Defences

As previously mentioned, when a person who has obtained a secret of another – commercial or not – on the occasion of his trade or profession, discloses it, he is liable to a penalty of three to six months in prison. On the other hand, the individual who steals papers or correspondence of another to obtain the secrets, commercial or of any other nature, and divulges them is punished with a sentence of three months to one year in prison. Criminal proceedings in the Dominican Republic are initiated through the filing of a complaint or a complaint before the competent tax attorney, which is the place where the offence has been committed.

Obviously, these old provisions of the penal code are narrower in describing the conduct than those behaviours classified as acts of unfair competition by the industrial property law and the antitrust law. These provisions do not establish penalties of a criminal nature, but exclusively serve as a possible basis for a civil liability action for unfair competition.

When a criminal investigation is initiated, it is possible to request the District Attorney to carry out investigation procedures. Some of these may require prior judicial authorisation, but it is normally the prosecutor and not the offended party who can request these measures or proceedings, including raids, seizure of equipment and documents, and seizure of products made using the victim's trade secrets.

10. ALTERNATIVE DISPUTE RESOLUTION

10.1 Dispute Resolution Mechanisms

Dominican law provides mechanisms for alternative dispute resolution, including mediation, conciliation, and arbitration. Arbitration can be institutional before one of the conflict resolution centres (CRC) attached to one of the official Chambers of Commerce and Industry, or ad hoc, before arbitrators chosen by the parties, not attached to any CRCs. The most widely used option tends to be the convention that submits eventual disputes to institutional arbitration, in law or in equity, before an arbitration panel appointed to judge the regulations of the CRC in question.

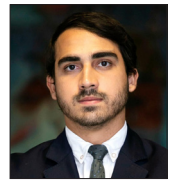
The advantages of an institutional arbitration are evident, since the law establishes that the awards issued by the arbitrators assigned to a CRC are enforceable without the need of a court's approval, in addition to the fact that the arbitration awards are not susceptible to being challenged through neither ordinary nor extraordinary resources. But, there is the unique possibility of attacking them in nullity, in a single instance, before the civil and commercial chamber of the competent Court of Appeal; the means of nullity provided by law being exhaustive and limited.

All institutional arbitrations are confidential by mandate of law. There are no particular rules in this jurisdiction for arbitrations on trade secrets. Arbitral tribunals may request judicial assistance, asking the judge to order – at their request – all provisional and investigative measures that they deem pertinent. In the firm's opinion, this constitutes a great advantage since this type of petition – where the tribunals come from an arbitration panel – does not receive the same treatment as those which come from the interested party.

Delgado Malagón – Veras Vargas is based in Santo Domingo and was founded in 1977. DMVV provides clients with a wide range of legal advice in a number of fields. The firm's team of nine lawyers regularly represents large privately owned banks and insurance providers, leading businesses in pharmaceutics, construction, hospitality and gambling, and private equity-holders. The firm's services include advice on corporate, real estate and tax affairs, as well as serving as a strategic counsel in civil and commercial litigation, constitutional reviews, arbitration, electoral, labour, and criminal proceedings. As well as serving Dominican companies in their IP needs, the firm has a long-lasting relationship with prominent European international firms specialised in IP, and whose multinational clients are referred to DMVV in order to handle all their IP needs and affairs in DR, including patent box regimes and tax planification.

AUTHORS

Edward Veras obtained his law degree in 1997. He proceeded to add several master's and postgraduate degrees to his professional training. For over 20 years he has taught business law and other subjects, at major universities, at undergraduate and graduate levels. He belongs to the Dominican Academy of Law and the Dominican Society of Business Law. His essays in specialised magazines on commercial law and commercial companies have been particularly valued by the legal community. He has achieved significant precedents in commercial law and intellectual property and is devoted to litigious practice in all matters.



Rodrigo Delgado obtained his law degree in 2016. With a master's degree in tax law, he also has extensive practice in corporate, intellectual property and tax affairs. He has been the face of the office in its correspondent relationships with major international law firms. From the registrations of trade marks and patents, consultancies and the elaboration of intellectual property licence contracts in general, his practice in this area of law has been steadily gaining relevance. He is a member of the Dominican Republic Bar Association. He has developed – and recently launched – a jurisprudence and doctrine consultation web platform that is popular with attorneys and judges.

Delgado Malagón – Veras Vargas

No. 54 of 27 de Febrero Av.
Galerías Comerciales building
Suite 412, El Vergel
Santo Domingo
Distrito Nacional
Dominican Republic
10107

Tel: 809 565 5356
Fax: 809 472 1600
Email: contact@dmvvlaw.com
Web: www.dmvvlaw.com

Trends and Developments

Contributed by:
Edward Veras and Rodrigo Delgado
***Delgado Malagón – Veras Vargas** see p.49*

Protection of Data as a Trade Secret: A Dominican Perspective

The digitisation of the economy at a global level – as a consequence of the development of communication networks, processing services and web technologies – has brought about a revolution in the creation of new companies, business models and business operations, and has forced traditional companies to adapt their production processes to this new economic, social and political context. This new ecosystem of companies, business models, production processes and regulations is called the digital economy, and it is here to stay.

Within the digital economy, data emerges as one of the main assets to be protected by natural and legal persons. The data within its technological meaning comprises both the personal data provided by the clients and users of the companies, as well as the information generated by said companies in their production processes. The latter includes patterns of behavior of customers and users, as well as the efficiency of companies in their internal processes. This information, which is collected, stored and exploited by entities that operate in the context of the digital economy, allows them to make intelligent decisions; commonly known as "data-based decisions". These decisions improve operations and, therefore, profitability.

In the Dominican Republic, the data that a natural or legal person collects, generates and stores can be considered a commercial secret as long as it complies with the requirements established in Law No 20-00 on Industrial Property: that said data, as a whole or in its configuration, has not been generally known by the public, nor easily accessible by those in the circles that normally handle the respective information and, furthermore, that the data has been the object of reasonable protection measures by its owner.

Regarding the requirement that the data has been the object of reasonable measures of protection by its owner, an interesting question arises: what is considered a reasonable measure of protection of a trade secret?

In the authors' opinion, the standard for evaluating whether or not the owner of the trade secret has taken reasonable measures to protect its secret varies, taking into consideration the situation of the potential infringer of his rights. For example, in the Dominican Republic, the standard for the worker, in relation to the technical, commercial, or manufacturing secrets of his employer, is lower since the law requires the worker not to disclose them during the employment contract nor after its termination. Regarding workers, the only other thing left to do then would be to determine whether or not the information constituted a technical, commercial or manufacturing secret. Because of this, it is convenient – but not essential – that workers write documents acknowledging their having come into contact with certain confidential information and its support, and reiterate the obligation not to disclose it in any way or copy it.

On the other hand, in cases of technology transfer (know-how) and licenses for the use of trade secrets, it is necessary to take contractual measures so that the recipients of the secret information keep it this way, and that all persons in their organizations that have access to this reserved

information are also obliged to maintain this reservation and not copy it.

In contractual practice, there is a tendency to confuse the instrument that supports the information protected by the trade secrets regime with the protected information itself. This occurs for strategic convenience so that the document that establishes the obligation of confidentiality regarding the commercial secret does not refer to the protected information, which would be kept secret from those who read the document. Given the aforementioned flexibility of the legislation, in principle, practically any commercial information – with respect to which the measure to keep confidential has been adopted – qualifies as a commercial secret in this jurisdiction.

Once the data protection requirements have been resolved by the holder, in accordance with the aforementioned scenarios and so that it can be considered as a trade secret, other interesting questions arise: What legal consequences are derived from the violation of a trade secret? What legal ways are open to take action against a natural or legal person who discloses or exploits a trade secret without the consent of its holder?

The unauthorised disclosure or exploitation of data as a trade secret constitutes an unfair practice in the Dominican Republic in accordance with the provisions of Law No 20-00 on Industrial Property and Law No 42-08 on the Defence of Competition.

In this sense, Law No 20-00 on Industrial Property establishes the following as an unfair commercial practice:

- exploitation without the authorisation of the legitimate owner of a trade secret, when access to said trade secret has resulted from a contractual or employment relationship;
- disclosure or communication of a trade secret without the authorisation of its legitimate owner, either for personal gain or that of a third party, or to harm the owner or owner of the trade secret; and
- acquisition of a trade secret by illegal or unfair means, as well as exploitation, communication or disclosure of said trade secret, for which purposes, the acquisition of a trade secret through industrial espionage, breach of a contract or an obligation, breach of trust, infidelity, or breach of a duty of loyalty is considered an unfair mean.

Unlike the sanctions established by Law No 20-00 on Industrial Property for violations related to patents, industrial designs and distinctive signs (trademarks, trade names, commercial slogans, etc) which carry important and well-defined criminal and financial sanctions, the Dominican legislator was lax in defining the sanctions related to unfair competitive practices, such as violations of trade secrets. In this sense, said law is limited to refer the natural or legal person considered harmed by an act of unfair competition to the civil and commercial courts, and – the only differentiating characteristic to the action in repair of damages of common law – extends the statute of limitations of the action in claim for damages from one to four years.

For its part, Law No 42-08 on the Defence of Competition considers as an unfair practice the appropriation, disclosure or exploitation without the authorisation of the owner of business and industrial secrets, constituting the data – as previously stated and under adequate protection by part of its owner – a trade secret.

Unlike what is enshrined in Law No 20-00 on Industrial Property in relation to the legal actions contemplated for unfair practices, Law No 42-08 on the Defence of Competition contemplates a series of legal actions that can be brought by the

owner of a trade secret when their legal rights are affected. Said actions must be filed before the civil and commercial court of first instance of the defendant's domicile, and are:

- declaratory action of the disloyalty of the act, where the judge may, as an accessory to said action, order the cessation of the unfair act if the disturbance created by it subsists; and
- action to repair the damages caused by the act, if fraud or fault of the economic agent (unauthorised disseminator or exploiter) has intervened.

Although it can be deduced from the above that the legislator wanted to contemplate a special regime of legal actions aimed at the protection of trade secrets and reparation of damages to its owner, specifically within the scope of competition law, the reality is that these legal actions are contemplated in the Civil Code and the Civil Procedural Code for any natural or legal person that is understood to be affected in their rights. The authors subsequently consider the inclusion of said regime of legal actions in Law No 42-08 to be superfluous. In this sense, the Dominican legal system provides for the possibility of accessing precautionary measures aimed at stopping illicit disturbances, such as situations that endanger a trade secret, which can be ordered by the referral judge.

Another interesting legal field for the protection of data as a trade secret is related to the labour field, say, the duty of protection of trade secrets that workers have to their employers. In this sense, in accordance with the Labour Code, it is established as a duty of every worker, vis-à-vis their employer: "To rigorously keep the technical, commercial or manufacturing secrets of the products to which they directly or indirectly produce, or of which have knowledge by reason of the work they perform, as well as the reserved administrative matters whose disclosure may cause damage to the employer, both while the employment contract lasts and after its termination".

This duty of reserve does not usually acknowledge a time limit, so it theoretically extends to the entire duration of the secret or the life of the worker or ex-worker. Violation of this obligation by the worker is also a cause for justified dismissal, that is, termination for just cause.

Additionally, and under some very specific scenarios, the possible ability of the possessor to initiate criminal actions against the natural person who discloses a trade secret without authorisation is possible. The Dominican penal code of 1884 makes it an offense, punishable by imprisonment from three months to a year, to seize papers or letters from a person to gain access to their secrets and disclose them. The same legislation sanctions – with imprisonment from one to six months – all persons who access the secrets of others by reason of their profession or trade (this applies to workers), and who disclose them to third parties (except in cases where the law obliges them to).

It is obvious, from the date this penal code was enacted and entered into force, that the purpose of this law was not to prevent or deter people from accessing a company's trade secrets to benefit from them. However, this legal regime of consequences will be useful every time the secret is revealed to third parties, although they are not applicable when the person stealing the secret uses the information for their personal gain without disclosing it to third parties.

As previously stated, both Law No 20-00 on Industrial Property and Law No 42-08 on the Defence of Competition qualify the fact of accessing commercial and trade secrets as an act of unfair competition, which gives place to the exercising of a civil liability action for acts

of unfair competition. Said rule, however, does not contain any special criminal offense on the matter.

The jurisprudential development in this country in relation to the protection of commercial and trade secrets has been scant and scarce. To date, there is no single precedent emanating from the Supreme Court of Justice that refers to the protection of trade secrets, unlike, for example, in the United States of North America and Europe, where there is a long tradition protection of this type of assets.

Although the Dominican legal regime created and established the protection of data as a trade secret, and its exploitation or disclosure as an act of unfair competition, it is inconsistent and flexible as the same is not the case when it comes to compilations of data or databases, which are considered as property that can be protected by copyright, in accordance with Law No 65-00 on Copyright, and entails a regime of special sanctions, protection and reparation.

In accordance with Law No 65-00, for a database to be protected by copyright it must constitute a creation of the intellect by virtue of the selection or arrangement of its content and it must be readable by machine or in any other way. In that sense, this copyright regime does not protect the data or materials themselves, but rather their selection and organisation on a specific compilation or basis – hence the ambiguity and ease of escaping its provisions when the asset disclosed or exploited without authorisation is the data itself and not the compilation of data or database that contains them. Additionally – and though not mandatory to benefit from the legal regime of said law – Law 65-00 orders the public registration of databases before the National Copyright Registry of the National Copyright Office, to give certainty to the protected property, which would cause precisely the opposite effect of what is intended with the protection of a trade secret which, as its name indicates, is of a confidential nature.

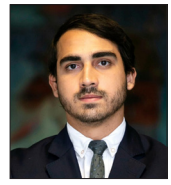
Due to such controversies and ambiguities, the authors prefer not to elaborate in this essay on the provisions of Law No 65-00 regarding the regime of consequences and legal actions established by said norm for intellectual property assets protected under its umbrella, including databases.

In conclusion, the authors are of the opinion that a protectionist trend of trade secrets should be developed in the Dominican Republic both legislatively and doctrinally – and, specifically, due to the preponderance of data – as an essential asset for all legal and natural persons in their production processes and business models within the digital economy. Regulations should be established to sanction, in a more burdensome way, the disclosure and exploitation of data without the consent of the owner, just as patents, distinctive signs and commercial designs are protected by Law No 20-00. Similarly, precautionary and provisional measures for embargoes and seizures must be established to protect the owner of the data, in a preventive manner, until a judicial decision intervenes.

Delgado Malagón – Veras Vargas is based in Santo Domingo and was founded in 1977. DMVV provides clients with a wide range of legal advice in a number of fields. The firm's team of nine lawyers regularly represents large privately owned banks and insurance providers, leading businesses in pharmaceutics, construction, hospitality and gambling, and private equity-holders. The firm's services include advice on corporate, real estate and tax affairs, as well as serving as a strategic counsel in civil and commercial litigation, constitutional reviews, arbitration, electoral, labour, and criminal proceedings. As well as serving Dominican companies in their IP needs, the firm has a long-lasting relationship with prominent European international firms specialised in IP, and whose multinational clients are referred to DMVV in order to handle all their IP needs and affairs in DR, including patent box regimes and tax planification.

AUTHORS

Edward Veras obtained his law degree in 1997. He proceeded to add several master's and postgraduate degrees to his professional training. For over 20 years he has taught business law and other subjects, at major universities, at undergraduate and graduate levels. He belongs to the Dominican Academy of Law and the Dominican Society of Business Law. His essays in specialised magazines on commercial law and commercial companies have been particularly valued by the legal community. He has achieved significant precedents in commercial law and intellectual property and is devoted to litigious practice in all matters.



Rodrigo Delgado obtained his law degree in 2016. With a master's degree in tax law, he also has extensive practice in corporate, intellectual property and tax affairs. He has been the face of the office in its correspondent relationships with major international law firms. From the registrations of trade marks and patents, consultancies and the elaboration of intellectual property licence contracts in general, his practice in this area of law has been steadily gaining relevance. He is a member of the Dominican Republic Bar Association. He has developed – and recently launched – a jurisprudence and doctrine consultation web platform that is popular with attorneys and judges.

Delgado Malagón – Veras Vargas

No. 54 of 27 de Febrero Av.
Galerías Comerciales building
Suite 412, El Vergel
Santo Domingo
Distrito Nacional
Dominican Republic
10107

Tel: 809 565 5356
Fax: 809 472 1600
Email: contact@dmvvlaw.com
Web: www.dmvvlaw.com

FINLAND

Law and Practice

Contributed by:
Jussi Talvitie and Sophie Zimmermann
Frontia Attorneys at Law see p.65

CONTENTS

1. LEGAL FRAMEWORK

1.1 Sources of Legal Protection for Trade Secrets

Prior to 2018, several bodies of law governed trade secret legislation in Finland. Various provisions providing comprehensive protection for trade secrets were included in laws such as the Criminal Code, the Unfair Business Practices Act, the Employment Contracts Act and several others.

Since the implementation of Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (hereinafter the Trade Secrets Directive) into national law in 2018, trade secret regulation was codified into one general act.

The definition of a trade secret was included in the Finnish Trade Secrets Act. References to trade secrets in other Finnish legal texts were similarly unified in accordance with the new act. Therefore, as of recently, the general source of civil regulation concerning trade secrets is the Finnish Trade Secrets Act while most offences concerning trade secrets remain criminalised in the Criminal Code.

1.2 What Is Protectable as a Trade Secret

The type of information protectable as a trade secret has not been limited as such, but information does have to fulfil certain requirements in order to be considered a trade secret. That is to say that information of any type or form may be protectable as long as it fulfils the three requirements established for a trade secret in the Trade Secrets Act; for more detail, see **1.4 Elements of Trade Secret Protection**.

1.3 Examples of Trade Secrets

Since there are no strict limitations to the type of information protectable as a trade secret, the examples that could be given are many and varied. Common examples of protectable trade secrets include information of a technical or financial nature. Concrete examples would constitute product development information, business methods, pricing and market information, economic predictions, competition analysis, client registers as well as administrative and organisational information about a company. Moreover, trade secrets could constitute parts of computer code or algorithms within software as well as food recipes.

Importantly, the Finnish legislator has specifically pointed out that, in addition to positive information, so-called negative information (for example, that a certain solution does not work for a particular product) may also constitute a trade secret.

1.4 Elements of Trade Secret Protection

Through the implementation of the Trade Secrets Directive, the criteria for a trade secret have been harmonised EU-wide. According to the derivative Trade Secrets Act, a trade secret has three requirements. Firstly, it must not be generally known or readily accessible to persons who normally deal with the type of information in question. Secondly, the secrecy of the information must have economic value for a business. Thirdly, the definition requires that the rightful owner of the trade secret has taken reasonable measures to ensure the protection of the information. Since the implementation of the Trade Secrets Act, references to trade secrets in other acts of Finnish legislation have been linked to this definition.

1.5 Reasonable Measures

Taking reasonable measures means that the rightful owner of the trade secret on the one

hand endeavours to keep the information secret, and on the other hand ensures that people handling trade secrets are aware of it. Whether the measures taken are reasonable enough must be assessed on a case-by-case basis. Such measures can again be many and varied depending on the nature of the protectable information and the protection methods available to the owner.

Reasonable measures taken can be as simple as maintaining physical barriers to secret information – for example, by storing confidential documents behind locked doors. In the electronic era, more common and widely used measures of protection include adequate security for IT systems through the use of passwords and firewalls as well as limited access to certain databases. In addition to any security measures taken, up-to-standard confidentiality agreements between companies, their employees and business partners constitute a vital form of protection.

Despite the fact that reasonable measures may include a wide variety of methods, some specific measures which have not fulfilled the criterion have also been identified in Finnish case law. Measures include physical signs conveying that an area contains confidential information or oral expressions alone about the secrecy of certain information have not been considered adequate enough to be considered reasonable measures.

1.6 Disclosure to Employees

In general, successful business practice often requires certain trade secrets to be shared with a considerable amount of a company's employees. However, the fact that trade secrets must at times be disclosed to employees does not translate to them losing their protection.

In Finland, the protection of information disclosed to employees is regulated in the Trade Secrets Act, the Employment Contracts Act and the Criminal Code. According to the Trade Secrets Act, an employer's trade secrets may not be unlawfully disclosed or used for the employee's own benefit during the duration of the employment. Moreover, the Finnish Employment Contracts Act identically dictates that an employee may not unlawfully disclose an employer's trade secrets or use them for their own benefit.

Further, the offences concerning trade secrets in the Criminal Code are similarly applicable to an employee as to anyone else. Therefore, the availability for protection per se is not limited when disclosing secret information to employees, it simply means that the circle to which secret information is trusted to has grown, which in turn means that more focus must be put on protective measures.

Despite the fact that trade secrets are protected in relation to employees similarly as to anyone else, there are some specific limitations to the length of the protection. Both the Trade Secrets Act and the Employment Contracts Act only limit the employee's right to disclosure and use of the trade secrets to the duration of the employment. The Criminal Code, on the other hand, limits use and disclosure up to two years after employment has ended. This is only relevant in connection to trade secret violations. Misappropriation and industrial espionage offences, which can also be committed by an employee, have no similar time limitations. In order to extend the length of protection, relevant confidentiality agreements must therefore be in place between the employer and employee to prevent the leakage of secret information by former employees.

Another form of protection used in an employment relationship that is particular to the Finnish Trade Secrets Act is the so-called "technical instruction". The provision prohibiting the unlawful use or disclosure of a technical instruction is derived from the prior Unfair Business Practices

Act and was therefore included in national trade secret legislation.

According to the act, it is prohibited to disclose or use a technical instruction in order to gain financial benefit for oneself or another, or in order to harm another. A technical instruction does not need to fulfil the requirements of a trade secret to be granted protection and the protection thereof is based on the fact that it constitutes information which has been disclosed to an employee or business partner in confidence. Thus, the requirements for a piece of information to constitute a technical instruction are less rigid than those of a trade secret and moreover the protection of a technical instruction has no statutory time limit.

1.7 Independent Discovery

The Finnish Trade Secrets Act confirms that gaining information through independent discovery or reverse engineering does not constitute trade secret misappropriation. According to the Trade Secrets Act, the acquisition of a trade secret is lawful when it occurs through discovering a trade secret through the observation, study or testing of a product or an object which has been made available to the public, or that is lawfully in the possession of someone who has no duty to limit the acquisition of the trade secret.

Thus, the principle is that lawful independent discovery should be fairly easy and not require an unreasonable amount of time or effort to conclude. In case law, the Supreme Court of Finland has, for example, found that what can be visually detected from a publicly available product cannot constitute a trade secret to begin with. Products which are available to the public cannot constitute a trade secret for the part that human sensory-based detections can be made from them. These same products may, however, include trade secrets which cannot be visually detected. For example, tolerance levels of products constitute product information which cannot be visually detected. On the other hand, case law has also confirmed that the drawings and sketches of specific machinery may include trade secrets even if the principle and the outlines of its mechanics are generally known information.

1.8 Computer Software and Technology

There are no specific provisions concerning protection of computer software or other technology as trade secrets. In general, computer software is protected by the Finnish Copyright Act. Despite copyright being the accepted primary protection method of software, it has been considered insufficient at times.

Whereas copyright protects the exact form in which code is presented, the idea behind it is left unprotected. Therefore methods, principles and other relevant information concerning software would, upon fulfilling the necessary requirements, have to be protected as trade secrets in lack of any other form of protection. What must be considered is that reverse engineering of information is allowed. This also affects the protection of computer software and source code as trade secrets in particular. Moreover, information concerning software and technology may be protectable as technical information as described in **1.6 Disclosure to Employees**.

1.9 Duration of Protection for Trade Secrets

There is no definite statutory timeline for the duration of trade secret protection in Finnish legislation and, therefore, a trade secret has protection for as long as it fulfils the requirements set out for it. As time passes, if information which has previously been considered a trade secret becomes public information or otherwise loses its economic value, it simultaneously loses its legal protection. That is to say that the value of any such information considered a trade secret

at one point in time may and most likely will also dilute when time passes. This is especially relevant for fast-paced technical developments or financial figures from previous years.

Conversely, some information may fulfil the requirements of a trade secret indefinitely. A common example of such information is iconic recipes. Although there is no limit to the duration of protection, the relevant statutes of limitations described in more detail in **5.2 Limitations Period** pose restrictions on the timeframe during which lawsuits can be raised against misappropriation.

1.10 Licensing

Licensing a trade secret does not differ from licensing any other intellectual property right as such. Licensing agreements can therefore be freely concluded under the consideration of the trade secret owner. However, when information being licensed is solely protected as a trade secret, as opposed to any other IP right, relevant confidentiality agreements must be in place in order to ensure an adequate level of protection.

1.11 What Differentiates Trade Secrets from Other IP Rights

Unlike other IP rights, trade secrets do not create an exclusive right to use protected information. The same trade secret may therefore be independently known to many parties at the same time while still enjoying legal protection. Unlike most other intellectual property rights, there are also no conditions to what a trade secret protection may protect in terms of its shape, form or other technical, aesthetic or formal elements. As previously noted, there is also no set timeline to how long a trade secret is protected. While many other IP rights may be registered or even require registration for validity, trade secrets cannot be registered as their protection is based solely on the fact that they are kept secret.

1.12 Overlapping IP Rights

The concept of "double protection" exists in connection to IP rights. In essence, double protection means that, for example, something enjoying a copyright may also well be protected as a trade secret. Although double protection is possible, these overlapping rights constitute separate methods of protection and are regarded individually.

1.13 Other Legal Theories

In cases where bringing claims for trade secret misappropriation, violation or suchlike is not possible on the basis of the Trade Secrets Act or the trade secret offences enshrined in the Criminal Code, other legal theories may still be available. Offences relating to trade secrets may amount to the misuse of a position of trust which has been criminalised in the Criminal Code or even to a secrecy offence, at least indirectly. Additionally, any violation of an employee's loyalty towards their employer may be taken into consideration when assessing the rights to termination of employment.

1.14 Criminal Liability

Please see **1.13 Other Legal Theories**.

1.15 Extraterritoriality

The Criminal Code identifies three types of trade secret offences: industrial espionage, the misappropriation of a trade secret and the violation of a trade secret.

In the Criminal Code, the offence of misappropriation is defined as unlawfully using a trade secret which has been acquired or disclosed through an act punishable in the Criminal Code or disclosing a trade secret in order to obtain financial benefit. The closely related offence of trade secret violation is defined in the Criminal Code as unlawfully disclosing or utilising a trade secret which has been learned while in the service of another or in any other trusted position,

to obtain financial benefit or to harm another; see also **2.4 Industrial Espionage**. An attempt to violate trade secrets in any of the above ways is likewise punishable.

Both civil and criminal claims may in principle be pursued. Civil claims concerning a trade secret offence may be pursued either together with the criminal claims in criminal proceedings, or alternatively in separate civil proceedings. It should, however, be taken into account that only trade secret lawsuits against companies can be pursued before the Market Court. In the case that the offender is an individual, a trade secret law suit is always tried before a district court.

The possible penalties for a trade secret offence vary from a fine to up to two years of imprisonment.

2. MISAPPROPRIATION OF TRADE SECRETS

2.1 The Definition of Misappropriation

Following the Trade Secrets Directive, the Trade Secrets Act recognises misappropriation in three main categories: unlawful acquisition, use and disclosure.

Unlawful acquisition constitutes stealing and unauthorised copying, tracing, observation or other handling of documents, objects, materials, substances or electronic files which contain a trade secret or from which a trade secret can be derived, as well as any other method of acquisition going against good business practices. Accordingly, a trade secret may not be used or disclosed by someone who has unlawfully acquired it. Moreover, a trade secret may not be used or disclosed when it has been obtained through working in different roles in a company such as part of the management, reorganisation proceedings or other trusted positions.

The Criminal Code identifies three types of trade secret offences: corporate espionage, the misappropriation of a trade secret and the violation of a trade secret. In the Criminal Code, the offence of misappropriation is defined as unlawfully using a trade secret which has been acquired or disclosed through an act punishable in the Criminal Code or disclosing a trade secret in order to obtain financial benefit. The closely related offence of trade secret violation is defined in the Criminal Code as unlawfully disclosing or utilising a trade secret which has been learned while in the service of another or in any other trusted position, to obtain financial benefit or to harm another. An attempt to violate trade secrets is likewise punishable.

2.2 Employee Relationships

As described in **1.6 Disclosure to Employees**, the Trade Secrets Act, Employment Contract Act and Criminal Code all protect trade secrets from misappropriation or violation by an employee. In principle, the elements of the claim do not differ in substance but, as previously noted, the window of time during which a claim may be brought against an employee or former employee in trade secret violations is narrower and must be supplemented with adequate confidentiality agreements.

2.3 Joint Ventures

Finnish legislation does not recognise the existence of any obligations between joint ventures with respect to trade secrets. Such obligations are thus dependent on individual contracts laid out between the parties.

2.4 Industrial Espionage

Industrial espionage is one of the three trade secret offences criminalised in the Criminal Code. According to the code, a person who unlawfully obtains information regarding the business secret of another by entering an area closed to unauthorised persons or access-

ing an information system protected against unauthorised persons, by gaining possession of or copying a document or other record, or in another comparable manner, or by using a special technical device with the intention of unlawfully revealing this secret or unjustifiably utilising it shall, unless a more severe penalty has been provided elsewhere in law for the act, be sentenced for business espionage to a fine or to imprisonment for two years.

The attempt of industrial espionage is likewise punishable. That is to say that industrial espionage covers a wide variety of situations and being convicted of industrial espionage may result in severe consequences. Additionally, the processing of trade secret cases under the criminal offence of industrial espionage does not mean that civil remedies such as damages could not be simultaneously sought out by the owner of the trade secret.

3. PREVENTING TRADE SECRET MISAPPROPRIATION

3.1 Best Practices for Safeguarding Trade Secrets

Recognised and commonly used ways to ensure the safeguarding of trade secrets beyond what has been provided by legislation again are varied. The most important practices include having separate confidentiality and non-disclosure agreements, confidentiality clauses in employment contracts and possible non-compete clauses in place when disclosing trade secrets to employees, business partners or others.

Similarly, a business partner should be required to ensure trade secret confidentiality with their own employees and business partners through appropriate confidentiality agreements. It is also prevalent to ensure that the disclosure of certain trade secrets to employees or business partners only happens on a need-to-know basis.

Other day-to-day practices to ensure the protection include ensuring both physical and electronic restrictions to secret information. It is also important to identify risks of leaks and secure them with adequate measures.

Additionally, and very importantly, anyone who may receive secret material or information must be made fully aware of its secrecy as well as their obligations towards trade secrets. In many situations, a company's own employees pose the greatest risk of leakage, which is why adequate training and instructions on the lawful handling, as well as of the consequences of mishandling, trade secrets must be present at a workplace.

An employee must be made aware of how they can best ensure that they are acting lawfully in their daily practice – for example, by advising on how to handle information when teleworking. Important practices concerning employees leaving and joining the company are described in more detail in **3.2 Exit Interviews** and **4.2 New Employees**.

3.2 Exit Interviews

There are no legal obligations within Finnish legislation concerning written or other assurances with respect to confidentiality, secrecy and/or trade secrets when employment comes to an end. However, during an exit interview, it is a diligent employer's responsibility to have their exiting employees understand their obligations toward their now former employee and remind them of their confidentiality agreements and legal obligations. It may also be necessary to remind employees of the information that they have handled which constitutes trade secrets or examples thereof. Importantly the former employee must also be asked to return all mate-

rial and or access keys, etc, to information containing trade secrets.

4. SAFEGUARDING AGAINST ALLEGATIONS OF TRADE SECRET MISAPPROPRIATION

4.1 Pre-existing Skills and Expertise

In principle, general professional knowledge, skills, expertise or experience do not constitute trade secrets as such. Moreover, the fact that an employee is personally skilled or talented cannot be protected by an employer as a trade secret. The Trade Secrets Act specifically provides that information which is either general knowledge or easily discoverable to a person used to handling such information does not fulfil the secrecy requirement of the Trade Secrets Act. Therefore, knowledge gained through education or conventional skills and experience that may be gained by anyone in the profession clearly do not constitute trade secrets. What is more, the use of a person's professional knowledge and expertise in their future work can only be limited so far.

In practice, however, drawing a line between pre-existing skills or expertise and trade secrets may pose a challenge. For example, a person who has worked in a highly technical project for the same company for a long period of time may possess skills and expertise through their work that also constitute information protectable as their employer's trade secrets. Another example would be the case that knowledge has been gained through training offered by an employer. Even if the substance of the training itself may constitute general information, the training material itself is the property of the employer.

Legislation does not offer a clear-cut answer as to when skills and expertise cross a certain line and become trade secrets. This question must therefore be assessed on a case-by-case basis. In the government proposal for the Trade Secrets Act, the Finnish legislator provided some guidelines for conducting this assessment. The legislator suggested that information that is written or recorded instead of being memory-based, which is detailed rather than general, and which is in the possession of only very few companies could constitute a trade secret rather than professional skills or expertise. While the legislator's guidelines offer a framework for reference when considering the relationship of pre-existing skills and expertise with that of trade secrets, they are not airtight. For example, a previous employee may well have memory-based knowledge of information which still constitutes a trade secret.

4.2 New Employees

Generally, any new employees would have already been informed of their confidentiality obligations and have signed relevant non-disclosure agreements with their previous employer prior to taking on a new position at a competitor. However, especially when hiring an employee from a competitor to a higher position requiring special skills or expertise, the above-mentioned assessment between such skills and experience and trade secrets becomes highlighted and a new employee should be made aware of this.

Furthermore, a new employee should not bring with them documents, files or other material containing a previous employer's trade secrets to their new place of work. In any case it is good practice to remind new employees that, equivalent to their obligations concerning your trade secrets, their obligations also extend to their previous employer's trade secrets.

5. TRADE SECRET LITIGATION

5.1 Prerequisites to Filing a Lawsuit

The procedure for initiating a civil lawsuit concerning misappropriation of trade secrets is the same as any other civil procedure in Finland, with the exception that a trade secret lawsuit may be also brought in the Market Court instead of a District Court. However, there are no prerequisites or preliminary steps to filing a civil lawsuit in either a district court or the Market Court.

5.2 Limitations Period

Filing a civil claim concerning trade secret misappropriation under the Finnish Trade Secrets Act must be done within five years from when the rightful owner of the trade secret became informed of the misappropriation. Notwithstanding, a claim can only be brought a maximum of ten years from when the misappropriation took place. Initiating a criminal process under the Criminal Code must take place within five years of the criminal act.

5.3 Initiating a Lawsuit

Initiating a lawsuit concerning trade secret misappropriation follows the normal procedural steps of a civil process when claims are brought under the Trade Secrets Act. In accordance with the Finnish Code of Judicial Procedure, a civil process is initiated with a written application for a summons which is to be delivered to the relevant District Court or, in the case of certain trade secret lawsuits, the Market Court, which in turn will deliver a summons to the defendant.

Similarly, initiating a criminal process follows the normal procedural steps when offences are reported under the Criminal Code. A criminal process is initiated by making a report of an offence to the police in order for the police to start a pre-trial investigation. After the pre-trial investigation has been concluded, the matter is delivered to a prosecutor for a consideration of charges.

5.4 Jurisdiction of the Courts

A trade secret misappropriation claim can be filed in two different venues. Civil procedures against natural persons as well as criminal procedures are tried in district courts as general courts of first instance. Civil procedures against undertakings or natural persons pursuing business activities in turn may also be tried in the Market Court, as a court with special expertise on the matter.

5.5 Initial Pleading Standards

There is no legal obstacle to raising a claim concerning trade secret misappropriation in a civil procedure without concrete evidence. However, it must be noted that successful litigation concerning trade secret misappropriation usually requires a considerable amount of proof, and therefore raising a claim before having concrete evidence is likely to result in losing the case and having to reimburse your counterparty's legal costs.

As for reporting a criminal offence, the likelihood of the pre-trial investigation resulting in the prosecutor raising charges is lowered when there seems to be no evidence on the matter. In a criminal procedure there is also the possibility of being charged for false denunciation in the event that accusations have no grounds. Although this is highly unlikely, it highlights that reports on criminal offences should not be made without good reason.

Where there is knowledge of misappropriation, but concrete evidence is not at hand or available, collecting the necessary proof for a successful claim may pose difficulties or require further efforts. Documents that are not accessible may be required to be included in evidence by, for example, the opposing party but, even then,

these documents have to be identified. Therefore, and due to the fact that the police have extensive powers to conduct a pre-trial investigation, it may be worthwhile to bring a case of trade secret misappropriation as a criminal process instead of a civil process when concrete evidence cannot be accessed or identified by the owner of the trade secret.

5.6 Seizure Mechanisms

According to the Trade Secret Act, seizure of certain products is possible in connection to a temporary injunction under the Trade Secret Act. Thus, the seizure of products may be ordered when the requirements for a temporary injunction are fulfilled and concern the ban to sell, produce or circulate goods that infringe upon trade secret rights. These products may be temporarily seized until a final judgment on the matter has been given.

5.7 Obtaining Information and Evidence

In a criminal process the police carrying out the pre-trial investigation has a much larger right to obtain information and evidence from the parties than the plaintiff does in a civil process. The police may obtain information and evidence through home searches, seizures and other highly effective measures. In civil procedures, the information obtained must be based on what evidence the parties themselves have gathered from sources that are available to them. In principle, it is up to the party to gather their own evidence whereas their attorney then mirrors this evidence against relevant legal sources. It is possible for a party to also request during trial that a piece of information which is in the possession of the other party or a third party be presented as evidence during the trial.

5.8 Maintaining Secrecy While Litigating

In Finland, trade secrets in relation to the public and third parties during trial are protected by the Act on the Publicity of Court Proceedings in General Courts. The act enables limiting the public's access to written material, oral proceedings and the final decision of the court in order to protect trade secrets. That is to say that trade secrets enjoy protection even during the trial process. The Trade Secret Act in turn goes a step further and even regulates publicity in relation to the other parties. In principle, and in accordance with the Act on the Publicity of Court Proceedings in General Courts, another party's right to take part in hearings or to have access to the full decision cannot be limited on the grounds of trade secret protection. The Trade Secret Act, however, provides the possibility to minimise the circle of people to whom trade secrets are disclosed to during the trial process.

5.9 Defending against Allegations of Misappropriation

There are two main lines of defences against allegations of misappropriation. The first of them constitutes demonstrating that the information in question does not meet all the requirements of a trade secret and thus does not constitute a trade secret as defined in the Trade Secret Act. If the information is general or easily accessible, has no economic value due to its secrecy or if its lawful owner has not taken the necessary steps to protect it, it is not a trade secret and cannot be misappropriated. The second line of defence is demonstrating that the handling of the trade secret does not constitute misappropriation – ie, that unlawful acquiring, use or disclosure of the trade secret has not taken place as required in legislation or that unlawful acquiring, use or disclosure has not been intentional.

5.10 Dispositive Motions

A court may dismiss a case without consideration on certain formal or procedural grounds. Generally, the court determines its lack of jurisdiction and other formal or procedural grounds for dismissal ex officio. However, a claimant may bring dispositive motions concerning the lack of

so-called dispositive procedural requirements such as the lack of territorial jurisdiction or that the matter should be resolved by an arbitrator rather than a court.

5.11 Cost of Litigation

The cost of litigation, especially in a civil lawsuit, may accrue up to a sizeable amount. This is mainly due to the fact that a trade secret lawsuit demands a considerable amount of presentable proof, the collecting and processing of which in turn requires a lot of time and effort.

In criminal proceedings, on the other hand, the police will handle most of the investigation and collection of evidence and costs thereof. However, due to the nature of trade secret offences and the fact that their investigation requires a great amount of special information about the nature of the business which is not accessible to the police, the criminal process also requires a lot of co-operation between the police, the plaintiff and their attorney.

6. TRIAL

6.1 Bench or Jury Trial

Trials by jury do not exist in Finland as all cases are handled and decided in a bench trial. Only in very exceptional and severe criminal cases can the popular sense of justice be represented by so-called "lay judges" who take part in the decision-making process of the court.

6.2 Trial Process

There are three different trial processes that may be followed in a trade secret case. Firstly, there is a choice of trying the case as a civil process under the Trade Secrets Act or a criminal process under the Criminal Code. If the case is tried as a criminal process, it will be handled through an ordinary criminal process in the District Court. Upon trial through a civil process, depending on the defendant (natural person or an undertaking) the case will be tried through an ordinary civil process in a district court or in the Market Court.

Each of these trial processes entail unique characteristics but, in principle, follow the same pattern. After the process has been initiated, a trial process begins with written, and in some cases oral preparation, and follows with a main hearing during which witness testimony is heard, oral arguments are made, and evidence is examined. The process ends with closing statements by both parties. The length of a trial always depends on the complexity of the matter and the amount of witnesses to be heard, the amount of evidence to be examined, etc.

6.3 Use of Expert Witnesses

The use of expert witnesses during a civil trial in a district court has been specifically regulated in the Trade Secrets Act. According to the Act, a district court may use a maximum of two experts in a trial concerning misappropriation, during which the court poses questions to the experts who produce written statements to these questions. These statements may be commented by both parties.

In addition to the provision concerning experts in the Trade Secrets Act, the general regulation concerning the use of experts during trial can be found in the Code of Judicial Procedure. According to the Code, both the court and the parties may freely name any number of experts for statements. The use of an expert is separate from that of a witness per se. Experts, unlike witnesses, are asked to produce insight on an area of their expertise. Therefore, their testimony is legally separate from witness testimony, although in practice the distinction might not be clear.

Unlike the case for the district courts, the use of expert witnesses in market court proceedings

is not regulated in the Trade Secrets Act but instead in the more open-ended Market Court Act, according to which the Market Court may use expert witnesses if the nature of the case requires it. The parties may additionally name experts for statements or as witnesses as is the case in any other trial.

7. REMEDIES

7.1 Preliminary Injunctive Relief

Derived from Article 10 of the Trade Secrets Directive, the Trade Secrets Act also specifically provides for a possibility to seek a temporary injunction until a final decision on the case has been made by the court. The possibility of obtaining such relief has already been enshrined into the Finnish Code of Judicial Procedure, but the prerequisites to imposing such a relief are different between the two acts.

According to the Trade Secrets Act, a court may temporarily ban the continuation of the use or disclosure or other infringement of a trade secret holders rights by a person who has unlawfully acquired, used or disclosed the trade secret. This ban can be demanded and granted if the plaintiff shows that it is likely that a trade secret exists, that they are the rightful owner of the trade secret and that their right is or imminently will be infringed.

7.2 Measures of Damages

The Trade Secrets Act provides a new and harmonised approach for civil remedies for trade secret misappropriation. Instead of corrective measures, the court may order the defendant to pay compensation and damages to the plaintiff. According to the Trade Secrets Act, damages must be paid to the rightful owner of the trade secret by a person who intentionally or negligently acquires or discloses a trade secret. Compensation, in turn, must be paid if a person, intentionally or negligently, unlawfully uses a trade secret as described in the Trade Secrets Act. Despite the existence of a separate Tort Liability Act as the main act concerning damages, the Trade Secrets Act includes a new separate damages provision which implements Article 14 of the Trade Secrets Directive.

As for punitive damages, they are not recognised in Finnish legislation and therefore only what has been lost can be payable as damages.

7.3 Permanent Injunction

In accordance with the Trade Secrets Directive, the Finnish Trade Secrets Act allows for a court to impose permanent injunctions in addition to corrective measures on the infringer. According to the act, a court may order an injunction to prohibit the infringer from beginning, continuing or repeating misappropriation. However, the injunction may not be disproportionate to the circumstances at hand or unnecessarily limit the actions of the defendant.

7.4 Attorneys' Fees

A plaintiff may recover their attorney's fees in a civil litigation as part of their recoverable costs. In principle, it is up to the unsuccessful party to compensate the successful party's trial costs which include attorneys' fees. Despite this being the general rule, a court will not order costs to be recovered from the unsuccessful party ex officio. Therefore, a party must specifically claim the costs from the opposing party. The court will then examine the claimed costs and order reasonable costs as recoverable from the other party.

7.5 Costs

Other costs that may be recovered from the unsuccessful party include, for example, reimbursements for expert statements, witness fees, travel and living expenses during the proceed-

ings (public transport, hotel visits) as well as the loss of any earnings due to the time spent in trial. Again, these costs must be specifically claimed by the party.

8. APPEAL

8.1 Appellate Procedure

Appealing a decision in a trade secret case follows the ordinary appellate procedure in place in Finland. Thus, both parties have the right to appeal an unsatisfactory decision made by the court. The appealing process differs depending on whether the claim was brought in a district court for either a civil or criminal process or the Market Court for a civil process.

Appealing a decision of the District Court to the appellate court must be done within 30 days of receiving the decision. Appealing the decision of an appellate court can be done by application to the Supreme Court for leave to appeal within 60 days of the decision of the appellate court. If the Supreme Court does not grant leave to appeal, the decision made by the appellate court will remain final. An appeal concerning a decision of the Market Court on the other hand, is made directly to the Supreme Court, which again must grant leave to appeal for the appellate procedure to be successful.

8.2 Factual or Legal Review

The appellate courts and the Supreme Court in Finland review both factual and legal issues. The case is retried from the beginning orally by the appellate court; in certain cases, an oral retrial is possible even by the Supreme Court. However, this occurs rarely. Additionally, in criminal procedures new evidence and facts of the case may be presented in appellate courts as well as the Supreme Court. In civil procedures new evidence might be considered during appeals procedures if the party can show that the information was not available at the trial of first instance. As described above in **8.1 Appellate Procedure**, a party must appeal a decision of a court within a set timeframe.

9. CRIMINAL OFFENCES

9.1 Prosecution Process, Penalties and Defences

The Criminal Code recognises offences under the titles of corporate espionage, trade secret violation and trade secret misappropriation. The process for initiating a criminal prosecution for any of these trade secret offences follows that of any other criminal proceeding in that the first line of duty is to file a criminal report of an offence to the police.

The potential penalties for all three offences are fines or imprisonment for a term not exceeding two years. Trade secret offences also entail an undertaking's criminal liability – ie, if the offence was committed within an undertaking, this undertaking may be fined between EUR850 and EUR850,000. Similar to defences in civil law cases concerning trade secrets, the defences in a criminal case would also constitute proving either that (i) the information at hand does not constitute a trade secret or (ii) that it has not been misappropriated or that such misappropriation lacked intention.

There are no separate mechanisms for trade secret owners to co-ordinate with law enforcement authorities in investigation trade secret offences. As with any criminal case, the target of the offence is interviewed by the law enforcement authorities as part of their investigations. The law enforcement authorities may also be provided with necessary material for the investigation of the case.

10. ALTERNATIVE DISPUTE RESOLUTION

10.1 Dispute Resolution Mechanisms

As with any dispositive matter, trade secret matters may be resolved through alternative dispute resolution when this is agreed upon between parties. The most commonly used alternative dispute resolution is arbitration. However, a number of other mechanisms such as legal advisory services, mediation and other panels also exist in Finland and they may be freely used as agreed on between parties.

Frontia Attorneys at Law is a Finnish law firm providing services in dispute resolution, competition law and public procurement. The team consists of 14 lawyers who provide first-class advocacy, responsibly and effectively, with over 100 years of combined experience from the biggest law firms in Finland. Frontia only takes on assignments in which it has leading expertise: this includes handling demanding commercial disputes, representing companies in criminal and administrative proceedings, handling matters in any and all competition law disciplines – both domestically and internationally – as well as matters of public procurement. The firm considers success to mean that both its clients and team are satisfied; its philosophy is that this will follow from positive customer experiences that stem from Frontia's uncompromised focus on the client's interest, the well-being of its staff and the way it works.

AUTHORS

Jussi Talvitie is a senior attorney at Frontia. He has 15 years of experience in white-collar crime and criminal proceedings as well as litigating and arbitrating commercial and employment-related disputes. Mr Talvitie advises clients in matters relating to corporate criminal liability and white-collar crime. He specialises in anti-corruption and bribery (in both public and private sectors) and trade secret issues which typically involve extensive pre-trial investigations and complex proceedings. Mr Talvitie has acted as counsel in one of the largest and most complex bribery cases ever litigated in Finland, a case related to the defence industry and alleged bribery in several jurisdictions. He has also acted as counsel for a Fortune 500 company in a major trade secret litigation. Mr Talvitie has been counsel to domestic and international clients in a number of large and demanding business disputes, including matters concerning management and shareholder disputes and employment law as well as exclusive distribution rights.

Sophie Zimmermann works as an associate at Frontia. She assists in a variety of matters related to dispute resolution, competition and public procurement. Prior to starting her career at Frontia, Ms Zimmermann gained experience through various traineeships in corporate law firms as well as an international organisation. Ms Zimmermann has assisted in a variety of competition matters as well as in representing clients before the Market Court; she currently works as part of several teams in large and complex dispute matters both domestically and internationally.

Frontia Attorneys at Law

Unioninkatu 30
00100 Helsinki
Finland

Tel: +358 40 5109 409
Email: frontia@frontia.fi
Web: www.frontia.fi

GERMANY

Law and Practice

Contributed by:
Thomas Nägele, Simon Apel, Jonathan Drescher and Alexander Stolz
SZA Schilling, Zutt & Anschütz see p.85

CONTENTS

Contributed by: *Thomas Nägele, Simon Apel, Jonathan Drescher and Alexander Stolz,*
SZA Schilling, Zutt & Anschütz

1. LEGAL FRAMEWORK

1.1 Sources of Legal Protection for Trade Secrets

Since April 2019, legal protection of trade secrets in Germany has mainly been governed by the German Trade Secret Act (TSA) (*Gesetz zum Schutz von Geschäftsgeheimnissen*, or *GeschGehG*). The TSA implements the requirements of the Directive on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure ((EU) 2016/943) (the European Trade Secret Directive, or ETSD).

Amongst other things, the TSA regulates the requirements that information must meet in order to be protected as a trade secret (Section 2), the scope of such protection (Section 3 et seqq) and the legal consequences of an infringement (Section 6 et seqq). Furthermore, it establishes specific rules to protect trade secrets in (civil law) litigation (Section 15 et seqq) and stipulates certain conduct regarding trade secrets as a criminal offence (Section 23).

Even if the TSA is the main act with regard to trade secrets, it should be noted that there are several provisions throughout different acts of German law that may provide flanking protection. Such provisions are mainly designed as special liability provisions for particularly qualified professional groups (such as members of the works council, board members and managing directors, lawyers, notaries or civil servants) that prohibit the disclosure and exploitation of trade secrets.

In addition, depending on the individual case, provisions that serve mainly other purposes – such as the security of the Federal Republic of Germany (Section 93 et seqq of the German Criminal Code (GCC) (*Strafgesetzbuch*, or StGB)), the integrity of electronic data (Section 202a et seqq, GCC) or postal and telecommunications secrecy (Section 206, GCC), to give just some examples – may also provide auxiliary protection for trade secrets.

1.2 What Is Protectable as a Trade Secret

In principle, any information that relates in any way to a business and has any kind of commercial value can be protected as a trade secret under the TSA. Inter alia, this applies to:

- commercial information (eg, lists of customers);
- technical know-how (eg, unpatented inventions, recipes);
- so-called negative information, meaning knowledge about adverse circumstances (such as production problems or an imminent insolvency); and
- cases where the fact itself (eg, a particular process) is not secret, but the fact that the company in question uses the process and wants to prevent competitors from using it by keeping it secret.

In summary, only information that is purely private and cannot be used in business transactions is excluded from protection under the TSA. With regard to information about illegal activities in a company (eg, tax evasion, violation of labour law or antitrust regulations), it is disputed whether such information can also be protected under the TSA. However, even if such information should be covered by the scope of the TSA's protection (which is convincing), its disclosure will in some cases be permitted by an overriding public interest.

1.3 Examples of Trade Secrets

While neither the TSA nor the underlying ETSD provides for specific examples to illustrate the types of information that are protectable, under German law before the enactment of the TSA,

the Federal Court of Justice (FCJ) (*Bundesgerichtshof*, or BGH) has affirmed all kinds of secret information as trade secrets; eg, customer and supplier lists, cost information, business strategies, company data or market analyses, manufacturing processes, design drawings, prototypes, formulas and recipes, production equipment and tools, templates and computer programs. As outlined in **1.2 What Is Protectable as a Trade Secret**, any of these examples could generally be protected under the TSA as well.

1.4 Elements of Trade Secret Protection

Pursuant to Section 2 No 1 of the TSA, any type of information can be protected as a trade secret as long as it meets the following requirements:

- it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question and has commercial value because it is secret;
- it has been subject to reasonable measures of protection against disclosure considering the respective circumstances, by the person lawfully in control of the information; and
- there is a legitimate interest in confidentiality.

Whereas the German legislator took the first two conditions directly from the ETSD, the requirement of a "legitimate interest in secrecy" was inserted autonomously. The practical relevance of this additional requirement, however, is doubtful. Since Article 1 (1) of the ETSD lays down a minimum standard for the protection of trade secrets, which the member states may extend but not restrict, it can be assumed that information, even if it does not fulfil the condition of the third point, is nevertheless to be regarded as a trade secret in accordance with the superior ETSD.

1.5 Reasonable Measures

Pursuant to Section 2 No 1 litera b) of the TSA, the trade secret owner is obligated to take reasonable measures of protection considering the specific circumstances to keep the information secret and, in the event of a dispute, has to prove that the measures taken were sufficient. As the requirement of appropriate confidentiality measures was only recently introduced by the TSA, coming into effect in 2019, there is little case law yet regarding this matter, and neither the TSA nor the ETSD stipulates any specific requirements as to what specific types of secrecy measures must be taken.

However, it is common sense that the trade secret owner must "only" ensure appropriate (and not the best possible or maximum effective) safeguards. Apart from that, the measures to be taken cannot be determined in the abstract, but will depend on the specific nature and value of the trade secret as a whole and for the company, the size of the company, the costs and the standard of the measures. In general, five types of measures may be considered (usually in a combination that is not necessarily required to cover all types):

- first, information should be marked as confidential, either individually or in its entirety, where its secrecy does not become apparent from the circumstances;
- secondly, confidentiality obligations should be expressly provided for in the contract controlling the share of the information in question, if they are not apparent from the nature of the contract; the conclusion of a separate non-disclosure agreement (NDA) before sharing any confidential information is usually the minimum of adequate protection of secrecy;
- thirdly, applying the "need to know" principle, employees or third parties should only have access to the confidential information they

need to fulfil their contractual obligations or exercise their rights;
- fourthly, technical and organisational protection measures may be required, which can range from simple password protection to firewalls, encryption and complex security systems; and
- fifthly, every company will have to consider whether and to what extent each employee should be given the opportunity and the authority to store company information on their own data carriers or to use their own computer in their office at home.

Furthermore, it is safe to assume that large companies or companies with numerous and valuable secrets will be subject to stricter requirements than small and medium-sized enterprises. However, the question of how much effort will be required for qualifying the steps taken as the required level of reasonableness will ultimately have to be decided by the CJEU (for best practices, see **3.1 Best Practices for Safeguarding Trade Secrets**).

1.6 Disclosure to Employees

In general, the disclosure of a trade secret to employees does not affect the availability of legal protection for the trade secret, as long as the employee is under an obligation of secrecy. In most cases, such an obligation to secrecy can be derived from the individual's employment contract.

However, there is a strong opinion in German legal literature that the secrecy measures necessary to classify information as a trade secret are not met if employees are not expressly informed of their duty of confidentiality and sign a confidentiality agreement (ideally with a contractual penalty) – with the consequence that there would be no trade secret to begin with. Since it is not yet foreseeable whether the courts will follow this view, it is strongly recommended that appropriate NDAs be concluded (this also applies vis-à-vis third parties who get in touch with trade secrets; see **1.5 Reasonable Measures**).

1.7 Independent Discovery

In principle, neither independent discovery nor reverse engineering has any impact on the existence of trade secret protection. The right in a trade secret under the TSA is not an exclusive right, so parallel ownership by several entities is possible.

While the owner of a trade secret cannot prevent third parties from independent discovery or reverse engineering (and consequently cannot prevent the third party from using or licensing the secret), this does not affect the existence of the secret itself as long as the third party does not disclose it publicly. If, however, the third party makes the secret publicly known, the protection for all other owners also lapses.

1.8 Computer Software and Technology

There are no protections in German law that are unique to computer software and/or technology with regard to trade secrets. There are some provisions regarding data protection, the integrity of electronic data, copyright protection of computer software or telecommunications secrecy that may also apply in the case of breach of a trade secret. However, it should be noted that these regulations only provide legal protection in their respective areas. This protection may overlap in individual cases, but not necessarily.

1.9 Duration of Protection for Trade Secrets

Trade secrets do not have a fixed or maximum term of protection: they remain protected under the TSA as long as the respective information meets the relevant requirements (see **1.4 Elements of Trade Secret Protection**). As soon as the information is no longer secret, its protection is irrevocably lost, regardless of a con-

trolled or accidental – or even illegal – disclosure. However, it should be noted that "disclosure" in this regard means disclosure to the public or at least to a larger group of people that normally deal with the kind of information in question. A description of the secret in a professional journal, at a trade fair or in a lecture is sufficient to trigger disclosure.

By contrast, disclosure to employees and contractual partners will usually not affect trade secret protection as long as they are obliged to secrecy on the basis of employment contracts or by confidentiality agreements (see **1.6 Disclosure to Employees**).

1.10 Licensing

In principle, the trade secret owner can license a trade secret like any other intellectual property right. As long as the licensee is obliged to secrecy during the term of the licensing agreement and afterwards (ideally with an adequate contractual penalty in the case of a culpable infringement), licensing does not affect the existence of the trade secret.

1.11 What Differentiates Trade Secrets from Other IP Rights

Protection for trade secrets differs from the other types of intellectual property protection available in Germany in many ways.

The differences in the scope of protection are the most notable: while the owner of intellectual property rights is granted absolute protection and may prohibit third parties from using and exploiting the protected intellectual property in any way (notwithstanding statutory exemptions), the trade secret owner is not granted similar rights. While they may prohibit employees and contractors from using or disclosing their secrets, there is no comparable absolute protection for trade secrets outside of such special contractual relationships.

On the contrary, the TSA does not prohibit third parties from using trade secrets per se, but only penalises the breach of factual security measures that its owner must actively ensure (see **1.5 Reasonable Measures**). In other words, trade secret protection exists only against the unfair disclosure of the information; if the information becomes known due to negligence in the protection of secrets, its protection is lost. This means, on the one hand, that protection is lost if the information in question becomes public (even if unlawfully) and, on the other hand, that the owner cannot take action against an independent parallel creation by third parties.

Furthermore, there are significant differences regarding costs, the scope and the duration of the protection; in particular, in comparison to patents: while patent protection entails high fixed costs due to application and maintenance fees, secrecy protection entails ongoing costs. Intellectual property rights are limited to the respective legal system, whereas secrecy leads to a de facto worldwide monopoly (even though the scope of protection may differ from jurisdiction to jurisdiction). In contrast, an invention patented in Germany can be used in other countries without legal consequences, unless independently patented there. In addition, protection by secrecy has an immediate and unlimited effect, whereas the patent application procedure can take several years and the term of protection is limited to 20 years.

1.12 Overlapping IP Rights

Generally, parallel protection of the same information as a trade secret and as any other IP right (with the exception of copyright, which does not require publication) will factually not be possible in most cases. In particular, the protection under the TSA and as a registered intellectual property right are mutually exclusive. This is because protection as a trade secret requires the information in question to be secret, whereas protection as

a registered right (eg, as a patent) requires an application – and thus its disclosure.

Therefore, parallel protection for technical secrets can only apply in (extremely rare) circumstances, where the information in question is registered as a so-called secret patent pursuant to Section 50 of the German Patent Act.

1.13 Other Legal Theories

The TSA is not exhaustive. Therefore, in principle, it is possible to bring a claim for breach of fiduciary duty against an employee who steals a trade secret or to bring a claim for tortious interference with contract against a defendant where it has induced an employee to breach a contractual confidentiality obligation to the owner/employer. However, there is an interdependence between contractual liability and liability under the TSA.

On the one hand, the design of the respective contract forms the framework of the legal protection of trade secrets and restricts such protection. For example, Section 3 (2) of the TSA gives general precedence to contractual agreements over the provisions of the TSA and Section 4 (2) Nos 2 and 3 forbids the use or disclosure of trade secrets only as long as it is in violation of a contract. On the other hand, the considerations of the TSA must be taken into account when interpreting contractual agreements and when determining the scope of non-explicitly agreed confidentiality obligations and rights of use. As a result, the scope of secrecy protection under the TSA does not generally differ from the scope of contractual claims.

1.14 Criminal Liability

German law imposes criminal penalties for trade secret misappropriation if the offender deliberately infringes a trade secret:

- to promote competition, whether internal or external;
- out of self-interest;
- for the benefit of a third party; or
- with the intention of causing damage to the owner of a business.

The penalty is imprisonment for up to three years or a fine. However, if the offender acts on a commercial basis, knows that the trade secret is to be used in foreign countries, or uses the trade secret in foreign countries themselves, the penalty is imprisonment for up to five years or a fine. A trade secret owner can pursue both civil and criminal claims. In fact, the initiation of criminal proceedings (and the investigative powers of the public prosecutor's office) is often the only way in which the trade secret owner can obtain the necessary evidence for his civil action (see **9.1 Prosecution Process, Penalties and Defences**).

1.15 Extraterritoriality

The question of whether and under which conditions it is possible to bring a claim under the German TSA based on misappropriation of trade secrets that take place in another country is highly controversial. When it comes to cross-border disputes, the rules of private international law – in particular, the Rome I Regulation and the Rome II Regulation – determine which law applies. This means that contracts on trade secrets (eg, licence agreements or NDAs) are governed by the Rome I Regulation with the consequence that (unless the parties explicitly made a different choice of law) the contract will be regularly governed by the law of the country where the trade secret owner has their habitual residence.

In contrast, trade secret misappropriations constitute tortious acts and thus are governed by the Rome II Regulation. While the Rome II Regulation contains special provisions for unfair competi-

tion and for infringements of intellectual property rights, there are no separate provisions for the infringement of trade secrets. This is problematic, because under German law, trade secret protection is seen as hybrid law that cannot be clearly assigned to either intellectual property or unfair competition law. For this reason, in German literature, different opinions are held on the applicable law, which depend on the area of law to which the respective author allocates the protection of trade secrets.

- The first opinion understands trade secret protection neither as intellectual property law nor as competition law and applies the general conflict rule of Article 4 of the Rome II Regulation. Therefore, the law of the country in which the damage occurs is applicable. This, in turn, is where the owner of the secret has its registered office or its (branch) office, or where the business or part of the business concerned is located. Therefore, in most cases, trade secret misappropriation could be prosecuted under the German TSA. However, if there is a pre-existing relationship between the violator and the trade secret owner (such as a contract that is closely connected with the trade secret misappropriation) and if that connection is subject to the law of a different country, that law may apply to the trade secret misappropriation as well.
- The second opinion views the misappropriation of trade secrets as an act of unfair competition and therefore as subject to Article 6 of the Rome II Regulation. This provision differentiates between market-related (Article 6 (1), Rome II Regulation) and bilateral (Article 6 (2), Rome II Regulation) infringements. Market-related infringements are acts that are not only directed against the infringed party (the trade secret owner), but also affect third parties. With regard to trade secrets, this would primarily be the case with the distribution of infringing goods, the disclosure of trade secrets to the general public or the use of trade secrets for marketing. Such acts of misappropriation would then be subject to the law of the state in which the products are distributed or the trade secrets are disclosed – and thus not subject to the German TSA, if the misappropriation takes place in another country. In contrast, for purely bilateral breaches of competition that only affect the interests of the owner of the trade secret (in particular, unauthorised access to the trade secret), the law of the country in which the damage occurs would be applicable. Therefore, if no third parties are affected, trade secret misappropriation could be prosecuted under the German TSA. Additionally, with regard to bilateral breaches, the information provided in bullet point 1 applies accordingly.
- The third opinion understands trade secret law as an intellectual property right and applies Article 8 of the Rome II Regulation. Therefore, the trade secret misappropriation would be governed by the law of the country in which the infringement takes place. However, it is unclear whether prior offences (eg, the acquisition of the trade secret) would have to be assessed separately according to their place of action or whether they would also be subject to the law of the country where the subsequent act (the use or disclosure) occurs.

It is not yet foreseeable which of these three opinions will ultimately prevail. Before the TSA came into force, most scholars followed the first opinion, differentiating between market-related and bilateral infringements; however, with the introduction of the TSA, the protection of trade secrets has shifted significantly in the direction of intellectual property law. Therefore, a conflict rule designed specifically for the protection of trade secrets would be preferable.

Contributed by: Thomas Nägele, Simon Apel, Jonathan Drescher and Alexander Stolz,
SZA Schilling, Zutt & Anschütz

2. MISAPPROPRIATION OF TRADE SECRETS

2.1 The Definition of Misappropriation

German trade secret law recognises four types of conduct that can be used to support a claim for trade secret misappropriation.

The first is the unlawful acquisition of the secret: a trade secret shall not be obtained by (i) unauthorised access to, appropriation of, or copying of any documents, objects, materials, substances or electronic files, lawfully under the control of the trade secret holder, containing the trade secret or from which the trade secret can be deduced, or (ii) any other conduct that, under the circumstances, is considered contrary to honest commercial practices. This alternative covers most activities commonly known as "industrial espionage" and can be conducted by anyone.

Secondly, a trade secret shall not be used or disclosed by anyone who:

- has acquired the trade secret unlawfully (see above);
- is in breach of a confidentiality agreement or any other duty not to disclose the trade secret; or
- is in breach of a contractual or any other duty to limit the use of the trade secret.

While the first alternative seeks to prevent further misappropriation of an already illegally acquired trade secret, the second and third variants are primary acts of infringement, which can only be fulfilled by offenders who gained access to the trade secret lawfully but breach their contractual duties by disclosing or using it (ie, employees and other contractual partners).

Thirdly, the acquisition, use or disclosure of a trade secret shall also be considered unlawful whenever a person, at the time of the acquisition, use or disclosure, knew or ought, under the circumstances, to have known that the trade secret had been obtained directly or indirectly from another person who was using or disclosing the trade secret unlawfully, as previously described. This provision seeks to prevent the "receiving of stolen secrets". While an infringement of the alternatives above is independent of fault, this variant requires the offender to act with negligence.

Lastly, the production, offering or placing on the market of infringing goods (which means goods whose design, characteristics, functioning, production process or marketing significantly benefits from trade secrets unlawfully acquired, used or disclosed) or the importation, exportation or storage of infringing goods for those purposes shall also be considered an unlawful use of a trade secret where the person carrying out such activities knew or ought, under the circumstances, to have known that the trade secret was used unlawfully.

The prohibition of the distribution of infringing products is very extensive and aims to prevent third parties from using foreign work without the consent of the trade secret owner and to ensure that the trade secret owner receives their pioneering return; ie, their competitive advantage.

If the owner's claim of misappropriation is based on an unlawful acquisition, it is sufficient to show that the defendant gained access to the trade secret without permission; there is no need to show that the trade secret was actually used. If, however, they refer to an unlawful use or disclosure, they have to prove the act of usage or disclosure and either the unlawful acquisition or a contractual breach.

If the owner does not base their claim on a contractual breach, they have to show and bear the burden of proof that the defendant (or the person

from whom the defendant got the secret) gained access to the trade secret through unlawful means. This is a major problem for the owner in many cases, even if presumptions and indications may work in their favour in certain circumstances.

2.2 Employee Relationships

In principle, it makes no difference in a lawsuit whether or not the defendant is an employee of the owner. With regard to trade secrets that the employee has (legally) obtained through their work, however, the claim may only be based on unlawful use or disclosure of the trade secret.

In principle, an employee is obliged to keep all trade secrets of their employer in confidence – even without an explicit obligation of secrecy. However, if the need for confidentiality of a piece of information cannot be clearly deduced from its nature, the employer must prove that it has instructed the employee about the need for confidentiality. It should also be noted that the enforcement of claims against employees is subject to the jurisdiction of the labour courts in Germany.

2.3 Joint Ventures

In principle, there are no special legal obligations between joint venture companies with regard to trade secrets. This means that the conclusion of confidentiality agreements between joint venturers is essential for companies under the new legal situation. According to the previous legal situation, the disclosure of trade secrets to third parties without concluding a confidentiality agreement did not lead to the loss of the characterisation as a trade secret, at least not to the extent that the recipient was obliged to maintain secrecy based on the interpretation of the contract. It is questionable whether this still applies with the introduction of the TSA.

Although the conditions for qualifying confidentiality measures as appropriate are still unclear due to the lack of case law (see **1.5 Reasonable Measures**), there are reasonable grounds to believe that a court could consider, for example, the release of particularly important trade secrets without concluding an NDA as an act of irresponsible negligence that could lead to the loss of the legal protection.

In order both to avoid this risk and to ensure that appropriate confidentiality measures are in place, any disclosure of trade secrets to a business partner, including joint ventures, should therefore only be made after an NDA has been concluded. It should also be noted that contractual partners are entitled, without deviating from contractual provisions, to reverse-engineer products or prototypes provided by the other partner.

2.4 Industrial Espionage

Section 4 (1) of the TSA provides protection against acquisition methods that cover most of the activities typically considered industrial espionage; ie, acquisition of a trade secret by unauthorised access to, appropriation of, or copying of any documents, objects, materials, substances or electronic files, lawfully under the control of the trade secret holder, containing the trade secret or from which the trade secret can be deduced. Trade secrets obtained in such ways may not be used or disclosed in any way. If the offender acts deliberately and with certain elements of malicious intent, obtaining trade secrets is also punishable by a fine or imprisonment (see **9.1 Prosecution Process, Penalties and Defences**).

In addition, there is a sophisticated regime of legal consequences consisting of injunctions and claims for damages as well as the destruction, surrender, recall, removal and withdrawal of infringing products from the market. These

consequences correspond to those of patent infringement.

3. PREVENTING TRADE SECRET MISAPPROPRIATION

3.1 Best Practices for Safeguarding Trade Secrets

Until 2019, appropriate confidentiality measures were not required for a legal protection of trade secrets under German law. Rather, the subjective intention of the owner of the secret to keep it secret was taken into account. Therefore, for "best practices" it is necessary to refer to literature and guides on know-how protection. In this respect, it is always emphasised that a comprehensive protection system is required that interlinks personnel, technical and organisational measures (also see **1.5 Reasonable Measures**).

- Organisational measures – the basis of a know-how protection concept is always an analysis of requirements for protection, in which it is defined which information needs to be kept secret. It is recommended to classify the information as "secret", "confidential" and "openly accessible" and to establish clear rules for handling classified information. A security officer should also be appointed. Finally, suspicious features should be systematically observed (eg, strangers on the premises, anomalies in the infrastructure, dismissals, copying of large amounts of data, presence of employees at unusual times, untraceable documents, unexplained loss of orders or customers, and appearance of copies on the market). Furthermore, property protection measures can include the control of access to company premises, securing the server area and video surveillance of sensitive areas.
- Personnel measures – the standard in this regard includes confidentiality agreements with employees and business partners, a clean-desk policy and the implementation of a need-to-know policy. Furthermore, employees should be sensitised and trained for the risks of espionage. Finally, measures to increase employee commitment to the company can help prevent employees from disclosing secrets.
- Technical measures – including, in particular, IT security measures; eg, firewalls, password protection, virus scanners, encryption of data carriers, network connections and email traffic, monitoring of log files, penetration tests, intrusion detection and systems.

Ultimately, however, "best practices" are difficult to define in the abstract, but must always be oriented to the requirements of the respective company and the trade secret to be protected. It remains to be seen how German case law will develop with regard to such "best practice".

3.2 Exit Interviews

In Germany, employers usually do not conduct exit interviews for departing employees. While such interviews are not prohibited, the employee is not obligated to answer questions regarding their new employer.

4. SAFEGUARDING AGAINST ALLEGATIONS OF TRADE SECRET MISAPPROPRIATION

4.1 Pre-existing Skills and Expertise

In theory, German trade secret law distinguishes between an employee's general knowledge and skills, which they are free to use after they leave the employer, and protectable trade secrets, which remain in the control of the employer. In practice, however, this distinction is extremely

difficult and has become known as a major problem of German trade secret law.

The general rule is that the employee is not permitted to use records of any kind containing trade secrets of their employer, but may use everything they know by experience and/or by heart. Furthermore, according to case law of the FCJ, the employee is also forbidden from systematic memorisation of the trade secret.

However, there is no assignment in the sense that the employee may use his general knowledge and acquired skills, whereas factual knowledge (eg, the composition of a specific product or customer lists) is solely assigned to the company. As long as the relevant secret is sufficiently complex and the employee cannot reproduce it without recourse to documents, this is not a problem. There are, however, countless secrets that can only be explored with great effort (eg, a recipe or the ideal temperature for a burning process), but are very easy to remember. Since German law does not recognise the doctrine of "inevitable disclosure", the employer's only option is to agree a non-competition clause with the employee. However, this is only possible subject to a consideration and for a limited time.

4.2 New Employees

As far as is apparent, the potential risk of liability for trade secret infringements due to the recruitment of employees from competitors is, strangely enough, often ignored by companies in Germany. The standard compliance manuals contain no reference to this problem. This is presumably related to the fact that the consequences of a trade secret misappropriation have not been particularly serious for the infringer so far. This has now changed with the TSA coming into force due to the stricter liability (in particular, the introduction of claims by the trade secret owner for recall and destruction of infringing goods).

However, since German law does not assign the content of trade secrets to a company, but allows the former employee to use all knowledge they have memorised, the new employer fulfils its obligations if it informs the employee of the prohibition on using old documents.

5. TRADE SECRET LITIGATION

5.1 Prerequisites to Filing a Lawsuit

There are no specific prerequisites to be obeyed before initiating litigation (eg, a mediation procedure) in main proceedings. However, an immediate filing of a lawsuit without sending a warning letter might have implications for the owner's obligation to bear the costs if the defendant immediately acknowledges the claims raised as justified. Furthermore, due to a recent change in case law, in preliminary injunction proceedings the applicant is usually required to send a warning letter and to await the reaction of the defendant before filing a motion for preliminary injunction.

5.2 Limitations Period

Under the TSA, trade secret claims are subject to German law's standard limitation period of three years. This period commences at the end of the year in which the claim arose and the trade secret owner obtains knowledge of the circumstances giving rise to the claim and of the identity of the obligor, or would have obtained such knowledge if they had not shown gross negligence.

Furthermore, in so far as the infringer has acted intentionally or negligently, they are obliged, even after expiry of the limitation period, to return to the trade secret owner whatever they have obtained through the unlawful use at the expense of the owner. However, this applies only to the extent that the enrichment is still in

the infringer's possession. This claim expires six years after the expiry of the limitation period of the original claim.

5.3 Initiating a Lawsuit

To initiate a trade secret lawsuit, the owner must identify the competent court (see **5.4 Jurisdiction of the Courts**), pay an advance on court costs (see **7.4 Attorneys' Fees**) and file the application. In addition, the owner may request the court to classify all or part of the information in dispute as confidential (see **5.8 Maintaining Secrecy While Litigating**).

5.4 Jurisdiction of the Courts

With regard to trade secret claims, the regional courts (*Landgerichte*, or LG) have exclusive jurisdiction. Furthermore, in each German state there is a limited number of specialised regional courts that deal exclusively with trade secret cases. Thus, a trade secret owner would have to review which regional court is competent for the alleged trade secret infringement in the respective case. The standard local jurisdiction is that of the court in whose district the defendant has their general place of jurisdiction.

5.5 Initial Pleading Standards

There is no stricter particularity standard applicable to trade secret claims. This means that, in principle, the allegation of a misappropriation of a trade secret based on "information and belief" is sufficient for the submission of a pleading. However, if the defendant denies the infringement, the claimant must prove their claim.

5.6 Seizure Mechanisms

The trade secret owner can sue for recall, removal and withdrawal of infringing products from the market. In order to prevent further distribution of infringing products, they can have infringing products seized even before a final judgement. To obtain such a seizure order, the claimant must plausibly demonstrate that their right to recall exists and that the matter is urgent, meaning that an immediate seizure of the infringing products is necessary to prevent further infringement. The seizure is carried out by the bailiff.

5.7 Obtaining Information and Evidence

The German Code of Civil Procedure recognises five types of evidence:

- evidence taken by visual inspection;
- evidence provided by hearing witnesses;
- evidence provided by experts;
- evidence provided by records and documents; and
- evidence provided by examination of a party.

Since German law in general does not provide for disclosure or discovery, in many cases, obtaining the necessary evidence to support a trade secret claim constitutes a big problem for the trade secret owner. This is due to the fact that – in contrast to patent lawsuits, for example – the mere use of information is not sufficient for a claim under the TSA, but the owner must prove that it was acquired unlawfully.

If the infringement is obvious, or the owner has already filed an infringement action against the infringer, the owner of a trade secret has a special claim for disclosure of certain information against third parties who, in a commercial capacity, possessed infringing goods, used infringing services, rendered services that were used for the infringement or took part in any such action. In addition, during infringement proceedings, the defendant may be ordered to disclose specific information to the claimant as part of the infringement claims; eg, with regard to the revenue generated by the infringing goods or services. However, these claims generally do not enable the owner to prove that the trade secret was acquired unlawfully. This often requires the initiation of criminal proceedings in order to ben-

efit from the more extensive powers of the public prosecutor's office (search and seizure).

5.8 Maintaining Secrecy While Litigating

The court may, at the application of one of the parties, classify information relevant to the case as confidential, in whole or in part, if such information may be a trade secret. As a result, all participants in the proceedings are prohibited from using or disclosing the information outside the court proceedings. A breach of this confidentiality obligation may result in a fine of up to EUR100,000 or imprisonment for up to six months; in addition, the owner of a trade secret may initiate further proceedings for breach of a trade secret in the event of a breach of these obligations.

However, the described prohibition to use the secret does not solve the problem that the opposing party still gains knowledge of the secret and may be able to use this knowledge without exploiting the secret in the literal sense. This primarily concerns secrets such as market analyses, advertising strategies and price calculations that are not characterised by technical usability. But even if the secret could be protected by a prohibition of exploitation, the owner of the secret may have an interest in ensuring that the secret information does not become known to the competitor in the first place; for example, because they do not trust the other party to comply with the prohibition and are afraid of future proceedings. In all these circumstances, only the exclusion of the other party from the process of taking evidence – ie, a genuine secret trial – would be of any help. However, such a procedure is not possible under German law.

In the preliminary stage, namely when enforcing claims to inspection, there is also a method known as the "Düsseldorf Model", which was developed by the courts of Düsseldorf and in which the taking of evidence is carried out by an expert, excluding the applicant as far as possible. This procedure was developed for patent infringement litigation, but is also intended to be applied in trade secret litigation. However, this procedure is only applied in favour of the debtor and only in circumstances where the secret in question is merely evidence and does not constitute the subject matter of the dispute itself.

5.9 Defending against Allegations of Misappropriation

The available defences regarding trade secret litigation differ from case to case. Therefore, it is hard to identify the "best practices" a trade secret defendant should obey. However, there are some standard arguments the defendant may try to use.

- The defendant may challenge the fact that the information in question constitutes a trade secret at all. This is particularly recommended if it is doubtful whether the protective measures were sufficient, since the burden of proof lies with the owner.
- The defendant may deny that the acquisition, use or disclosure of the secret is an offence against the TSA. This can be particularly advisable in contractual relationships where no separate confidentiality agreements were concluded. As an employee, the defence might be that the relevant information was memorised.
- The defendant may claim that they have obtained the trade secret through their own independent development or via reverse engineering.
- If the lawsuit is brought against a third party who was not involved in the actual infringement, but only acquired the trade secret or infringing goods at a later date, the third party can defend itself by arguing that it did not know and did not have to know, under the circumstances, that the trade secret had been obtained unlawfully.

Furthermore, if the trade secret owner asserts claims for inspection against the defendant in order to obtain evidence, the defendant may be able to defend itself against this inspection by invoking its own confidentiality interests.

5.10 Dispositive Motions

German law does not provide for a dispositive motion. If the claim is inconclusive, it is dismissed. If the claim is conclusive and the defendant does not submit a motion, a judgment by default is issued. However, both kinds of decisions are rendered in the course of the court proceedings themselves.

5.11 Cost of Litigation

Attorney fees and court fees are subject to the value of the amount in dispute (*Streitwert*), which is determined primarily by the value of the trade secret. Every activity of the attorney will be remunerated according to the provisions of the German Act on Reimbursement of Lawyers (*Rechtsanwaltsvergütungsgesetz*), which determines the relevant business fee unit for every legal task and, in an annexed schedule, the applicable fee for the specific amount in dispute. Since trade secrets often have a very high value – which results in correspondingly high litigation costs – the amount in dispute may be adjusted appropriately by the court upon request.

However, in many cases the opposite will be the case. Even if, by law, the statutory legal fees may not be undercut, clients and attorneys are free to agree on a (significantly) higher fee rate by contract, which is quite common in IP cases (and in general), at least at well-known law firms. Hourly rates between EUR200 and EUR600, depending on the seniority of the counsel involved, are common practice. Thus, attorney fees usually exceed the amount of the statutory fees by a great deal.

Since the statutory legal fees may not be undercut, German attorneys generally are not permitted to work on a contingency fee basis. A contingency fee may be agreed only for an individual case and only if the client, upon reasonable consideration, would be deterred from taking legal proceedings without such agreement on account of his economic situation. These requirements are applied very restrictively. In contrast, litigation financing is available in Germany and is a market that has grown strongly in recent years.

6. TRIAL

6.1 Bench or Jury Trial

The law stipulates that civil proceedings usually shall be heard by a single judge in the regional court. However, in cases of particular difficulty, fundamental importance or at the application of both parties, the proceedings take place before a Chamber (*Kammer*) of the court that consists of three judges. In trade secret cases, such will usually be subject to jurisdiction of the regional courts and it may often be the case that, due to the complexity of such cases, the Chamber will hear the case.

6.2 Trial Process

Civil proceedings in Germany are primarily conducted through written submissions. However, live witnesses may also be heard for the purpose of discovery of the relevant facts if the party that bears the burden of proof applies for such a hearing. While the parties present legal arguments at trial, the court is not bound by them. However, the court may not award more than the plaintiff has requested. It typically takes about 12 to 24 months to complete a trade secret trial in Germany, depending on the complexity of the case.

6.3 Use of Expert Witnesses

German law allows for the presentation at trial of expert witness testimony. Since the TSA does not contain special provisions regarding this matter, the process for hearing expert witness testimony is governed by the German Code of Civil Procedure. The expert is usually nominated by the court, which takes into account suggestions by the parties. Such expert is neutral and their expertise may only cover factual questions (with the sole exception of questions of foreign law, which are treated as a matter of fact under German law).

Usually the expert provides a written expert testimony that the parties may challenge and that usually is also discussed in an oral hearing with the expert before the court. The parties are also free to provide expert testimony by experts that they engage. However, such testimony does not have formal value as evidence as the opinion of an expert nominated by the court is only part of the respective party's arguments, which the court may (or may not) give weight to. Costs for experts vary and can be significant, depending on the complexity of the case.

7. REMEDIES

7.1 Preliminary Injunctive Relief

The owner of a trade secret can – and in most cases will – seek for preliminary injunctive relief before a final judgment in the case. In principle, neither a permanent nor an interim injunction is subject to time limitations. However, the debtor of a preliminary injunctive relief may request the court to set the claimant a time limit for filing an action. If this deadline expires without the claimant taking legal action, the court will revoke the preliminary injunction upon request.

7.2 Measures of Damages

Pursuant to Section 10 of the TSA, a successful claimant in a trade secret case may calculate its damages in three ways.

- They can demand compensation for the damage effectively incurred as a result of the misappropriation of the trade secret. However, this requires a concrete presentation of the damage caused, which can prove difficult in the case of trade secret claims.
- They can demand that the infringer surrender the profit made with the trade secret. While in the case of infringement of any other intellectual property right, the injured party may claim only that part of the infringer's profit that is based on the infringing act, the owner of a trade secret may claim the entire profit for which the infringement of the secret was at least partly responsible; ie, not only that part that is caused by the infringement.
- They can demand an appropriate remuneration that would have had to be paid if the consent for use had been obtained (licence analogy).

The claimant is free to choose which of such methods they want to use to calculate their damages. While they cannot combine the methods above with regard to the same damage, they can use different methods regarding different damage claims (eg, demand compensation for litigation costs as damage effectively incurred and use a licence analogy to recoup their losses regarding the trade secret itself). Punitive damages do not exist in German law, unless the parties made any prior contractual arrangements in this matter.

7.3 Permanent Injunction

A successful trade secret claimant can obtain permanent injunctive relief against the defendant as well as an order requiring the defendant to recall any incriminating products. However, the

plaintiff cannot restrict the subsequent employment of an employee in order to protect their trade secrets. A permanent injunction issued remains in force until the trade secret is disclosed.

7.4 Attorneys' Fees

Firstly, the plaintiff is responsible for paying accrued court fees in order to start the proceedings. During the dispute, expenses incurred for procedural actions are borne by the party that requests them. But ultimately the losing party is required to reimburse the prevailing party for all costs of litigation fees inclusive of court fees, expenses and attorney fees of both parties in the statutory amount. The judgment rendered by a court always encompasses a decision on the reimbursement of cost. In the case of a partial win, the statutory amount of the total cost will be split pro rata.

7.5 Costs

In addition to lawyer's fees (see above), a successful claimant can recover disbursed court costs as well as costs for witnesses and experts. For the process for seeking an award of costs, see **7.4 Attorneys' Fees**.

8. APPEAL

8.1 Appellate Procedure

In general, the general civil law rules apply in appellate procedures, with some minor modifications.

Appeals against first-instance decisions (*Berufung*) will be conducted before the Higher Regional Courts (*Oberlandesgerichte*). Within one month of service of the full version of the judgment, the appellant must submit a statement of appeal. Within one more month, the appellant must submit a statement on the grounds of appeal describing the reasons why they consider the judgment to be erroneous and the significance of these errors for the judgment; such further filing period may usually be extended once for one month or even more, depending on the complexity of the case. Further extensions require the consent of the other party. The Higher Courts of Appeal review the case for points of law and with regard to the facts. With regard to the latter, they enjoy a considerable degree of discretion with regard to which facts they review again.

The second appellate level (revision) before the FCJ is subject to explicit permission to appeal being granted. This permission may be granted by the Higher Regional Court or by the FCJ itself upon the filing of a so-called non-admission complaint (*Nichtzulassungsbeschwerde*) against the denial to grant a second appeal. For the filing of a non-admission complaint and the non-admission complaint respectively, the same deadlines apply as in the first-level appeal (see the preceding paragraph). The content requirements are also similar, and it must be submitted by an attorney admitted to practice before the FCJ. The FCJ only reviews the decisions of the lower courts for points of law.

At the first appellate level, as a general rule, the duration of the proceedings will usually take at least 6 to 12 months. The second-level appeal very often lasts for a further 18 to 24 months, until a decision is rendered.

The appeal mechanism as described above is available to both claimants and respondents in the main proceedings. In proceedings for interim relief, only first-instance decisions can be appealed, while the second appellate level is not available.

8.2 Factual or Legal Review

On the first appellate level, as a general rule, a full review of the facts of the case and on points

of law will take place. However, a statement of completely new facts compared to the first-instance proceedings is only permitted subject to certain restrictions (eg, the facts only occurred after the judgment in review was made).

In contrast, the FCJ is bound by the facts found by the first-instance and the first appellate-level court. Thus, the second-level appeal is on points of law only.

9. CRIMINAL OFFENCES

9.1 Prosecution Process, Penalties and Defences

Trade secret theft is prosecuted only upon request of the victim, unless the prosecuting authority deems there to be a special public interest in prosecution that calls for ex officio intervention.

The available defences to a criminal charge for theft of trade secrets vary greatly depending on each individual case. It should be noted that, unlike in civil proceedings, there are no presumptions or rules on reversal of the burden of proof, which means that the prosecuting authority must prove all the relevant facts. However, the prosecuting authority may search the premises of the suspected offender and order seizures. This will often enable the prosecutor to prove that the offender is in possession of a foreign trade secret. However, if the perpetrator defends themselves by saying that he did not obtain the secret in an improper manner, or at least had no knowledge of an improper acquisition, it will often be difficult to refute.

The victim has a relatively weak position in German criminal proceedings. During the preliminary proceedings, the investigation of the case is the sole responsibility of the competent law enforcement authorities, so that the injured party's possibilities for co-operation are mainly restricted to providing testimony. In addition, the victim has (at least in principle) the right to inspect the investigation file. However, if there is a suspicion of a violation of secrecy and the file contains trade secrets of the accused, an inspection will often fail due to the confidentiality interests of the accused. The victim has no right to be present during searches by the public prosecutor's office.

If the main hearing takes place, the victim can join the criminal proceedings as a joint plaintiff. This enables themselves – at least to a certain extent – to influence the outcome of the proceedings in the form of statements, questions and motions.

10. ALTERNATIVE DISPUTE RESOLUTION

10.1 Dispute Resolution Mechanisms

In spite of the growing significance of ADR in Germany, at present it is not very common in IP matters, and even less so in trade secret cases. However, it has to be taken into account that due to the difficulties in proving the facts and the (at least up to now) insufficient means for keeping secrets confidential, only very rarely are proceedings concerning infringements of secrets brought before the regular courts.

However, with the TSA coming into force and the excellent work of German courts in litigating IP cases, it is to be expected that proceedings regarding trade secrets will rise. Compared to other countries, the courts work relatively quickly and at reasonable cost (see **5.11 Cost of Litigation**) and usually provide a substantial level of expertise. Hence, it is not necessary for the parties to rely on ADR in order to arrive at a proper solution for their dispute. Furthermore, a fruitless attempt at ADR is not a prerequisite

for any court action. Nevertheless, ADR may still be appropriate in cases of long-term and multinational agreements between the parties, rather than in infringement cases.

The most common ADR method in IP matters is arbitration. Provided that the parties conclude a valid arbitration agreement in an arbitrable matter, an action before a state court is not admissible. For all arbitral proceedings conducted in Germany, the tenth *Book of the German Code on Civil Process* (Sections 1025 to 1066) applies. The law is based on the UNCITRAL Model Law and Germany is party to various international arbitration treaties, such as the New York Convention.

Parties are then free to agree on the language used in the arbitral proceedings, the place of arbitration and the person and the number of arbitrators. Pertaining to the procedural rules, the parties may agree to pre-drafted arbitration rules (eg, by the ICC) or leave it to the arbitral tribunal to decide how to approach fact-finding and taking of evidence. In Germany, facts and evidence must usually be provided by the parties. "Discovery" rules are not applicable and witnesses are questioned by the judge (no cross-examination). The tribunal's final ruling has the same status as a final court judgment and can be declared enforceable. It includes a decision on the costs, taking into consideration all circumstances of the case; in particular, the outcome.

German courts do not normally intervene in a pending arbitration. However, exceptions are made, for instance, for the appointment or challenge of arbitrators if there is no agreement between the parties, interim measures or assistance in taking evidence or enforcement of orders. Moreover, the court can set aside an arbitral tribunal's jurisdiction under specific circumstances if certain essential prerequisites of German law are not met.

SZA Schilling, Zutt & Anschütz has been one of the most reputable German corporate law firms for almost a century. With close to 100 attorneys, it advises domestic and international clients on nearly all areas of corporate and commercial law. The IP/IT department of SZA is located in Mannheim and Frankfurt and currently practises with nine attorneys in all areas of IP and IT, as well as data protection law. With the establishment of its China Desk, SZA provides consultation for Chinese companies regarding investments and business activities in Europe in all fields pertaining to commercial law, especially in relation to the protection of intellectual property, including the registration, defence, and judicial and out-of-court enforcement of brands, patents and know-how. Further, in mutual co-operation with leading local law firms, SZA also provides consultation in the field of industrial property rights for European companies regarding their business in China.

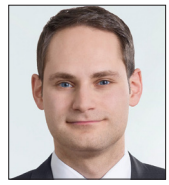
AUTHORS

Thomas Nägele is a partner specialising in intellectual property, trade marks and unfair competition, patent litigation, information technology, cybersecurity and data protection, and heads the IP/IT department. He is a lecturer at the University of Heidelberg and a member of numerous professional bodies, such as the executive committee of IZG – Interdisziplinäres Zentrum für Geistiges Eigentum an der Universität Mannheim e.V. (Interdisciplinary Centre for Intellectual Property at the University of Mannheim). He has contributed to a large number of articles in industry publications.

Simon Apel is a senior associate who specialises in copyright law, unfair competition law, law of trade secrets, trade mark law, information technology law and litigation. He is a member of the Deutsche Vereinigung für gewerblichen Rechtsschutz und Urheberrecht (GRUR) e.V and has contributed to over 80 publications; in particular, in the field of copyright law, unfair competition law and trade mark law. He has a Dr jur (University of Bayreuth, 2010), with a doctoral thesis on the legal rights of the musical performer in Germany and the USA.

Contributed by: *Thomas Nägele, Simon Apel, Jonathan Drescher and Alexander Stolz,*
SZA Schilling, Zutt & Anschütz

Jonathan Drescher is an associate. His practice covers copyright, unfair competition law, trade mark law, trade secret law, information technology law, media law and litigation. He has made several contributions to German law journals.



Alexander Stolz is an associate specialising in copyright, patent law, trade mark law, information technology law, media law and litigation. He has made several contributions to German law journals.

SZA Schilling, Zutt & Anschütz

Otto-Beck-Strasse 11
D-68165 Mannheim

Tel: +49 621 4257 247
Fax: +49 621 4257 286
Email: thomas.naegele@sza.de
Web: www.sza.de

SZA
SCHILLING, ZUTT & ANSCHÜTZ

Trends and Developments

Contributed by:
Thomas Nägele, Simon Apel, Jonathan Drescher and Alexander Stolz
SZA Schilling, Zutt & Anschütz see p.93

Introduction: A New Start for Trade Secrets Protection in Germany

Since 2019, the legal protection of trade secrets in Germany has experienced a phase of great upheaval. From 1896 to 2019, over a period of more than 120 years, criminal law and case law dominated the protection of trade secrets in Germany. The central provisions for the protection of trade secrets were Sections 17 to 19 of the German Act against Unfair Competition (UCA) (*Gesetz gegen den unlauteren Wettbewerb*, or UWG), which stipulated certain misconduct with regard to trade secrets as criminal offences.

Measured against the immense economic importance of secret know-how, these regulations were extremely rudimentary (for example, there was not even a statutory definition of the term "trade secret"; rather, this was left to the courts) and legal protection of trade secrets was rather complicated. With the (now repealed) UCA, only two criminal provisions existed that, under certain circumstances, made the acquisition, disclosure or use of trade secrets a punishable offence, provided that the perpetrator acted wilfully and with specific elements of intent.

Protection under civil law (claims for cease and desist, removal, damages, etc) could only be obtained by the trade secret owner on the basis of so-called transfer norms in German tort law. For this purpose, however, they had to prove that the infringer had committed at least one of the criminal offences under Sections 17 and 18 of the UCA. This often proved to be impossible in practice, because of the narrow scope of the aforementioned UCA provisions, in particular, and without limitation, regarding the narrow definition of potential perpetrators, the small scope of misconduct covered and the strict subjective requirements stipulated therein.

This system was turned upside down when the German Trade Secret Act (TSA) (*Gesetz zum Schutz von Geschäftsgeheimnissen*, or GeschGehG) came into force in April 2019. In stark contrast to the traditional German concept outlined above, where the legal protection of trade secrets was strictly accessory to criminal law, the TSA is based on EU law, implementing the Directive on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (Directive (EU) 2016/943, the EU Trade Secret Directive, or ETSD) and provides now (at last) a dedicated law for the protection of trade secrets, which is dominated by a civil law concept.

With regard to its general structure, the TSA comprises 23 sections in four parts.

Sections 1 to 5 of the first part contain the core provisions of the new TSA, such as the scope of application of the TSA (Section 1) and the definitions of key terms (Section 2), including, most notably, the first statutory definition of a trade secret in Germany. Thereafter, in concluding enumerations respectively, the TSA explicitly defines permitted conduct (Section 3) and prohibited acts of infringement (Section 4) with regard to trade secrets. This is followed by a provision on individual exceptions – or privileges – regarding conduct with trade secrets without the consent of the owner if such conduct is made

Contributed by: *Thomas Nägele, Simon Apel, Jonathan Drescher and Alexander Stolz,*
SZA Schilling, Zutt & Anschütz

for the protection of a legitimate interest (Section 5). These are, at first, purely civil law regulations.

Consequently, the second part of the Act (Sections 6 to 14) contains provisions on the civil law consequences of an infringement and the third part contains special provisions on proceedings in trade secret disputes (Sections 15 to 22).

Only in the fourth part of the TSA, in Section 23, can one find a criminal law provision, which penalises some of the prohibited actions mentioned in Section 4 if further subjective requirements – namely intention – are met. This is all that is left of the once dominant position of criminal law provisions in German law on the protection of trade secrets.

Such a far-reaching paradigm shift naturally leads to considerable uncertainty among courts, legal practitioners and companies alike. While the legal literature initially needed some time to seriously take notice of the TSA, in the past two years, the discussion has gained momentum as more and more articles appeared dealing with various facets of the TSA – from the correct draft of non-disclosure agreements to "best practices" for company know-how protection systems to the impact of the TSA on employment contracts. The first court decisions on the TSA have been rendered as well, dealing mainly with the temporal applicability of the new provisions and with the question of what requirements must be fulfilled in order to ensure "appropriate confidentiality measures" for information to be protected as trade secrets.

The purpose of this chapter is to shed some light on some of the most relevant changes that the TSA has brought to German law on the protection of trade secrets, namely:

- the new requirements that information must fulfil in order to be considered a trade secret;
- the new concept of legal consequences of an infringement; and
- the new provisions on the protection of secrets in civil proceedings.

Furthermore, some "traditional" issues relating to trade secret protection under German law that were not solved by the TSA will also be dealt with.

New Protection Requirement: Appropriate Confidentiality Measures

One of the most significant changes – especially for business practice – is that a piece of information can now only be protected as a trade secret under German law "if it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret". Although this requirement had already been established in international law by the 1990s, by Article 39 of the TRIPS Agreement, in Germany the mere subjective will of the owner to maintain the confidentiality of a trade secret had been deemed sufficient for protection by German courts under the UCA; in most cases, such will did not even have to be explicitly stated but was presumed if the trade secret had commercial value.

This, however, has now changed under the TSA. In the case of a dispute, the owner of a trade secret must now prove that they have taken appropriate security measures to protect confidentiality with regard to the secret in question.

But what does "appropriate" mean in this context? Neither the TSA nor the underlying ETSD provides an answer to this important question. Thus, it is difficult to find a solution that is not only in line with the policy of the TSA and the ETSD, but also operable in the ordinary course of business – not only for courts but for companies and legal counsel as well.

Against this backdrop of insecurity, it does not come as a surprise that by far the largest part of the past two years' court decisions and scholarly contributions on the subject of trade secret protection dealt with the issue of adequate protection measures.

While it is a matter of general consent among German courts and scholars (i) that the trade secret owner must "only" ensure appropriate (and not the best possible or maximum effective) safeguards, and (ii) even though consent is less strong in this respect, that the intensity of measures that must be taken to establish adequate protection of secrecy depends on the nature and value of the trade secret as well as the size of the company and the costs of the measures, many details (eg, on the validity of so-called catch-all clauses) are still unclear and controversial, and the subject of lively discussion.

As long as the CJEU does not decide under the ETSD how much effort will be required for qualifying the steps taken as the required level of reasonableness, it can be assumed that this question will continue to be one of the dominant issues. Such future decision of the CJEU will, however, also be binding for the German courts when applying the TSA.

Third-Party Liability and Legal Consequences

With regard to substantive law, the TSA significantly extended third-party liability as compared to the former German law on trade secrets. While the liability of those directly infringing a trade secret was already quite extensive under the latter, the use or disclosure of a trade secret by a third party in a merely negligent misjudgement of a prior breach of secrecy was not sufficiently covered.

Now, with the TSA taking over, the acquisition, use or disclosure of a trade secret is also considered unlawful "whenever a person, at the time of the acquisition, use or disclosure, knew or ought, under the circumstances, to have known that the trade secret had been obtained directly or indirectly from another person who was using or disclosing the trade secret unlawfully". This applies, in particular, with regard to the production, offering or placing on the market of infringing goods; or the importation, exportation or storage of infringing goods for such purposes.

In addition, the TSA significantly expanded the legal consequences for infringers. While under previous German law the claimant could already sue for injunctive relief or damages, claims to recall infringing goods or to have them removed from distribution channels were limited to very specific cases. The trade secret owner could only demand the destruction and surrender of documents containing the secret and of products in which the secret was embodied. However, it remained open in case law as to whether this also entitled them to recall infringing goods and to have them removed from distribution channels. And as long as the disclosed trade secret was not manifested, as such, in the products offered, the owner of the trade secret could not demand the surrender or destruction of such infringing goods. This was particularly problematic with regard to commercial (as opposed to technical) trade secrets, which can offer as great a competitive advantage to the offender as technical expertise from a technical trade secret, but without having a comparable relevance for products sold using such competitive advantage from the commercial trade secret.

To give an example: if the infringer used an unlawfully disclosed customer list in order to distribute their products on the market more quickly at the expense of the owner of the trade secret, the latter usually had no possibility of restoring their market position based on their right in the original trade secret. In contrast, the TSA now expressly grants the trade secret owner claims

Contributed by: *Thomas Nägele, Simon Apel, Jonathan Drescher and Alexander Stolz,*
SZA Schilling, Zutt & Anschütz

for recall and removal of infringing products, whereby even those products that have been manufactured completely legally but whose distribution was made possible by the unauthorised use of confidential customer lists or advertising concepts are considered to be "infringing".

The interaction of these two new elements substantially extends the scope of protection for the trade secret owner. If now, for example, someone uses the secret-process steps or the supplier data of a competitor in the manufacture of a product and obtained such information unlawfully, the legal protection is not only directed against the manufacturer, but extends to every person who is part of the downstream distribution chain involved – regardless of whether this person has knowledge of the secret or whether it is embodied in the product itself.

In turn, however, there is now a significant risk of third parties being caught up in the "undertow" of a breach of secrecy through no fault of their own, which results in substantial liability risks since the person responsible for the above-mentioned infringements can be held liable to recall and destroy infringing products. This can be very problematic, because, while the manufacture and distribution of products are often long-term in nature and require a long preparation phase, the required knowledge, by contrast, can also be obtained subsequently simply due to a notification from the trade secret owner. Therefore, as soon as the trade secret owner notifies the "indirect offender" of the unlawful nature of their conduct, the latter may no longer manufacture or distribute the products, to avoid conflict with the trade secret owner.

Confidentiality in Civil Proceedings

Another major issue addressed by the TSA concerns confidentiality in civil proceedings. Just as under the provisions of the UCA, the owner of a trade secret must demonstrate and prove that the information in question is a trade secret if they want to derive claims from the TSA. The content of the trade secret will therefore generally be the subject of the oral proceedings. Under German law, however, court hearings are generally public, so that disclosure in court is, by definition, accompanied by the disclosure of the secret. In the absence of a secret, the grounds for all claims asserted on account of violations of the TSA would then no longer apply. The owner of the secret would lose both, the secret and the lawsuit.

While it is true that under former German law the owner of a trade secret could already apply for the public to be excluded from a court hearing, the decision to do so was subject to the courts' dutiful discretion – and the courts proved to be very reluctant in this matter, as the publicity of court proceedings, as such, enjoys a high priority under German law. The TSA has considerably mitigated this issue, as the parties now have, for the first time under German law, the right to request exclusion of the public. In addition, the court may, at the request of a party and after weighing all interests, restrict access to documents filed or presented by the parties or third parties in order to protect trade secrets. These measures are not limited in their scope of application to the main hearing, but the restrictions on access may be imposed as soon as the application or reply is served and shall remain in force until the proceedings are concluded.

Civil procedural law had similar deficiencies with regard to secrecy vis-à-vis the opposing party (who could not be excluded from the oral hearings). While it was possible to impose a duty of secrecy on the opposing party, with the penalty of a fine, this only helped to a limited extent, as it only prohibited the disclosure of the information, but did not provide protection against the defendant's own use and also did not protect against negligent disclosure of secrets.

Moreover, the secrecy requirement was linked to the exclusion of the public, which could be imposed at the oral hearing at the earliest. However, the risk of disclosure of a trade secret to the opposing party is not limited to the oral proceedings, but extends from the filing of the action to the taking of evidence in the oral proceedings to the pronouncement of judgment throughout the entire infringement proceedings. Since the infringed owner of the trade secret has the burden of proof, they must disclose at least parts of their secret know-how in the statement of claim in order to provide substantiation. If they refer to a secret manufacturing process, for example, they must explain both the process itself and the reasons why it is secret.

Since civil procedural law did not provide for any measures of secrecy at that time, the statement of claim and annexes were served on the respondent without any further measures of secrecy, even if the trade secret owner had already asked for special secrecy or exclusion of the public in the statement of claim. The defendant thus regularly became aware of the facts requiring secrecy as soon as the statement of claim was served and not only at the hearing itself, so that the duty of confidentiality became largely meaningless. As a result, the owner of the secret was regularly faced with the decision either to disclose the secret to the opposing party or to lose the case. This problem has been partially mitigated with the TSA coming into force. Now, on the one hand, the opposing party can be prohibited from using the secret, and on the other hand, this restriction can be imposed as soon as the lawsuit is pending – ie, when the statement of claim is served – and continues to apply even after the conclusion of the court proceedings.

New Law, Old Problems: Former Employees and the Gathering of Evidence

While the new TSA has led to numerous changes and significant improvements in the protection of trade secrets under German law, there are some continuing issues that the TSA does not address. Apart from the question of what criteria are to be used to assess the value of a trade secret, these concern, inter alia, the following aspects.

No clear allocation of trade secrets

One – if not *the* – core problem of the statutory protection of trade secrets lies in the utilisation of trade secrets by former employees. For decades, case law and literature have been dealing with the issue of finding a proper balance between the confidentiality interests of companies and their former employees who wish to benefit from their professional experience and knowledge. In theory, German trade secret law distinguishes between an employee's general knowledge and skills, which they are free to use after they leave their employer, and protectable trade secrets, which remain at the employer. In practice, however, this differentiation has almost exclusively been based on whether the employee has had to access documents in order to be able to use the secret (in which case, they were not allowed to use it) or whether they could reproduce the information from memory (in which case, they were).

It remains to be seen whether the courts will maintain this schematic differentiation between "memorised knowledge" and "written knowledge". In the authors' opinion, against the background of the ETSD, it will be necessary to give greater consideration to whether an employee who has left a company is dependent on having access to the acquired knowledge in order to be able to compete successfully on the labour market. This is because, according to Article 1 (3) of the ETSD, "this Directive shall not offer any ground for: […] (b) limiting employees' use

Contributed by: *Thomas Nägele, Simon Apel, Jonathan Drescher and Alexander Stolz,*
SZA Schilling, Zutt & Anschütz

of experience and skills honestly acquired in the normal course of their employment". For example, an employee who has worked for decades as an expert in a specific field may be unduly impeded in their professional development if they are denied access to the documents they have created on their own.

In contrast, one might imagine a case where an employee has only worked for two weeks in their former employer's company, but during this time have participated in a lengthy and highly complex series of experiments. The result of this series of tests may be very easy to remember (eg, the ideal temperature for a melting or firing process), despite the great effort and expense required for the experiment. As a result, there can be no doubt that knowledge of this secret cannot be regarded as "experience or skill which the employee has honestly acquired in the normal course of his work", but must belong solely to the employer. It is hoped that future case law will increasingly focus on the conflicting interests of employers and employees in individual cases.

Insufficient means of obtaining evidence

A major weakness of the TSA – as well as the ETSD – is the lack of provisions for obtaining evidence. Although the owner has a claim to information against the infringer under certain conditions, claims for inspection often fail in practice due to predominant confidentiality interests of the debtor.

Procedural confidentiality measures not fully sufficient

Although the TSA's provisions on secrecy in civil proceedings represent a step forward, they are not entirely sufficient. On the one hand, a prohibition against the use and disclosure of a trade secret does not solve the problem of the other party gaining knowledge of the secret, which may enable it to use this knowledge without exploiting the secret in the literal sense. This primarily concerns secrets such as market analyses, advertising strategies and price calculations, which are not characterised by technical usability. On the other hand, the new provisions only apply in proceedings for trade secret litigation – and thus neither in proceedings in which a trade secret is not the subject of dispute but merely evidence (eg, in patent infringement actions) nor in criminal proceedings. It is a pity that the German legislator did not incorporate the provisions of the TSA regarding confidentiality measures as a new minimum standard for all types of proceedings.

Outlook

Overall, the protection for trade secret owners in Germany has improved significantly with the TSA's coming into force. Even if the new law does not eliminate every old problem and confronts the practice with a variety of new problems, the provision of a largely uniform Europe-wide protection for trade secrets is an important and overdue step.

Contributed by: *Thomas Nägele, Simon Apel, Jonathan Drescher and Alexander Stolz,*
SZA Schilling, Zutt & Anschütz

SZA Schilling, Zutt & Anschütz has been one of the most reputable German corporate law firms for almost a century. With close to 100 attorneys, it advises domestic and international clients on nearly all areas of corporate and commercial law. The IP/IT department of SZA is located in Mannheim and Frankfurt and currently practises with nine attorneys in all areas of IP and IT, as well as data protection law. With the establishment of its China Desk, SZA provides consultation for Chinese companies regarding investments and business activities in Europe in all fields pertaining to commercial law, especially in relation to the protection of intellectual property, including the registration, defence, and judicial and out-of-court enforcement of brands, patents and know-how. Further, in mutual co-operation with leading local law firms, SZA also provides consultation in the field of industrial property rights for European companies regarding their business in China.

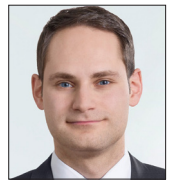
AUTHORS

Thomas Nägele is a partner specialising in intellectual property, trade marks and unfair competition, patent litigation, information technology, cybersecurity and data protection, and heads the IP/IT department. He is a lecturer at the University of Heidelberg and a member of numerous professional bodies, such as the executive committee of IZG – Interdisziplinäres Zentrum für Geistiges Eigentum an der Universität Mannheim e.V. (Interdisciplinary Centre for Intellectual Property at the University of Mannheim). He has contributed to a large number of articles in industry publications.

Simon Apel is a senior associate who specialises in copyright law, unfair competition law, law of trade secrets, trade mark law, information technology law and litigation. He is a member of the Deutsche Vereinigung für gewerblichen Rechtsschutz und Urheberrecht (GRUR) e.V and has contributed to over 80 publications; in particular, in the field of copyright law, unfair competition law and trade mark law. He has a Dr jur (University of Bayreuth, 2010), with a doctoral thesis on the legal rights of the musical performer in Germany and the USA.

Contributed by: *Thomas Nägele, Simon Apel, Jonathan Drescher and Alexander Stolz,*
SZA Schilling, Zutt & Anschütz

Jonathan Drescher is an associate. His practice covers copyright, unfair competition law, trade mark law, trade secret law, information technology law, media law and litigation. He has made several contributions to German law journals.



Alexander Stolz is an associate specialising in copyright, patent law, trade mark law, information technology law, media law and litigation. He has made several contributions to German law journals.

SZA Schilling, Zutt & Anschütz

Otto-Beck-Strasse 11
D-68165 Mannheim

Tel: +49 621 4257 247
Fax: +49 621 4257 286
Email: thomas.naegele@sza.de
Web: www.sza.de

SZA
SCHILLING, ZUTT & ANSCHÜTZ

JAPAN

Law and Practice

Contributed by:
Madoka Shimada, Toshihiko Hamano and Nobuhiro Tanaka
Nishimura & Asahi ***see p.109***

CONTENTS

1. LEGAL FRAMEWORK

1.1 Sources of Legal Protection for Trade Secrets

Definition of the term "trade secret" is provided in the Unfair Competition Prevention Act (UCPA), which has covered trade secrets since 1990; they were previously protected by general tort law. The protection of trade secrets by the UCPA is characterised so as to ratify the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS, which Japan joined in 1995, based on negotiations that were conducted beginning in 1987), which establishes the minimum standards for the protection of trade secrets by its members. The protection of trade secrets has been further strengthened by many amendments of the UCPA.

1.2 What Is Protectable as a Trade Secret

"Trade secret" means technical or business information that is:

- kept secret (secrecy management);
- useful for business activities – eg, methods of manufacturing or marketing (usefulness); and
- not publicly known (non-public domain).

Trade secrets can be protected by civil and criminal measures under the UCPA.

If a trade secret is infringed (Articles 2 (1) 4 to 10 of the UCPA), a claim for an injunction, a claim for damages and a request to take necessary measures to restore a business reputation can be made, collectively.

Persons who commit an infringement of trade secrets (Article 21 (1) of the UCPA) will be punished by imprisonment with required labour for not more than ten years or a fine of not more than JPY20 million, or both.

1.3 Examples of Trade Secrets

Trade secrets are divided into two types of information: technical information and business information.

Typical examples of technical information are manufacturing technology, manufacturing device design drawing, experimental data, research reports, inspection methods, CAD (computer-aided design) data, and so on.

Typical examples of business information are customer lists, "vendor and supplier lists", material purchase prices, costs, sales amounts, suppliers, personal information, and so on.

The infringement of trade secrets outside Japan is also protected by the UCPA if the trade secrets are owned by a company outside Japan that is also doing business in Japan.

1.4 Elements of Trade Secret Protection

Trade secrets are defined as technical or business information that is:

- kept secret (secrecy management);
- useful for business activities – eg, methods of manufacturing or marketing (usefulness); and
- not publicly known (non-public domain).

For the requirement of "secrecy management" to be satisfied, it is necessary for the corporation or entity that owns the trade secret to inform its employees of its intention to manage its secrets by means of rational and economically feasible secrecy management measures according to the specific circumstances of the given case, thereby allowing the employees to easily discern the company's intention to manage the secrets. However, it is not appropriate to require a specific corporation to implement high degrees of security measures regarding a piece of information in order to receive legal protection for its trade secrets under the UCPA.

The requirement of "usefulness" aims mainly to protect information that is recognised as "commercially valuable" in a broad sense, and to exclude information regarding violations of public welfare and morality (eg, information about tax evasion, careless release of harmful substances, and other antisocial conduct). Therefore, almost all types of information meet the requirement of "usefulness".

The requirement of "non-public domain" refers to a state where the relevant trade secret is not generally known, or a state where the secret is not easily discovered. The non-public domain requirement for trade secrets is not interpreted in the same manner as "inventions that were publicly known" (Article 29 of the Patent Act). In the interpretation of the Patent Act, any information can be in the public domain if the relevant person has no obligation to keep it confidential, even if only specific persons know the relevant information. Trade secrets that are not publicly known may be considered to be not in the public domain if the information is only known by specific persons who keep it confidential.

1.5 Reasonable Measures

There is no requirement for a trade secret owner to show that it took reasonable measures to protect its trade secrets.

However, the owner has to show that the information was treated in a manner that fulfils the requirement of "secrecy management". Therefore, the owner has to show that the information was kept confidential by adequate secrecy management measures. The required levels of specific security measures vary with the size and business style of specific corporations, the responsibilities of the employees, the nature of the information, and other circumstances.

1.6 Disclosure to Employees

Generally, the disclosure of a trade secret to employees has no effect on the availability of protection for the trade secret, because employees have a duty of confidentiality under their employment contracts.

The disclosure to other employees, without limitations, ofinformation that was accessible only to a specific employee may result in a ruling that the company failed to comply with the requirement for secrecy management.

1.7 Independent Discovery

Independent discovery or reverse engineering do not have an effect on the existence of trade secret protection, as long as the trade secret is kept secret and is not publicly known. If the information is easily discovered through reverse engineering, it may seem that the information was not (kept) secret.

1.8 Computer Software and Technology

There are no special protections for trade secrets that are unique to computers and/or technology. Computer software and/or technology are treated the same as other forms of trade secrets.

1.9 Duration of Protection for Trade Secrets

There is no limitation on the duration of protection for trade secrets; information is protected as a trade secret for as long as it qualifies under the definition of "trade secret". Disclosure (including controlled disclosure) of trade secrets does not have any effect on the existence of trade secret protections, as long as the trade secret is kept secret and is not publicly known. When disclosing trade secrets, owners of those trade secrets should impose a duty of confidentiality on those who receive the trade secrets; otherwise, disclosure of the information may result in a failure to comply with the requirement of secrecy management.

1.10 Licensing

A trade secret owner has the right to license the trade secret. Licensing does not have any effect on the existence of trade secrecy, as long as the trade secret is kept secret and is not publicly known. There is no statutory requirement for a trade secret owner to maintain the trade secret where the owner has granted a licence to use the trade secret. In practice, the licensor imposes a duty of confidentiality on the licensee, requiring the information to be kept secret and not become publicly known.

1.11 What Differentiates Trade Secrets from Other IP Rights

There is no registration system for trade secrets. However, patents, utility model rights, design rights, trade marks, layout-design exploitation rights and plant breeder's rights are protected through registration under the Patent Act, the Utility Model Act, the Design Right Act, the Trademark Act, the Act on the Circuit Layout of Semiconductor Integrated Circuits and the Plant Variety Protection and Seed Act. A registration process is available for copyrights but only on limited grounds, and no registration is necessary under the Copyright Act.

In Japan, "data for limited provision" has also been protected as intellectual property since July 2019. Data for limited provision means technical or business information that is accumulated or managed in significant volume by electronic or magnetic means as information provided to certain persons (such as a business) on a regular basis. It does not cover data that constitutes a trade secret or is provided to non-specified persons free of charge (Article 2 (7) of the UCPA). There is no registration system for data for limited provision.

Trade secrets and data for limited provision are protected from acts of wrongful acquisition, disclosure and use, and a subsequent acquirer can also be penalised for those acts (Articles 2 (1) 4 to 16 of the UCPA). A subsequent acquirer who, due to a serious mistake, was not aware that wrongful acquisition or similar actions were involved in the subsequent acquisition can be penalised for wrongful acquisition or similar actions with regard to trade secrets, but not with regard to data for limited provision.

Trade secrets and data for limited provision are not disclosed to the public.

However, patents, utility model rights, design rights, trade marks, layout-design exploitation rights and plant breeder's rights are disclosed through the registration process.

Copyright has no compulsory disclosure system.

There is no definition of or limitation on the duration of protection for trade secrets and data for limited provision; information is protected as a trade secret or as data for limited provision as long as it qualifies under the definition of "trade secret" or "data for limited provision".

A patent right is effective upon registration, and expires 20 years after the application filing date.

A utility model right is effective upon registration, and expires ten years after the application filing date.

A design right expires 20 years after the date of its registration.

Registered trade mark protection expires ten years after the date of registration, and the registration can be renewed for additional periods of ten years, repeatedly.

In principle, copyright protection commences automatically upon creation of the work, and

continues for 70 years after the death of the author.

A layout-design exploitation right expires ten years after the date of its registration.

A plant breeder's right expires 25 years after the date of its registration (30 years for a perennial plant).

1.12 Overlapping IP Rights

A plaintiff may assert trade secret rights in combination with other intellectual property rights, such as copyrights, as long as the elements for the protection of trade secrets are still met. However, there are very few cases in which trade secrets overlap with other intellectual property rights.

1.13 Other Legal Theories

It is possible to bring claims relating to trade secrets that do not turn on misappropriation. For example, it is possible to bring claims that someone incited the perpetrator's misappropriation or that someone acted as an accessory to the perpetrator (Article 719(2) Civil Code). In addition, it is possible to bring a claim for tortious interference (Article 709 Civil Code) if, for example, a defendant has induced an employee to breach a contractual confidentiality obligation to the owner of the trade secrets.

1.14 Criminal Liability

Criminal penalties for trade secret misappropriation in Japan were introduced by the 2003 amendment of the UCPA. Under the UCPA, trade secret misappropriation is a criminal offence that could result in imprisonment with labour as well as criminal fines that can be levied on individuals found guilty of trade secret misappropriation. Under Articles 21 and 22 of the UCPA, criminal penalties will be imposed on individuals as well as the corporations to which they belong.

Trade secret owners can pursue both civil and criminal liability at the same time. As explained in detail in **9. Criminal Offences**, it is common for a victim to consult with the police to commence a criminal investigation and obtain necessary evidence from the criminal files to use as evidence in a civil case.

The possible penalties include imprisonment with labour for not more than ten years or a fine of not more than JPY20 million, or both, for an individual, and a fine of not more than JPY500 million for the corporation to which the individual belongs. If trade secret misappropriation is conducted for the purpose of using trade secrets outside Japan, the criminal fines will be higher. For more details, please see **9. Criminal Offences**.

1.15 Extraterritoriality

Japanese courts have jurisdiction over an action that is brought against a person domiciled in Japan and/or a corporation or any other association or foundation whose principal office or business office is located in Japan, regardless of the type of case (Article 3-2 of the Code of Civil Procedure).

Therefore, it is possible to bring a claim in Japan based on misappropriation that occurs in another country if the defendant is a person, corporation, association or foundation that is domiciled in Japan.

In addition, Japanese courts have jurisdiction over tort claims for torts that take place in Japan and for those that take place outside of Japan but whose results arise in Japan, unless the occurrence of those results in Japan are ordinarily unforeseeable (Article 3-3, Item 8 of the Code of Civil Procedure). Misappropriation of trade secrets is considered a tort under Japanese law, and the place where a tort takes place legally includes both the place where the tor-

tious act was committed and the place where the result of that act arose.

Therefore, it is possible to bring a claim in Japan based on misappropriation that occurs in another country if the result of (ie, damages incurred from) the misappropriation arises in Japan and is not ordinarily unforeseeable.

2. MISAPPROPRIATION OF TRADE SECRETS

2.1 The Definition of Misappropriation

Trade secrets are protected against acts of wrongful acquisition, disclosure and use (Article 2 (1) 4-10 of the UCPA). If the owner of a trade secret asserts wrongful use, they must be able to show that the trade secret was actually used by the defendant.

There are two types of misappropriation. One involves the unauthorised acquisition set forth in Article 2 (1) 4, and the other involves significant violations of the principle of good faith set forth in Article 2 (1) 7. If the owner claims misappropriation based on Article 2 (1) 4, they have to prove that the acquisition was unauthorised, such as by theft, fraud, duress or other wrongful means. If a plaintiff verified the defendant's wrongful acquisition (prescribed in Article 2 (1) 4, 5, 8) of a certain technical trade secret and the defendant's production, et al, of the object or other thing produced by using the technical trade secret, then the defendant is presumed to have conducted production, et al, as a wrongful use (prescribed in Article 2 (1) 4, 5, 8) of the technical trade secret (Article 5-2).

2.2 Employee Relationships

The elements of a trade secret misappropriation claim do not differ if the misappropriation involves an employee of the owner. There is no specific statutory obligation for an employee to protect the trade secrets of his/her employer; however, generally speaking, an employee has a duty of confidentiality included in his or her employment contract or in the employer's Work Rules, which are the contractual rules that employees must observe.

2.3 Joint Ventures

In Japan, there is no special obligation between joint venture parties with respect to trade secrets. In practice, a licensor generally imposes a duty of confidentiality on licensees with regard to the information being kept secret and not becoming publicly known.

2.4 Industrial Espionage

In Japan, there are no special laws or claims that are unique to industrial espionage, unlike other jurisdictions such as the USA or Korea. However, a heavier statutory penalty is imposed on certain offences, including intentional misappropriation of trade secrets overseas, as described in Article 21 (3) of the UCPA.

3. PREVENTING TRADE SECRET MISAPPROPRIATION

3.1 Best Practices for Safeguarding Trade Secrets

In 2015, the Ministry of Economy, Trade and Industry (METI) published the Handbook for Protecting Confidential Information (the Handbook), which described "best practices" for safeguarding trade secrets. The Handbook provides guidance with regard to defining "Confidential Information" or trade secrets, how to prevent leakage of trade secrets, and how to deal with a possible misappropriation of trade secrets. For example, according to the Handbook, when considering measures to prevent leakage of trade secrets, it is important to note how to restrict access to the information, how to make it difficult to remove

or reveal the information, how to create a visible environment, how to improve employees' understanding of confidential information, etc. The Handbook further describes the recommended measures to be taken to prevent being accused of infringement of other's trade secrets, in particular when you accept new employees from another company (see **4.2 New Employees**) and when you develop new technologies independently from other's trade secrets.

The best practices described in this Handbook do not explicitly differ across industries or depending on the nature of the trade secrets, although the Handbook identifies ways that technical information (eg, chemical formulas, mechanical designs, technical manuals) and non-technical information (eg, customer lists, price lists, sales know-how) could be treated differently.

3.2 Exit Interviews

In exit interviews, departing employees are often asked to provide written assurances with respect to maintaining the confidentiality of information they obtained during their work, in addition to the Work Rules that are applicable to existing employees, which often include confidentiality clauses. Departing employees are also requested to return or delete any documents or media containing the company's confidential information. It is not very common for employers to ask departing employees about the nature of the new position that they will take, and there is no obligation for departing employees to disclose their new jobs or positions. In addition, in some cases, non-competition agreements may be considered, although the effectiveness of non-competition obligations is strictly examined if argued before a Japanese Court (see **4.1 Pre-existing Skills and Expertise**).

4. SAFEGUARDING AGAINST ALLEGATIONS OF TRADE SECRET MISAPPROPRIATION

4.1 Pre-existing Skills and Expertise

In Japan, protectable trade secrets are information that meets three conditions:

- the information is kept confidential;
- the information is useful for business activities; and
- the information is not publicly known.

If these conditions are met, an employee's personal knowledge and skills – if not recorded in writing or shared with others – can be protected as trade secrets. Thus, theoretically speaking, there is no particular distinction between an employee's general knowledge and skills and protectable trade secrets. In practice, protectable trade secrets should be stored on physical media, such as hard copy documents and data, since it is easier to prove infringement if an employee wrongfully acquires trade secrets stored on such media.

The doctrine of "inevitable disclosure" is not explicitly recognised in Japan. It is difficult for a court to issue an injunction against an employee transferring to another company in order to prevent an inevitable disclosure of trade secrets because the employee is entitled to freedom of choice in his or her employment. In many cases, non-competition clauses in written assurances entered into with departing employees are controversial, and Japanese courts generally take a strict stance against restricting employees' freedom of choice in employment. In many cases, non-competition clauses with an effective period of more than one year and/or without any remedy are deemed to be null and void.

4.2 New Employees

The best practices that employers in Japan use when hiring employees from competitors are as follows:

- before the individuals are hired – confirming the contractual restrictions imposed on the individuals by their previous employers;
- during the on-boarding process – obtaining written assurances from the employees to ensure that they have not brought with them any confidential information that belongs to previous employers or third parties, and that the employees will not use any confidential information belonging to previous employers in their work for their new employers; and
- after the new employees start work at their new places of employment – the employers check the employees' work periodically to ensure that they are not using confidential information belonging to previous employers.

These approaches are useful in proving that the new employers did not exercise gross negligence in their hiring process if they become subject to trade secret misappropriation claims.

5. TRADE SECRET LITIGATION

5.1 Prerequisites to Filing a Lawsuit

In Japan, filing a written complaint with the relevant court is sufficient; no prerequisites or preliminary steps are required before filing a trade secret civil lawsuit. No mediation or ADR procedure is necessary in Japan.

5.2 Limitations Period

Under Article 15(1) of the UCPA and Article 724 of the Civil Code, there are two applicable statutes of limitations. First, an owner must exercise its right to seek an injunction/damages within three years from the time they become aware of the infringement. In addition, the owner must exercise its right to seek an injunction/damages within 20 years of the commencement of the infringement. In principle, the owner needs to take formal legal action (such as filing a lawsuit) within these periods.

5.3 Initiating a Lawsuit

An owner must submit a written complaint to one of the courts that has jurisdiction, including relevant facts to support their claim. The owner needs to identify the trade secret in dispute, though precise identification at the initial stage is sometimes very difficult.

5.4 Jurisdiction of the Courts

Unlike patent litigation, there is no exclusive jurisdiction clause in the Code of Civil Procedure for trade secret litigation; the owner can choose from wherever the Code of Civil Procedure stipulates. The relevant jurisdictions include the place of the defendant's residence, the place of the infringement and the place of performance of the obligation. The Code also provides additional special jurisdictions in case of trade secret litigation either in the Tokyo District Court or the Osaka District Court, depending on the location of the original jurisdiction. The Tokyo District Court and the Osaka District Court have special divisions that focus on intellectual property rights, including trade secret rights.

5.5 Initial Pleading Standards

In Japan, there is no notion of "initial pleading standards". However, the owner bears the burden of proof under the high probability doctrine and needs to collect and present evidence by itself, as there is no US-type discovery system in Japan. Although the owner can collect and supplement evidence through evidence collection systems such as document production orders, the owner needs to allege facts with evidence to convince the judges to proceed with the litigation and to allow the use of some evidence

collection systems. No particularity standard is applicable to trade secret claims.

5.6 Seizure Mechanisms

In Japan, unlike in the United States, there are no mechanisms available for seizing accused products or other evidence ex parte. Seizure is available through preliminary injunctions or permanent injunctions, which are not ex parte proceedings. Seizure orders can be issued together with injunctive orders. Owners of trade secrets need to prove the necessity of seizure orders together with the requirements for injunctive relief. As explained in **7.1 Preliminary Injunctive Relief**, the bar for seizure orders at the time of preliminary injunctions (before a final judgment) is said to be very high, as judges tend to regard preliminary injunctions against sales as being sufficient at such an early stage.

5.7 Obtaining Information and Evidence

In Japan, there is no US-type discovery system and the owner needs to collect evidence by itself to support its allegation. In principle, the owner needs to provide sufficient facts and evidence during the court proceedings, but not necessarily completely at the time of the filing. At the initial stage, the owner normally needs to gather circumstantial evidence through collaborators. The owner can also use the "preservation of evidence" system under the Code of Civil Procedure to gather evidence, even before filing a civil lawsuit. Also, if there is a relevant criminal case, it is possible for the owner to gather criminal records to support its allegation through the so-called "commission to send document system" during the lawsuit. Furthermore, a court can issue a document production order to the defendant to have it submit internal documents to support trade secret misappropriation (Article 7 of the UCPA), though Japanese document production orders are a much more specific and narrow request compared to US-type discovery.

5.8 Maintaining Secrecy While Litigating

Civil litigation hearings should be open to the public, but because of sensitivity in trade secret cases, courts frequently use preparatory hearings, which are private proceedings, so that third parties cannot access the trade secrets in dispute. The litigation record should also be open to the public in principle, but the owner can file a motion to seal to prevent third parties from accessing the trade secrets at issue. The seal is valid even after the case ends. The owner can also file a motion to seal in judicial fact-gathering or evidence-gathering cases.

In relation to the opposing party, the owner can request a protective order when they need to disclose their trade secrets to the other party in the course of litigation so that the opposing party cannot use those trade secrets for any purpose other than the litigation. A protective order can also limit the scope of recipients who can receive the trade secrets. However, as a protective order is not so flexible, it is also practical to execute a confidentiality agreement between the parties.

5.9 Defending against Allegations of Misappropriation

Defences depend on the case and the identity of the defendant, but it is very common to attack the basic requirements of a trade secret – ie, that it is kept secret, that it is non-public and that it is useful. It is also common to argue that the plaintiff has not specified what the trade secret is. If the defendant is an indirect recipient of a trade secret, it is also possible to argue that the defendant did not have any knowledge of and was not grossly negligent in failing to know of the illegal disclosure. As the Code of Civil Procedure does not have a US-type discovery system, it is also common to point out that the plaintiff has not sufficiently proven its allegation, given that the plaintiff owes the burden of proof, though the

plaintiff can supplement its evidence through the evidence collection systems.

5.10 Dispositive Motions

There is no US-type dispositive motion system in Japan (such as motions to dismiss with prejudice or motions for summary judgment). However, a court can end a case earlier and issue a judgment if appropriate, when it considers that it has no jurisdiction over the case, for example.

5.11 Cost of Litigation

Litigation costs depend on various circumstances, so it is very difficult to provide an estimate thereof. In general, however, because there is no US-type discovery in Japan, litigation costs are much lower than in the USA. Court costs such as filing fees and travel expenses of witnesses should be paid by the losing party, in principle. Attorneys' fees should be paid by each party, but it is possible to include some attorneys' fees in the damages to be compensated. Contingency litigation is a recognised concept in Japan, though it is not popular in practice. Litigation financing is not prohibited in Japan but is still very uncommon, partly because of the lack of clear rules and lower litigation costs in Japan.

6. TRIAL

6.1 Bench or Jury Trial

There is no civil jury system in Japan. All cases are decided by professional judges, including trade secret cases.

6.2 Trial Process

As there is no civil jury system in Japan, there are no clear distinctions between trial processes. During the entire litigation, judges examine facts and evidence, and intensive examination of witnesses and parties is conducted after the issues are identified. There is no hearsay rule in Japanese civil litigation, so theoretically the judges can decide based on documents/evidence. Judges scrutinise what each side argues on paper and what the written evidence stipulates. If there is a disagreement over facts, each party calls its live witnesses and the judges hear testimony. In practice, each party's argument is presented by written briefs, not by oral arguments. The length of a trial or the intensive examination period largely depends on each case, but trade secret cases tend to take longer than normal commercial disputes because of the complex issues involved. In Japan, most cases are settled before judgment.

6.3 Use of Expert Witnesses

Expert witnesses are used in Japan, but the parties provide the expert opinions in written form first and later call the experts as witnesses. Expert witnesses will be examined through direct and cross-examination. No specific rules or guidelines exist in relation to expert testimony. The cost largely depends on each case, but generally tends to be lower than in the USA.

7. REMEDIES

7.1 Preliminary Injunctive Relief

Preliminary injunctive relief is available in Japan, based on the Civil Provisional Remedies Act. In addition to the requirements in the main proceedings, the owner must prove substantial detriment or imminent danger relating to trade secret infringement. The preliminary injunctive relief lasts until the judgment in the main proceedings. The owner normally needs to place a bond in advance of the court's order. The amount of the bond is decided based on various factors, including the scale of the business and the impact of the preliminary injunction.

7.2 Measures of Damages

There is no restriction on damages, as long as the owner proves legally sufficient cause between

the infringer's intentional act or negligence and the damage suffered by the owner (Article 4 of the UCPA). As it is very difficult to prove the exact amount of damages in trade secret cases, Article 5 of the UCPA basically stipulates the following three presumptions for damages and the owner can choose the presumption:

- the amount obtained by multiplying the infringer's assigned quantity by the amount of the owner's profit per unit;
- the profits obtained by the infringer; and
- the amount of the licensing fee.

The owner can seek additional damages beyond the amount of the aforementioned presumption, such as some attorneys' fees and research fees. Punitive damages are not available in Japan.

7.3 Permanent Injunction

Permanent injunctive relief is available in Japan. The claimant can obtain an order to destroy the accused products, but the order is only enforceable to the extent the claimant still has ownership. The claimant cannot request an order requiring a recall. Also, it is not normally possible to obtain an order that limits an employee's subsequent employment, unless the employee agrees to a duty not to compete in advance. There are no limitations on the duration of a permanent injunction, as long as the claimant files within the statutory limitation period mentioned in **5.2 Limitations Period**.

7.4 Attorneys' Fees

In trade secret cases, plaintiffs can recover some attorneys' fees as part of the owner's damages, as long as they have legally sufficient cause with the infringement. The judges decide the amount of attorneys' fees that should be recovered in the judgment on the litigation. No separate process for recovering attorneys' fees is needed.

7.5 Costs

In principle, court costs such as filing fees and witnesses' fees and their travel expenses should be paid by the losing party, but judges can decide who should bear the court costs in their final judgment on the main case and the amount to be owed. Attorneys' fees are not included in court costs, but the claimant can seek them as a part of the damages. No separate process is needed.

8. APPEAL

8.1 Appellate Procedure

With regard to the process of appealing a judgment, the losing party must submit a written petition of appeal to the original court where the original judgment was issued within two weeks from the date when service of the judgment is received. Both claimants and respondents can appeal, as long as at least part of their claims are denied in the judgment. The length of the appeal process depends on each case, but it tends to be shorter than the first instance process as the appeals courts need only one hearing in most cases.

Only a final judgment is eligible for appeal, but in the appeal process the appellant can contest the original court's intermediate judgment or decisions that do not allow independent appeals.

As Japan adopts a nationwide, uniform judicial system, there is no significant difference between each high court with regard to the appeal process.

8.2 Factual or Legal Review

The appeals courts review both factual and legal issues. As the appeals courts are still regarded as consecutive fact-finding proceedings, they review cases de novo, though the scope of review is limited to what the appellant dis-

putes in the petition of appeal. Also, the appeals courts have discretion to reject new evidence/arguments if the parties have failed to submit them in a timely manner. The parties can agree not to appeal prior to obtaining a judgment, as long as both parties agree in writing. The parties can agree not to appeal while retaining a "leap appeal" right to the Supreme Court for legal issues prior to judgment. Unless the parties agree as stated above, they can reserve their right to appeal any matter, but need to include the issues in the petition of appeal. The parties must submit an appeal within two weeks of the date when service of the original judgment is received. The appeals courts can conduct two or more hearings, including a new examination of witnesses, but in most cases they conduct only one hearing before judgment and decide based on the papers, including the litigation records from the original court.

9. CRIMINAL OFFENCES

9.1 Prosecution Process, Penalties and Defences

Prior to 2016, initiating criminal proceedings required an accusation by the victim, because it was thought that the decision of whether trade secret infringement should be tried in court should be left to the victim. Now, no accusation by the victim is required and the prosecutor's office can issue an indictment at its own discretion. In practice, however, the victim should first consult with the police regarding possible infringement of its trade secrets. Once a case is initiated, the police may conduct a dawn raid to investigate, and a prosecutor will issue an indictment. The case will then be sent to court (the right to a jury trial is not applicable to the crimes of trade secret misappropriation). There are special rules for protecting the confidentiality of trade secrets at issue during criminal proceedings in court.

With regard to potential penalties, Article 21 of the UCPA provides that a person who acquires, uses or discloses trade secrets through an act of fraud, etc, or through the usurpation of management for the purpose of obtaining a wrongful gain or causing damage to the owner of the trade secrets, or a person who obtains trade secrets in breach of the legal duties regarding management of the trade secrets, will be punished by imprisonment with labour for not more than ten years or a fine of not more than JPY20 million, or both. Also, a person who – for the purpose of obtaining a wrongful gain or causing damage to the owner of trade secrets – assigns, delivers, displays for the purpose of transfer or delivery, exports, imports or provides through a telecommunications line things created through trade secret infringement (excluding a person who has received the things by transfer without knowing that the things were created by an act of illegal use) will also be punished by imprisonment with labour for not more than ten years or a fine of not more than JPY20 million, or both.

The corporation to which the person who conducted such trade secret misappropriation belongs will be punished by a fine of not more than JPY500 million, levied in addition to the fine imposed on the individual (Article 22 of the UCPA).

If those actions are conducted for the purpose of using trade secrets outside Japan, the criminal fines will be higher:

- for an individual, a criminal fine of not more than JPY30 million;
- for a corporation, a criminal fine of not more than JPY1 billion.

An (ultimately unsuccessful) attempt of trade secret misappropriation can result in criminal sanctions. In addition, the distribution of products that were manufactured by using misap-

propriated trade secrets can result in criminal sanctions and civil remedies.

Prior to 2016, wrongful acquisition of a trade secret outside Japan would not have resulted in criminal liability in Japan; only wrongful use or disclosure outside Japan would have potentially triggered criminal sanctions in Japan. This limitation has since been removed from the law, and wrongful acquisition of a trade secret outside Japan has been added as grounds for criminal sanctions.

In order to be criminally liable, the violator must have "the purpose of obtaining a wrongful gain or causing damage to the owner of the trade secrets" in conducting misappropriation. Therefore, possible defences against a criminal charge for theft of trade secrets include lack of the purpose of obtaining a wrongful gain or causing damage to the owner of the trade secrets. Also, if the violator does not have the intent to acquire, disclose or use trade secrets, he/she cannot be criminally liable. Such defences could differ from the defences available in a civil case because, in a civil case, there is no need to prove "the purpose of obtaining a wrongful gain or causing damage to the owner of the trade secrets", and the violator can be civilly liable even if he/she does not have the intent to acquire, disclose or use trade secrets, if he/she is grossly negligent in doing so.

In the past, criminal sanctions for trade secret misappropriation were not actively used in Japan. As the standard of proof required to make a criminal case is higher than that for a civil case (it needs to be "beyond a reasonable doubt"), there was a tendency for prosecutors to be reluctant to actually indict cases. Due to multiple amendments of the UCPA to increase the number of criminal cases, including expansion of the coverage of criminal offences and the introduction of measures to protect confidentiality of trade secrets in criminal courts, criminal investigations are now being used more frequently than before. Many of the recent civil cases involve criminal cases being investigated concurrently or previously.

It is a typical approach for a victim to consult with the police to start a criminal investigation and obtain necessary evidence from the files of the criminal case, which will be used as the plaintiff's evidence in a civil case. Although there is no particular law regarding economic espionage, a victim should take the same approach as above in pursuing criminal sanctions as well as civil damages/injunctions against a violator in case of economic espionage.

10. ALTERNATIVE DISPUTE RESOLUTION

10.1 Dispute Resolution Mechanisms

In Japan, there is no specific alternative dispute resolution mechanism designed for trade secret disputes. For general intellectual property disputes, the "Intellectual Property ADR" system is available but it is still in a preliminary stage, and it is not clear whether trade secrets disputes have been resolved through Intellectual Property ADR.

In Japan, more generally, the Japan Commercial Arbitration Association offers an arbitration mechanism, which is often used in international/domestic commercial disputes. As far as is known, however, it is not very common to use such arbitration forum to resolve trade secret disputes in Japan. This may be because, as a forum to resolve trade secret disputes, the intellectual property division of the Tokyo/Osaka District Court and the Intellectual Property High Court in Tokyo have ample experience in trade secrets disputes as well as other forms of intellectual property cases. It is also possible to use

various measures to protect the confidentiality of trade secrets in court proceedings, such as protective orders and orders to keep litigation files confidential from any third parties; thus, there is no particular need for alternative dispute resolution mechanisms to protect the confidentiality of trade secrets at issue.

Nishimura & Asahi is Japan's largest law firm, covering all aspects of domestic and international business and corporate activity. The firm has more than 600 Japanese and foreign lawyers, and employs over 700 support staff, including licensed tax counsel and patent attorneys. Since 2010, it has opened offices in various Asian countries and in the USA, the Middle East and Europe. As experts in international law, Nishimura & Asahi has also created a network covering many countries in Europe, the United States and beyond. The firm represents companies in major civil and criminal cross-border trade secret litigation in Japan, including several leading trade secret misappropriation cases, such as the Nippon Steel-POSCO and Toshiba-SK Hynix cases. Through the enhancement of professional and organisational synergies resulting from the firm's expansion, an unprecedented level of client service is made possible in highly specialised and complex areas of commercial and corporate law, including intellectual property practice.

AUTHORS

Madoka Shimada is a partner at Nishimura & Asahi. She advises clients on various matters of competition law, and is especially active in cross-border cases. She also advises in the area of unfair competition prevention, particularly on trade secret misappropriation cases, including the investigation thereof and large cross-border litigation. Madoka graduated from the University of Tokyo (LLB) in 1997 and earned an LLM from Harvard Law School and an MPA from Kennedy School of Government, Harvard University, in 2003. She has been admitted as an attorney in Japan since 1999 and in New York since 2005.

Toshihiko Hamano is a counsel at Nishimura & Asahi and advises clients on various matters of intellectual property law and technology, including IP litigation (especially trade secret litigation), patents, trade secrets, copyrights, cross-border transactions, artificial intelligence (AI), information technology, data protection and data security. He has a technical background in electronics, and he mainly studied neural networks, which are fundamental technologies for AI. Toshihiko graduated from the University of Tokyo Graduate School of Frontier Sciences (MS) in 2004 and from Waseda Law School (JD) in 2007, and has been admitted as an attorney in Japan since 2008.

Nobuhiro Tanaka is a senior associate at Nishimura & Asahi and handles a broad range of cross-border dispute cases, especially trade secret and antitrust cases. He also handles merger filing and white-collar crimes. Nobuhiro graduated from the University of Tokyo (LLB) in 2007, the University of Tokyo School of Law (JD) in 2009 and Stanford Law School (LLM) in 2017. He was seconded to Paul, Weiss Rifkind, Wharton & Garrison LLP in New York from 2017 to 2018, and has been admitted as an attorney in Japan since 2010 and in New York since 2018.

Nishimura & Asahi

Otemon Tower
1-1-2 Otemachi
Chiyoda-ku
Tokyo
100-8124
Japan

Tel: +81 3 6250 6200
Fax: +81 3 6250 7200
Email: m.shimada@nishimura.com
Web: www.nishimura.com/en/offices/tokyo.html

MALAYSIA

Law and Practice

Contributed by:
Bahari Yeow, Lim Zhi Jian and Alex Choo
Gan Partnership see p.132

CONTENTS

1. LEGAL FRAMEWORK

1.1 Sources of Legal Protection for Trade Secrets

In Malaysia, the most important source of law is the Federal Constitution, the State Constitutions, legislation and subsidiary legislation. Case law is also an important body of law, and plays a pivotal role in providing the requisite guidelines on trade secret and confidentiality protection.

1.2 What Is Protectable as a Trade Secret

The principle propounded by Megarry J in Coco v A.N. Clark (Engineers) Ltd. [1969] RPC 41 is deeply entrenched in Malaysian jurisprudence. Very briefly, as long as the information sought to be protected has the necessary quality of confidence, it will be guarded by law in Malaysia.

In Lionex (M) Sdn Bhd v Allen Lim Lai Wah [2016] 1 LNS 1799, Lau Bee Lan J (as her Ladyship then was) held that what is confidential is a question of fact in each case. The relevant factors to be considered in deciding whether the information sought has the necessary quality of confidence include:

- whether skill and effort were expended to acquire the information;
- whether the information is jealously guarded by the employer, is not readily made available to employees and could not, be acquired by others without considerable effort and/or risk;
- whether it was plainly made known to the employee that the material was regarded by the employer as confidential;
- whether the usages and practices of the industry support the assertion of confidentiality; and
- whether the employee in question has been permitted to share the information only by reason of his or her seniority or high responsibility within the employer's organisation.

These factors merely illustrate the approaches adopted by the courts in earlier cases where claims were made for the protection of trade secrets or confidential information. What constitutes a trade secret varies from industry to industry.

Information that enters the public domain, or that is useless or trivial, may not possess the necessary quality of confidence for protection.

If the information is partly public and partly private, it does not take away the confidential nature thereof. In Lionex (supra), the court adopted the "Springboard doctrine" propounded in the English Court of Appeal case of Seager v Copydex, Ltd. [1967] 2 All ER 415: "When the information is mixed, being partly public and partly private, then the recipient must take special care to use only the material which is in the public domain. He should go to the public source and get it: or, at any rate, not be in a better position than if he had gone to the public source. He should not get a start over others by using the information which he received in confidence."

1.3 Examples of Trade Secrets

The following have been judicially recognised as being confidential in nature and considered trade secrets:

- information relating to cost prices, quoted prices, the specific needs and requirements of customers and suppliers, the status of all ongoing negotiations with customers, and price lists (Schmidt Scientific Sdn Bhd v Ong Han Suan & Others [1998] 1 CLJ 685);
- compilations of information and data on suppliers and customers and the individual contacts therein (Worldwide Rota Dies Sdn Bhd v Ronald Ong Cheow Joon [2010] 8 MLJ 297; Lionex (supra));
- internal marketing strategies;
- internal financial data and information;

- know-how and business strategy;
- customer lists or customer lists that are deliberately memorised by the employee with the intention of using them later;
- a list of names of suppliers and customers and the individual contracts (Lionex (supra));
- a list of prices negotiated with and quoted to various customers, the contents of various agreements, records of sales, requirements of customers (Certact Pte. Ltd. v Tang Siew Choy & Others [1991] 4 CLJ (Rep) 716); and
- stock listing on various locations as well as certification information (Lionex (supra)).

Trade secrets or information, as lucidly laid down by Lord Goff of Chieveley in Attorney-General v Observer Ltd. And Others, Attorney-General v Times Newspapers Ltd. And Another [1990] 1 A.C. 109, includes "certain situations, beloved of law teachers – where an obviously confidential document is wafted by an electric fan out of a window into a crowded street, or where an obviously confidential document, such as a private diary, is dropped in a public place, and is then picked up by a passer-by" (Worldwide Rota (supra)).

1.4 Elements of Trade Secret Protection

In order to succeed in an action for breach of confidence or trade secret, the plaintiff must prove that the documents and information were:

- of a confidential nature;
- communicated in circumstances importing an obligation of confidence; and
- used in an unauthorised way to the detriment of the plaintiff (China Road & Bridge Corporation & Another v DCX Technologies Sdn Bhd [2014] 7 CLJ 644; Coco (supra); Seven Seas Industries Sdn Bhd v Philips Electronic Supplies (M) Sdn Bhd & Another [2008] 4 CLJ 217; Lionex (supra)).

1.5 Reasonable Measures

The court will only lend its aid to provide protection if the document or information sought to be protected has the necessary quality of confidence.

Whilst the existence of reasonable measures may not be a prerequisite for a trade secret owner to enjoy protection of its trade secret, failure to take proper or reasonable measures may compromise the categorisation of the information sought to be protected.

For example, if particular information enters the public domain, it may prejudice the trade secret owner's action in court. Thus, it is always prudent to take reasonable measures to ensure that intangible assets and intellectual property are jealously guarded.

The higher the value of the trade secret, the more measures need to be taken, and less accessibility should be granted to employees or any third party.

It is good practice to make the confidential nature of the documents or information known to the employee (or recipient).

Whilst the protection of trade secrets does not depend on any contract, express or implied terms, or otherwise, and depending on the principle of equity (that he who has received information in confidence shall not take unfair advantage of it), when there is an agreement (eg, an employment agreement or a non-disclosure and confidential agreement) that clearly spells out the terms (which include restrictive covenants), this may elevate certain controversies at the time of disputes.

Other reasonable measures include:

- adopting a clear policy, including restricting disclosure and accessibility;
- implementing secure passwords and tailored "access profiles";
- where practicable, implementing the proper categorisation, marking and labelling of documents and information; and
- proper storage of documents and information.

1.6 Disclosure to Employees

In general, an employee owes the employer a duty of fidelity and good faith throughout their employment.

This duty of good faith or fidelity does not just require the employee to refrain from misusing or disclosing information whilst still in the employment; there is also an implied duty not to use any confidential information obtained during the employment, without the employer's consent, for the employee's own or someone else's use after the employment contract ends.

In Schmidt Scientific (supra) the court held that: "… it is a breach of the fidelity clause and the implied duty to remove a customer list or to deliberately set out to memorise the said list with the intention of using it later, even though any use or disclosure is confined to the post-employment period. In such a case the eventual exploitation of the information is considered to be no more than an extension of the original breach of good faith and fidelity."

In Robb v Green [1895] 2 QB 315 the Court of Appeal held that the employee was in breach of an implied term of the contract of service in making copies of his employer's list of customer names and addresses, with the intention of using it for the purpose of soliciting orders from them after he had left his employer's service and set up a similar business on his own account.

Lord Esher MR said: "… the question is whether such conduct was not what any person of ordinary honesty would look upon as dishonest conduct towards his employer and a dereliction from the duty which the defendant owed to his employer to act towards him with good faith. I think the judge was perfectly justified in holding that such conduct was a breach of the trust reposed in the defendant as the servant of the plaintiff in his business. The question arises whether such conduct is a breach of contract. That depends upon the question whether in a contract of service the court can imply a stipulation that the servant will act with good faith towards his master. In this case it is said that the contract of service was in writing; but there is nothing in the express terms of the contract that contradicts such an implication. I think that in a contract of service the court must imply such a stipulation as I have mentioned, because it is a thing which must necessarily have been in view of both parties when they entered into the contract."

The above has been accepted by the Malaysian courts in various decisions, including Lionex (supra) and Worldwide Rota (supra).

Notwithstanding the above, it is important to bear in mind that the plaintiff must establish to the satisfaction of the court the following three elements in order to succeed in an action for breach of confidence or trade secret:

- that the information the plaintiff is seeking to protect is of a confidential nature;
- that the information in question was communicated in circumstances importing an obligation of confidence; and

- that an unauthorised use of that information would be to the detriment of the party communicating it.

Whilst disclosure of a trade secret to employees may not, in general, directly affect the availability of protection for the trade secret, it is important for certain measures to be put in place so that the employer's rights are not compromised.

1.7 Independent Discovery

The fact that a product is sold in the market does not necessarily destroy the confidential information relating to how it is produced, even it is possible to discover the confidential information through reverse engineering. If, for example, substantial work is required to analyse a product and discover the confidential information on how saidproduct is produced, such information remains confidential.

However, the law on trade secrets is not intended to restrict anyone's ability to compete. The use of technological advances and innovations, including independent discovery or reverse engineering, may be acceptable in law. It will be potentially harmful to swing the pendulum by imposing a new form of servitude or serfdom.

When the information is partly public and partly private, the recipient must take special care to use only the material that is in the public domain. He or she should go to the public source and get it, or should at least not be in a better position than if he or she had gone to the public source. The recipient should not get a headstart over others by using the information they received in confidence (Seager (supra)).

1.8 Computer Software and Technology

Apart from trade secret protection, computer software and/or technology may be subject to protection through copyright, patent or trade marks.

The IP laws are important to accord protection to computer software and/or technology, particularly when the computer software and/or technology are developed for commercialisation.

Copyright

Literary work is eligible for copyright protection in Malaysia (Section 7(1)(a) of the Copyright Act 1987).

"Literary work" includes:

- tables or compilations, whether or not expressed in words, figures or symbols and whether or not in a visible form; and
- computer programs (Section 3 Copyright Act 1987).

"Computer program" means an expression, in any language, code or notation, of a set of instructions (whether with or without related information) intended to cause a device having an information processing capability to perform a particular function either directly or after either or both of the following:

- conversion to another language, code or notation;
- reproduction in a different material form (Section 3 of the Copyright Act 1987).

The works shall be protected irrespective of their quality and the purpose for which they were created as long as:

- sufficient effort has been expended to make the work original in character;
- the work has been written down, recorded or otherwise reduced to material form; and
- the author of the work is a "qualified person" under the Copyright Act 1987.

The owner of copyright in a literary work or a derivative work has the exclusive right to control

the following in Malaysia, regarding the whole work or a substantial part thereof, in either its original or derivative form:

- the reproduction in any material form;
- the communication to the public;
- the distribution of copies to the public by sale or other transfer of ownership; and
- the commercial rental to the public.

Patent

An invention is patentable if it is new, involves an inventive step and is industrially applicable (Section 11 of the Patents Act 1983).

An invention may be either a product or a process, and permits in practice the solution to a specific problem in the field of technology.

An invention is new if it is not anticipated by prior art (Section 14(1) of the Patents Act 1983).

Prior art consists of:

- everything disclosed to the public, anywhere in the world, by written publication, by oral disclosure, by use or in any other way, prior to the priority date of the patent application claiming the invention; and
- the contents of a domestic patent application having an earlier priority date than the patent application referred to above, to the extent that such contents are included in the patent granted on the basis of said domestic patent application.

An invention shall be considered as involving an inventive step if, having regard to any matter that forms part of the prior art, such inventive step would not have been obvious to a person that has ordinary skill in the art (Section 15 of the Patents Act 1983).

If the computer software and/or technology is new, involves an inventive step and is industrially applicable, it may qualify for protection under the law of patent in Malaysia.

The owner of a patent has the following exclusive rights in relation to the patent:

- to exploit the patented invention;
- to assign or transmit the patent; and
- to conclude licence contracts.

Trade Marks

Trade mark law accords certain protection for computer software and/or technology. Whilst it does not protect code or the contents of software, for example, it does protect the brand name and trade marks (including logos).

1.9 Duration of Protection for Trade Secrets

Duration

In Dynacast (Melaka) Sdn Bhd v Vision Cast Sdn Bhd [2016] 6 CLJ 176, the Federal Court affirmed the principle of law in Svenson Hair Center Sdn Bhd v Irene Chin Zee Ling [2008] 8 CLJ 386 that protection of confidential information and trade secret "does not have any time limits".

In coming up with such a proposition of law, the courts rationalised that a contrary view would mean that an ex-employee could exploit confidential information with impunity; they would just need to wait until the expiry of the restriction period. Such an outcome could not have been intended by any of the contracting parties as it would defeat the very purpose of having a confidentiality provision in an employment agreement.

The only caveat to be placed on this is the criteria set out in **1.4 Elements of Trade Secret Protection**.

Effect of Disclosure

The disclosure of trade secrets may or may not have an impact of the trade secret owner's rights.

For example, if a disclosure is made in a haphazard manner and results in the trade secret being widely circulated in the public domain, it may result in the document or information losing its confidential nature.

Thus, if the trade secret owner decides to disclose certain trade secrets to a third party or any person, it is crucial that the recipient is made aware that the trade secret was communicated in circumstances importing an obligation of confidence.

Accidental Disclosure

In general, an accidental disclosure does not ipso facto mean that the trade secret loses its confidential nature.

As rightly noted in Observer Ltd (supra), "where an obviously confidential document is wafted by an electric fan out of a window into a crowded street" or "where an obviously confidential document, such as a private diary, is dropped in a public place, and is then picked up by a passer-by", a duty of confidence may arise in equity independently of such cases to protect those trade secrets (Worldwide Rota (supra)).

However, it is important to take immediate steps to retrieve these trade secrets or prevent further disclosure of such information or to control the circulation of such information.

1.10 Licensing

As the proprietor of intangible assets and/or intellectual property, a trade secret owner certainly has rights, like any other proprietary right to grant any party a licence.

In order to maintain the value of the trade secret and not to allow the licensee to dilute the value, or harm the nature of the trade secret to the extent that it loses its "quality of confidence", it may be important for the parameter of use to be expressly spelt out in the agreement between the parties.

Certain measures and terms ought to be expressly provided, including the following:

- the ownership of the trade secret;
- the licensee's obligation to maintain confidence;
- the duration of such obligation – eg, "forever" and in perpetuity; and
- measures to be taken by the licensee, including:
  - (a) restricting disclosure and accessibility;
  - (b) proper storage of documents and information; and
  - (c) steps to be taken in the event of accidental disclosure.

1.11 What Differentiates Trade Secrets from Other IP Rights

Intellectual property includes copyrights, patents, industrial designs and trade marks.

The term "trade secret" speaks volume. Information or documents that have a quality of confidence ought to be jealously guarded and not made readily available or accessible to others in order for them to be "secret". The higher the value of the "secret", the more onerous the measures that should be taken to store those "secrets". For this obvious reason, there is no registration system, and no requirement for trade secrets to be registered in order to enjoy legal protection.

On the other hand, a registration mechanism is available for patents, industrial designs and trade marks. In particular, for patent and indus-

trial designs, the IP owner ought to file for registration prior to its disclosure to the public.

1.12 Overlapping IP Rights

Generally, there is no restriction on a plaintiff asserting trade secret rights in combination with other types of intellectual property rights. The only caveat is that it must fulfil the requirements of the respective branch of intellectual property.

By way of an example, a trade secret owner may claim for protection in tort to protect its trade secret, and at the same time sort protection under the law of copyright, provided, for example, that the necessary requirements for the subsistence of the copyright are met.

Category

The subject matter of the trade secret is one of the following:

- literary works;
- musical works;
- artistic works;
- films;
- sound recordings; or
- broadcasts.

Criteria

The following criteria must be met:

- sufficient effort has been expended to make the work original in character;
- the work has been written down, recorded or otherwise reduced to material form; and
- the trade secret does not merely consist of an idea, a procedure, a method of operation or a mathematical concept.

Author

The author of the work is a qualified person:

- a citizen of, or a permanent resident in, Malaysia; or
- a body corporate established in Malaysia and constituted or vested with legal personality under the laws of Malaysia.

1.13 Other Legal Theories

The third element the plaintiff is required to establish in an action for breach of confidence or trade secret is that the documents and information were used in an unauthorised way to the detriment of the plaintiff. Whilst "misappropriation" may complete the equation in a claim for breach of confidence, the element to be established is, in essence, "unauthorised use".

Like all cases, one need not put all one's egg into one basket. One may formulate a claim based on breach of statutory duty, breach of fiduciary duty or tortious claim, for example, based on unlawful interference of trade or unlawful interference of contract.

Breach of Statutory Duty

A director of a company shall at all times exercise his or her powers for a proper purpose and in good faith in the best interest of the company (Section 213(1) of the Companies Act 2016).

A director of a company shall exercise reasonable care, skill and diligence with:

- the knowledge, skill and experience that may reasonably be expected of a director that has the same responsibilities; and
- any additional knowledge, skill and experience held by the director (Section 213(2) of the Companies Act 2016).

Any breach of these duties may be an offence. The company may also initiate action against the director for breach of his or her statutory duties.

Breach of Fiduciary Duty

A fiduciary is someone who has undertaken to act for or on behalf of another in a particular

matter in circumstances that give rise to a relationship of trust and confidence (The Board of Trustees of the Sabah Foundation & Others v Datuk Syed Kechik Syed Mohamed & Another [2008] 3 CLJ 221).

For example, a director has three broad categories of duties: fiduciary duties, duties of skill, care and diligence, and statutory duties.

A director's main and overriding duty is to act in what he or she honestly considers to be the company's interests, and not in the interests of some other person or body.

A director must not place himself in a position where his or her duty to the company and his or her personal interests may conflict.

A director must employ the powers and assets that he or she is entrusted with for the purposes for which they were given, and not for any collateral purpose (Lionex (supra)).

When a director is disloyal, the principal is entitled to bring an action against the director for breach of fiduciary duties.

Unlawful Interference with Trade

Very briefly, the elements that constitute the tort of unlawful interference with trade or business are:

- interference with the plaintiff's trade or business;
- unlawful means;
- intention to injure the plaintiff; and
- the plaintiff is injured thereby (H & R Johnson (Malaysia) Bhd v H & R Johnson Tiles Limited & Another [1995] 2 CLJ 581; Megnaway Enterprise Sdn Bhd v Soon Lian Hock [2009] 8 CLJ 130).

Unlawful Interference of Contract

In order to succeed in a claim for tort of inducing a breach of contract, five conditions are to be fulfilled:

- there must be "direct" interference or "indirect" interference coupled with the use of unlawful means;
- the defendant must be shown to have knowledge of the relevant contract;
- the defendant must be shown to have had the intent to interfere with it;
- in bringing an action other than a quia timet action, the plaintiff must show that he or she has suffered more than nominal damage; in any quia timet action, the plaintiff must show the likelihood of damage occurring to him or her if the act of interference is successful; and
- so far as it is necessary, the plaintiff must successfully rebut any defence based on justification that the defendant may put forward (Loh Holdings Sdn Bhd v Peglin Development Sdn Bhd & Another [1984] 2 MLJ 105; SV Beverages Holdings Sdn Bhd & Others v Kickapoo (Malaysia) Sdn Bhd [2008] 4 CLJ 20; Lionex (supra)).

1.14 Criminal Liability

A trade secret owner may pursue a civil claim against an infringer.

In addition to the remedy in a civil claim, an infringer may commit an offence of misappropriating a trade secret, which is the "property" of another. Some examples follow.

Section 378 of the Penal Code

Offence:

- whoever, intending to take any movable property dishonestly out of the possession of any person without that person's consent, moves that property in order to such taking, is said to commit theft;

- the words "movable property" are intended to include corporeal property of every description, except land and things attached to the earth or permanently fastened to anything that is attached to the earth (Section 22).

Penalty:

- seven years or a fine or both; a second or subsequent offence shall be punished with imprisonment and also be liable to a fine or whipping.

Section 403 of the Penal Code

Offence:

- whoever dishonestly misappropriates any property, or converts it to his or her own use, or causes any other person to dispose of it, commits an offence.

Penalty:

- imprisonment for a term of not less than six months and not more than five years and whipping, in addition to being liable to a fine.

Section 3 of the Computer Crimes Act 1997

Offence:

- a person shall be guilty of an offence if:
  (a) he or she causes a computer to perform any function with intent to secure access to any program or data held in any computer;
  (b) the access he or she intends to secure is unauthorised; and
  (c) he or she knows at the time of causing the computer to perform the function that that is the case.

Penalty:

- fine not exceeding MYR50,000 or imprisonment for a term not exceeding five years, or both.

Section 3 of the Computer Crimes Act 1997

Offence:

- a person shall be guilty of an offence if he or she communicates a number, code, password or other means of access to a computer, directly or indirectly, to any person other than a person to whom he or she is duly authorised to communicate such information.

Penalty:

- fine not exceeding MYR25,000 or imprisonment for a term not exceeding three years, or both.

Section 218 of the Companies Act 2016

Offence:

- a director or officer of a company shall not, without the consent or ratification of a general meeting:
  (a) use the property of the company;
  (b) use any information acquired by virtue of his or her position as a director or officer of the company;
  (c) use his or her position as such director or officer;
  (d) use any opportunity of the company of which he or she became aware in the performance of his or her functions as the director or officer of the company; or
  (e) engage in business which is in competition with the company, to gain directly or indirectly a benefit for himself or herself or any other person, or cause detriment to the company.

Penalty:

- imprisonment for a term not exceeding five years or a fine not exceeding MYR3 million, or both.

1.15 Extraterritoriality

A claim for breach of a trade secret is a tortious claim.

The High Court has jurisdiction to try all civil proceedings in the following locations:

- where the cause of action arose;
- where the defendant or one of several defendants resides or has his place of business;
- where the facts on which the proceedings are based exist or are alleged to have occurred; or
- where any land the ownership of which is disputed is situated (Section 23(1) of the Courts of Judicature Act 1964).

Section 23(1) of the Courts of Judicature Act 1964 confers extraterritorial jurisdiction on the High Court. In determining whether the High Court has jurisdiction, the issue to be considered is whether the statement of claim disclosed that the plaintiff's action was based principally on:

- whether the causes of action arose within Malaysia;
- whether the defendant or one of several defendants resides or has his place of business in Malaysia; or
- whether the facts on which the proceedings were based in this case occurred or are alleged to have occurred within Malaysia (Goodness for Import and Export v Phillip Morris Brands Sarl [2016] 7 CLJ 303).

Whilst misappropriation may occur in another jurisdiction, if the trade secret is used in Malaysia in an unauthorised way to the detriment of the plaintiff, the Malaysian court will have jurisdiction to hear the claim by the plaintiff in Malaysia.

2. MISAPPROPRIATION OF TRADE SECRETS

2.1 The Definition of Misappropriation

Civil Action

The three elements to be established in order to succeed in an action for breach of confidence are that the information sought to be protected has the necessary quality of confidence, that the information was communicated in circumstances importing an obligation of confidence, and that there has been an unauthorised use of that information to the detriment of the party communicating it.

In respect of the third element, it may be argued that "misappropriation" per se may not meet the requirement. The plaintiff may need to establish that there has been "unauthorised use" and that such use is to the "detriment" of the plaintiff.

A trade secret is an intangible asset of the plaintiff, and the intellectual property of the plaintiff. The fact that the defendant has wrongfully gained access to the trade secret without the permission of the plaintiff may show that such access amounts to use.

In Svenson Hair Center (supra), the court held that "… it must be recognised that particulars such as customers' names, lists and details have also been judicially recognised as being confidential in nature, and wrongful utilisation of such particulars warrants injunctive protection."

In Schmidt Scientific (supra), the court held that "... [I]t is a breach of the fidelity clause and the implied duty to remove a customer list or to deliberately set out to memorise the said list with the intention of using it later, even though any use or disclosure is confined to the post-employment period. In such a case the eventual exploitation of the information is considered to be no more than an extension of the original breach of good

faith and fidelity. In Robb v Green [1895] 2 QB 315 the Court of Appeal held that the employee was in breach of an implied term of the contract of service in making copies of his employer's list of customers' names and addresses, with the intention of using it for the purpose of soliciting orders from them after he had left his employer's service and set up a similar business on his own account."

Thus, when the defendant has misappropriated and gained access to the trade secret, it is inherently improbable in itself to accept the argument that there is no "use" of the trade secret. The fact that one has gained access to the trade secret without permission may show that there is an intention to refer to or use such information at a later date. In fact, the obtaining of information is akin to the obtaining of an advantage. Based on the decided cases, this may be sufficient to fulfil the third requirement to complete the equation for a claim for breach of confidentiality.

Innocent "misappropriation" or "accidental misappropriation" may not be a valid defence for an action for breach of confidence.

Criminal Action

For criminal action, the burden of the prosecutor is higher. Mens rea is an important component.

Section 378 of the Penal Code

Offence: a person may be guilty of an offence if there is intention to take a trade secret dishonestly out of the possession of the trade secret owner without the latter's consent.

Section 403 of the Penal Code

Offence: a person may be guilty of an offence if he or she dishonestly misappropriates any property, or converts it to his or her own use, or causes any other person to dispose of it.

Section 3 of the Computer Crimes Act 1997

A person shall be guilty of an offence if:

- he or she causes a computer to perform any function with intent to secure access to any program or data held in any computer;
- the access he or she intends to secure is unauthorised; and
- he or she knows at the time of causing the computer to perform the function that that is the case.

2.2 Employee Relationships

The principle propounded in Coco (supra) is deeply entrenched in Malaysian jurisprudence. The elements to be established for a trade secret claim are applicable whether the person who misappropriated the trade secret is an employee of the owner or otherwise.

Employees are "fiduciaries", and an employer is entitled to the single-minded loyalty of their fiduciaries. The employee has the implied duty to act in good faith and must not make a profit out of the employer's trust, nor place himself or herself in a position where his or her duty and interest may conflict. The employee may not act for his or her own benefit or the benefit of a third person without the informed consent of their employer.

In brief, the law imposes the core duties of loyalty and fidelity on the employee. A breach of fiduciary obligation, therefore, connotes disloyalty or infidelity.

During employment, the duty of fidelity prevents an employee from acting in conflict with their employer, regardless of whether the information they use is confidential or otherwise. The duty of fidelity may continue after the termination of employment, although the scope of duty is narrower.

2.3 Joint Ventures

The law equally recognises the existence of obligations between joint venturers with respect to their respective trade secrets.

2.4 Industrial Espionage

In Worldwide Rota (supra), one of the employees was asked to join the defendant's company, and was instructed to obtain as much information about the plaintiff before joining the defendant's company. The court found that the employee was asked by the defendant to spy on the plaintiff for the benefit of the defendant, and this is akin to an industrial espionage.

For industrial espionage, there may be a basis for the plaintiff to claim aggravated damages or exemplary damages over and above a general damages and injunctive order.

In Worldwide Rota (supra), the court held that whenever the defendant's conduct is sufficiently outrageous to merit punishment in situations where the defendant's conduct discloses malice, fraud, cruelty, insolence or the like, then exemplary damages would be granted. Lord Devlin in Rookes v Barnard And Others [1964] AC 1129, at page 1226, aptly said that "... an award of exemplary damages can serve a useful purpose in vindicating the strength of the law and thus affording a practical justification for admitting into the civil law a principle which ought logically to belong to the criminal."

"Where a defendant with a cynical disregard for a plaintiff's rights has calculated that the money to be made out of his wrongdoing will probably exceed the damages at risk, it is necessary for the law to show that it cannot be broken with impunity. This category is not confined to moneymaking in the strict sense. It extends to cases in which the defendant is seeking to gain at the expense of the plaintiff some object – perhaps some property which he covets – which either he could not obtain at all or not obtain except at a price greater than he wants to put down."

3. PREVENTING TRADE SECRET MISAPPROPRIATION

3.1 Best Practices for Safeguarding Trade Secrets

There is no dearth of literature suggesting various "best practices" to safeguard trade secrets, but these practices are merely suggested guidelines.

It is important for an organisationto embrace trade secret protection and instil the culture from the top level down.

Taking stock of what the organisation possesses and what is properly regarded as trade secrets is always a fundamental start.

For example, a company should:

- implement proper internal policies for intellectual property rights;
- maintain a holistic system with regard to record keeping, storage and document classification, controlling accessibility and retention;
- develop a proper regime and procedures with regard to the system;
- formulate proper terms and conditions in employment agreements and agreements with third parties in the event of any disclosure of trade secrets – eg, non-disclosure and confidentiality agreements;
- conduct periodic audits;
- provide a training and awareness programme; and
- set up a team and develop a plan to react in the event of a breach.

3.2 Exit Interviews

An exit interview for departing employees is often conducted in Malaysia, generally by a member of human resources. Such interview enables the organisation to obtain full and frank feedback from departing employees.

A properly worded terms of employment would impose obligations on the employees, whether during the term of employment or thereafter, regarding their duties of confidentiality, and the employees would have assured the organisation with respect to confidentiality and/or trade secrets.

4. SAFEGUARDING AGAINST ALLEGATIONS OF TRADE SECRET MISAPPROPRIATION

4.1 Pre-existing Skills and Expertise

There is no fiduciary duty against legitimate competition between directors (including employees) with a company upon resignation.

There may not be any restriction on the employee using his or her general knowledge and skills in his or her undertaking post-employment.

What is guarded by law is information that has the necessary quality of confidence. If the impugned "information" was from within the general fund of the employee's own knowledge, exposure and experience accumulated in the industry over the years, there may be no grounds to assert that there has been a "breach of fiduciary duty" or even a breach of confidentiality (Vision Cast Sdn Bhd v Dynacast (Melaka) Sdn Bhd [2014] 8 CLJ 884).

The factors that are relevant to determining whether a given body of information is confidential include the following:

- the extent to which the information is known outside the owner's business;
- the extent to which it is known by employees and others involved in the owner's business;
- the extent of measures taken by the owner to guard the secrecy of the information;
- the value of the information to the owner and his or her competitors;
- the amount of effort or money expended by the owner in developing the information; and
- the ease or difficulty with which the information could be properly acquired or duplicated by others (ie, through their independent endeavours) (Electro Cad Australia Pty Ltd v Mejati RCS Sdn Bhd [2008] 4 CLJ 217).

In Philip Morris Products SA v Ong Kien Hoe [2010] 2 CLJ 106, the learned Judge Mary Lim (now FCJ) held that "Innocence is therefore not a defence to an infringement of a registered trade mark." Based on the same rationale, "inevitable disclosure" may not accord any defence to the infringer if the elements for breach of confidence are established by the plaintiff.

4.2 New Employees

There is no hard and fast rule on what is considered "best practices" for employers who hire employees from competitors to minimise the likelihood that the employer or new employees will be subject to a trade secret misappropriation claim. However, some due diligence may be important to minimise such risk.

For example, prior to the hire, it may be important to ascertain whether the employee is subject to any restraining clause from their previous employment.

For the terms of employment, it may be prudent to include a certain term to elicit assurance from the new employee that their conduct is within the law and not in breach of the rights of any third party.

Furthermore, having a proper policy in place and training within the organisation may eliminate the risk. Companies should embrace the culture of respecting others' trade secrets at all levels of the organisation.

5. TRADE SECRET LITIGATION

5.1 Prerequisites to Filing a Lawsuit

There is no prerequisite to filing a lawsuit.

5.2 Limitations Period

An action for breach of confidence is a tortious claim. Actions shall not be brought more than six years after the date on which the cause of action accrued.

The law on when a cause of action accrues is well settled and very much entrenched in Malaysian jurisprudence. A cause of action founded on tort accrues on the date of its breach and that time begins to run from that breach (Great Eastern Life Assurance Co. Ltd v Indra Janardhana Menon [2005] 4 CLJ 717).

A "cause of action" is the entire set of facts that gives rise to an enforceable claim; the phrase comprises every fact which, if traversed, the plaintiff must prove in order to obtain judgment.

5.3 Initiating a Lawsuit

A lawsuit is initiated by filing a writ and statement of claim or originating summons.

5.4 Jurisdiction of the Courts

Most cases for a trade secret claim are filed in the High Court. There is a specialised Intellectual Property High Court in certain states that hears IP disputes. Thus, if the action consists of a claim for breach of confidence and the infringement of IP rights, the action may be heard by the specialised Intellectual Property High Court.

If the claim is for a subject matter that does not exceed MYR1 million, a Sessions Court has jurisdiction to try the action.

5.5 Initial Pleading Standards

The remedy or relief being sought must be specifically pleaded.

In brief, every pleading shall contain:

- the particulars of the parties;
- a summary of the material facts and documents, but not the evidence;
- a matter showing illegality, including:
  - (a) alleging that any claim or defence of the opposite party is not maintainable;
  - (b) that any issue, if not specifically pleaded, might take the opposite party by surprise; or
  - (c) any issues of fact not arising out of the preceding pleading;
- a matter that has arisen at any time, whether before or after the issue of the writ;
- a raising of any point of law;
- the necessary particulars, including:
  - (a) the particulars of any misrepresentation, fraud, breach of trust, wilful default or undue influence on which the party pleading relies;
  - (b) where a party alleges any condition of the mind of any person, whether any disorder or disability of mind or any malice, fraudulent intention or other condition of mind except knowledge exists, and particulars of the facts on which the party relies; and
- the relief or remedy that the plaintiff claims, but costs need not be specifically claimed.

A party shall not, in any pleading:

- make an allegation of fact or raise any new ground or claim that is inconsistent with a previous pleading; or

- quantify any claim or counterclaim for general damages.

For a claim for breach of confidence specifically, the plaintiff must identify the "confidential information" that has been misused with sufficient particularity in their pleading (Statement of Claim), and whether it was peculiarly part of the plaintiff's intellectual property.

Details or the particulars of the confidential material or information sought to be protected or that formed the subject of the allegation of misuse must be pleaded. An averment in wide and general terms is not acceptable in law (Vision Cast (supra)).

5.6 Seizure Mechanisms

The plaintiff may also seek other forms of relief prior to service of the papers on the infringer, such as Anton Piller Orders or ex parte interlocutory injunctions. An Anton Piller Order enables a party to preserve evidence that is relevant to a suit so that the relevant evidence may be subsequently adduced in the suit, in the interest of justice.

Among other matters, the plaintiff must establish:

- an extremely strong prima facie case that the patent has been infringed;
- that the defendant has incriminating documents; and
- that there is a real possibility that such documents may be destroyed.

If the court grants an ex parte interim injunction order, that order shall automatically lapse 21 days from the date of the order, unless it is revoked or set aside earlier (Order 29 rule 1 (2B), RC). An ex parte order must be served within seven days of the date of the order, and the court, when granting the order, must fix a date to hear the application inter partes within 14 days of the date of the order (Order 29 rule 1 (2C), RC).

5.7 Obtaining Information and Evidence

At the outset, it may be worth mentioning that illegally obtained evidence remains admissible in law if it is found to be relevant to the case.

Discovery

Discovery applications are typically made at the High Court after the close of pleadings but before the start of a trial (Order 24, RC).

There are three stages:

- disclosure of a list of documents;
- copies of documents are inspected and taken; and
- production of the documents.

When the court orders for discovery, a party may be required to disclose documents that support or adversely affect their own or another party's case.

The list of prospective documents to be disclosed must be succinct.

Each relevant document must be identified.

Where a document is privileged, it must be described as such, along with justification.

The list is to be accompanied by an affidavit to verify its contents.

A pre-action order for discovery against a person or a Norwich Pharmacal Order may be given if there are sufficient grounds for doing so. The application must provide details of the intended proceeding and whether the person against whom the order is sought is likely to be a party to subsequent proceedings in court (Order 24 rule 7A, RC):

- pre-action discovery – obtaining relevant information to support a claim against a potential defendant who is already identified;
- Norwich Pharmacal Order – obtaining relevant information to identify a potential defendant.

5.8 Maintaining Secrecy While Litigating

The court has power to grant a Confidentiality Order or a Protective Order in appropriate cases, to maintain the secrecy of the trade secrets at issue in the litigation.

Generally, a trial is conducted in open court. In very limited circumstances, the court may order the proceedings to be conducted in camera, although this is usually confined to cases where the identity of minors may not be disclosed, for instance, in the interest of justice.

5.9 Defending against Allegations of Misappropriation

The following defences are available in trade secret litigation:

- the plaintiff's case does not fulfil the requirements for breach of confidence;
- the information sought to be protected does not have the quality of confidence;
- the plaintiff failed to identify the confidential information that was alleged to have been disclosed;
- the information is no longer confidential;
- there is just cause or justifies grounds for disclosure; and
- public interest.

5.10 Dispositive Motions

Upon the application of a party or on its own motion, the court may determine any question of law or the construction of any document arising in any cause or matter at any stage of the proceedings where it appears to the court that:

- such question is suitable for determination without a full trial of the action; and
- such determination will finally determine the entire cause or matter, or any claim or issue therein.

On such determination, the court may dismiss the cause or matter or make such order or judgment as it thinks just (Order 14A of the Rules of Court 2012).

At any stage of the proceedings, the court may order to be struck out or amended any pleading or the endorsement of any writ in the action, or anything in any pleading or in the endorsement, on the grounds that:

- it discloses no reasonable cause of action or defence, as the case may be;
- it is scandalous, frivolous or vexatious;
- it may prejudice, embarrass or delay the fair trial of the action; or
- it is otherwise an abuse of the process of the court (Order 18 rule 19 of the Rules of Court 2012).

5.11 Cost of Litigation

The court has discretion to award costs, and to determine the quantum of costs.

Generally, the winning party will be awarded costs.

Costs may be dealt with by the court at any stage of the proceedings or after the conclusion of the proceedings, and any costs ordered shall be paid at the conclusion of the proceedings unless the court orders otherwise.

Where in any cause or matter anything is done improperly or unnecessarily, or an omission is made, by or on behalf of a party, the court may direct that any costs to that party in respect of it shall not be allowed to that party, and that any

costs occasioned by it to other parties shall be paid by said party.

In assessing the costs, the court may have regard to all relevant circumstances, including:

- the complexity of the item or of the cause or matter in which it arises and the difficulty or novelty of the questions involved;
- the skill, specialised knowledge and responsibility required of, and the time and labour expended by, the solicitor or counsel;
- the number and importance of the documents prepared or perused, however brief;
- the place and circumstances in which the business involved is transacted;
- the importance of the cause or matter to the client;
- the amount or value of any money or property that is involved; and
- any other fees and allowances payable to the solicitor or counsel in respect of other items in the same cause or matter, but only where work done in relation to those items has reduced the work that would otherwise have been necessary in relation to the item in question.

6. TRIAL

6.1 Bench or Jury Trial
Trade secret trials are decided by a judge.

6.2 Trial Process
Upon the close of pleadings, the court will give directions for the exchange of documents between the parties. The court will also direct the exchange of witnesses' statements prior to trial.

Trials are conducted in open court, where witnesses will be called to testify and adduce evidence during Examination-in-Chief. Witnesses are subject to cross-examination by opposing counsel and re-examination by their respective counsel.

Generally, a matter filed in Malaysian courts will be disposed within nine months.

Due to the outbreak of the COVID-19 pandemic, the court has, in the interest of justice, conducted civil and criminal proceedings of any cause or matter through remote communication technology.

6.3 Use of Expert Witnesses
Expert witness testimony is allowed in court.

It is the duty of an expert to assist the court on the matters within his or her expertise. This duty overrides any obligation to the person who has instructed or paid the expert witness (Order 40A rule 2 of the Rules of Courts 2012).

Unless the court directs otherwise, expert evidence to be given at the trial of any action is to be given in a written report signed by the expert and exhibited in an affidavit sworn to or affirmed by said expert, testifying that the report exhibited is his or hers and that he or she accepts full responsibility for the report.

An expert's report shall:

- give details of the expert's qualifications;
- give details of any literature or other material upon which the expert witness has relied in making the report;
- contain a statement setting out the issues that the expert has been asked to consider and the basis upon which the evidence was given;
- if applicable, state the name and qualifications of the person who carried out any test or experiment that the expert has used for the report and whether or not such test or experi-

ment has been carried out under the expert's supervision;
- where there is a range of opinion on the matters dealt with in the report, summarise the range of opinion and give reasons for the expert's opinion;
- contain a summary of the conclusions reached;
- contain a statement of belief of the correctness of the expert's opinion; and
- contain a statement that the expert understands that their overriding duty in giving their report is to the court and that this duty has been complied with (Order 40A rule 3 of the Rules of Courts 2012).

7. REMEDIES

7.1 Preliminary Injunctive Relief

Interlocutory injunctions may be granted by the High Court where the applicant successfully establishes that:

- there is a bona fide serious issue to be tried;
- the balance of convenience tilts in favour of the grant of the interlocutory injunction; and
- damages would not be an adequate remedy if the plaintiff succeeded at trial (Keet Gerald Francis Noel John v Mohd Noor bin Abdullah [1995] 1 MLJ 193).

The court may also consider the following factors:

- where the justice of the case lies;
- the practical realities of the case;
- the plaintiff's ability to meet its undertaking in damages should the suit fail. The court may require the plaintiff to provide an undertaking – eg, a bank guarantee;
- whether there is any delay; or
- public interest.

Where the injustice to the plaintiff is manifest, the judge may dispense with the usual undertaking as to damages (Cheng Hang Guan v Perumahan Farlim (Penang) [1988] 3 MLJ 90).

Ex Parte Interim Injunction Order

An application for an ex parte injunction order requires strict compliance with the provision under Order 29 rule 1 (2A), RC (Motor Sports International v Delcont [1996] 2 MLJ 605; Pentamaster Instrumentation (supra)).

The affidavit in support of an ex parte application must contain a clear and concise statement of:

- the facts giving rise to the claim;
- the facts giving rise to the application for the interim injunction;
- the facts to justify the application ex parte, including details of any notice given to the other party or the reason for not giving notice;
- any answer by the other party (or which is likely to be asserted) to the claim or application;
- any facts that may lead the court not to grant the application;
- any similar application or order made earlier; and
- the precise relief sought (Order 29 rule 1 (2A), RC).

Furthermore, it is important that the plaintiff in an ex parte injunction application provides full and frank disclosure, failing which the ex parte order may be set aside (Pentamaster Instrumentation (supra)).

7.2 Measures of Damages

In most trade secret actions, the remedies granted by the courts are as follows:

- injunctive order;
- general damages;
- aggravated damages;

• exemplary damages; and
• costs.

The current potential civil remedy against an infringer is either an assessment of the profit made by the infringer or an award of damages representing the lost profit suffered by the originator.

It is trite law that the same principle applies when considering the award of damages. The usual principal head of damage is the loss of business profits caused by the defendant.

The plaintiff is entitled to "such damages as naturally flow from their unlawful act, and that there is no artificial limitation." Consistent with the established principle of law, the award of damages is compensatory – ie, it is to put the plaintiff in the same position he or she would have been in had the wrong not been committed. While it is quite easy to state the general principle, the mechanics of ascertaining damages actually sustained by the plaintiff are not simple to determine. There is no hard and fast rule that is foolproof and universally accepted (Taiping Poly (M) Sdn Bhd v Wong Fook Toh [2011] 3 CLJ 837).

See also **2.4 Industrial Espionage** regarding aggravated and exemplary damages.

7.3 Permanent Injunction

A permanent injunction is the main remedy for a successful trade secret claimant. Unless the court imposes a certain time limit, a permanent injunction provides for perpetual restrain against the infringer for unlawful use of the trade secret.

The court will not usually impose any limitation on an employee obtaining lawful employment else, but the permanent injunction will restrain the employee from unlawful conduct.

7.4 Attorneys' Fees

The costs of and incidental to court proceedings are at the discretion of the court, which has full power to determine by whom and to what extent the costs are to be paid.

7.5 Costs

See **5.11 Cost of Litigation**.

8. APPEAL

8.1 Appellate Procedure

An appeal may be made to the Court of Appeal.

Subsequently, parties may appeal the decision of the Court of Appeal to the Federal Court, with leave from the Federal Court.

8.2 Factual or Legal Review

Appeal at the Court of Appeal is by way of rehearing.

It is a settled principle of law that in an appeal, where facts have to be reviewed, it is undesirable for the findings of the court below to be disturbed by a court of appeal unless it appears that those findings are clearly wrong, and more especially that it is undesirable to do so where the conclusion reached must to a large extent depend on the credibility of the witnesses and the impression formed by a court that has seen them and can judge their honesty and accuracy.

An appeal before the Federal Court usually involves questions of law.

In the face of that finding by the trial judge on the question of fact, the Federal Court is only entitled to displace that conclusion if it is satisfied that the trial judge's view was plainly wrong and that any advantage which he or she enjoyed by having seen and heard the witness was not

sufficient to explain his or her conclusion, as the authorities already quoted show.

9. CRIMINAL OFFENCES

9.1 Prosecution Process, Penalties and Defences

A trade secret owner may lodge a police report.

Please refer to **1.14 Criminal Liability** and **2.1 The Definition of Misappropriation**.

10. ALTERNATIVE DISPUTE RESOLUTION

10.1 Dispute Resolution Mechanisms

Alternative dispute resolution mechanisms are available to parties who have consented to use such mechanisms. Consent may be obtained at the outset of the relationship (eg, in the agreement entered between the parties) or after a dispute arises.

Gan Partnership is led by a team of advocates with more than 20 years' experience, and is among the leading law firms specialising in dispute resolution, alternative dispute resolution and intellectual property (IP). Internationally recognised, Gan Partnership provides clients with an arsenal of services and skillsets, ranging from senior counsel with over 25 years' experience to aggressive junior and modern litigators. Following the latest addition of two partners with over three decades' experience between them, the firm has gone from strength to strength. The IP team is known for litigation and enforcement, registration and prosecution, commercialisation, strategy and branding, franchising and licensing, privacy and data protection, confidential information, entertainment, gaming, advertising and media, technology and telecommunication.

AUTHORS

Bahari Yeow has specialised in dispute resolution and intellectual property for over 20 years. An advocate and solicitor, he is a registered trade mark agent, industrial design agent, patent agent and panellist of the Domain Name Dispute Resolution, Asian International Arbitration Centre. Bahari's extensive IP experience covers litigation and enforcement, registration and prosecution, commercialisation, franchising and licensing, brand protection and anti-counterfeiting. He acts for leading suppliers, service providers and multinational corporations in various commercial sectors. He is highly skilled in handling outsourcing disputes across all the major commercial sectors, particularly in identifying appropriate structures and anticipating potential issues and trends in outsourcing.

Lim Zhi Jian handles complex and high-value disputes, with a focus on IP and technology, media and telecommunications at all levels of Malaysian courts. He has assisted clients in a multitude of contentious matters, including expungement of trade marks, obtaining urgent injunctive reliefs, and procuring the judicial assignment of patents. He has also advised on free trade zones and jurisdictional matters arising from cross-border IP disputes. Lim Zhi Jian advises clients ranging from tech start-ups to Fortune 500 companies on all aspects of IP, including litigation and prosecution, brand strategy and protection, management and monetisation, strategy in trade secrets protection and confidential information.

Alex Choo is an advocate and solicitor of the High Court of Malaya, who focuses on IP and dispute resolution. He has assisted in sophisticated contentious matters ranging from IP prosecution to IP infringement proceedings, patent invalidation proceedings and corporate commercial disputes before the courts of Malaysia. Alex is involved in various advisory and regulatory capacities, including the licensing and assignment of IP rights, personal data protection and compliance. He has worked with public listed and multinational clients from a wide range of industries, including technology, food and beverage, fashion and healthcare.

Gan Partnership

D-32-02, Menara SUEZCAP 1
KL Gateway, 2
Jalan Kerinchi
59200 Kuala Lumpur
Malaysia

Tel: +603 7931 8668
Fax: +603 7931 8063
Email: zhijian@ganlaw.my
Web: www.ganlaw.my

NETHERLANDS

Law and Practice

Contributed by:
Alexander de Leeuw and Mark van Gardingen
Brinkhof see p.146

CONTENTS

1. LEGAL FRAMEWORK

1.1 Sources of Legal Protection for Trade Secrets

For a long period of time, the protection of trade secrets in the Netherlands was governed by general tort law. A Supreme Court decision dating all the way back to 1919 (Lindenbaum/Cohen) established that it can be unlawful to misappropriate someone's trade secrets, because this would be contrary to proper social conduct. Once the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement) was adopted, Dutch case law continuously sought to align with the trade-secret provisions of TRIPS when interpreting Dutch tort law (eg, honest commercial practices). A significant shift occurred with the adoption of the EU Trade Secret Directive. The Directive was implemented in the Netherlands in specific statutory trade secret law: *Wet Bescherming Bedrijfsgeheimen* (in English: Law on the Protection of Trade Secrets). This statute codifies all relevant provisions regarding the protection of trade secrets, including the legal measures available upon misappropriation (such as preliminary relief). On the merits, however, the protection of trade secrets has remained largely the same.

Apart from civil law protection, trade secrets are also protected under employment law (non-compete) and the misappropriation of trade secrets can be punished under criminal law with a maximum prison sentence of one year.

1.2 What Is Protectable as a Trade Secret

There are no limitations as to what type of information can qualify as a trade secret under Dutch law.

1.3 Examples of Trade Secrets

Every type or form of information can qualify as a trade secret if (i) the information is secret, (ii) has commercial value because it is secret and (iii) has been subject to reasonable measures to protect its secrecy. From a practical point of view, the most important consideration is whether the information has commercial value because it is secret. This can, for example, be the case with a customer base, commercial plans, recipes, production processes, product configurations, etc.

Arguably, information with a negative commercial value (because it could be damaging) can also fall under this definition. The same holds true for information that has potential commercial value, for example in an early phase of research and development (R&D).

An important exception is in place for trivial information and the experience and skills gained by employees in the normal course of their employment.

1.4 Elements of Trade Secret Protection

As indicated in **1.3 Examples of Trade Secrets**, there are three criteria to qualify as a trade secret. More specifically, a trade secret means information which meets all of the following requirements:

- it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;
- it has commercial value because it is secret; and
- it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

1.5 Reasonable Measures

A trade secret-owner is required to show that it took reasonable measures to protect its trade secrets. What type of measures can be consid-

ered reasonable in a given case depends largely on the type of company invoking trade-secret protection, the type of information concerned and how other companies within the relevant market typically deal with the protection of that kind of information.

Some measures should be taken in any case – because they are relatively simple and cheap – such as non-compete and non-disclosure agreements with employees and NDAs with collaborations. There is Dutch case law stipulating that these are some of the minimum requirements that can be expected to protect trade secrets.

Other measures that could be implemented (depending on the type of company/information) are:

- limited access to areas, computers, documents or systems where trade secrets are stored/available (on a need-to-know basis);
- alarm and security systems;
- relabelling documents and products;
- encryption and data protection;
- no "bring your own device" policy, no personal e-mail, no personal USB sticks;
- logging (computer) activity for trade secrets.

1.6 Disclosure to Employees

It is advisable to disclose trade secrets to employees only on a need-to-know basis. Also, it is important to have contractual obligations in place which prevent the employee from sharing/using the trade secret. Likewise, when an employee exits the company, it is advisable to schedule an exit conversation to discuss which information the company considers a trade secret and which information the employee can freely use. If these measures are taken, disclosing a trade secret to an employee will likely not affect the availability of protection for the trade secret.

1.7 Independent Discovery

In principle, independent discovery and reverse engineering is allowed. Unlike, for example, patent protection, trade-secret protection does not confer an exclusive right upon its holder. This means that a third party can freely disclose or use the independently developed or reverse-engineered information. Once the information becomes publicly available, trade-secret protection is no longer possible. However, if both companies decide to keep the information secret, they can both still rely on trade-secret protection.

The possibility of reverse engineering can be contractually excluded by the trade secret-holder. This will generally require complex contractual arrangements, also preventing downstream reverse engineering.

1.8 Computer Software and Technology

There are no unique provisions for the protection of trade secrets in the realm of computer software and/or technology.

1.9 Duration of Protection for Trade Secrets

In principle, trade-secret protection can be infinite. As long as the information is kept secret, it will enjoy trade-secret protection. Likewise, once the information becomes public (or readily available to those within the circles that normally deal with the kind of information in question) protection ends. In this regard, it does not matter whether the disclosure was accidental.

It is, of course, possible to obtain patent protection for the general invention encompassed by the trade secret – thereby making it publicly available to a certain extent – but at the same time protect the specifics of the invention as a trade secret. For instance, a patent can claim the generality of a specific technical innovation, but does not necessarily have to disclose each spe-

cific embodiment (there is no "best mode disclosure" requirement in Europe/the Netherlands). The details of a specific, favourable embodiment or method of manufacturing can be kept secret, and as such may enjoy trade-secret protection.

1.10 Licensing

A trade secret can be licensed in any way the holder deems fit. Dutch law provides significant contractual freedom in this regard. However, it is crucial to agree on appropriate confidentiality terms when licensing a trade secret. Usually, this means that the licensee must take all the measures also taken by the licensor to protect the trade secret. Also, all secret information should be returned/destroyed once the licence ends.

1.11 What Differentiates Trade Secrets from Other IP Rights

The key difference is that a trade secret does not confer an exclusive right upon its holder. The fact that a trade secret is not considered to be an intellectual property right also means that the EU Enforcement Directive is not applicable. In practice, however, this has relatively little meaning, as the Dutch trade-secret legislative provides for the possibility of preliminary relief and (ex parte) evidentiary seizures. The only measure not available is ex parte injunctive relief.

1.12 Overlapping IP Rights

It is very much possible (and common) for a party to assert a trade secret in combination with other types of intellectual property rights. Usually, trade secrets go hand in hand with patent and copyright protection, but there are no limits as to which combination of rights can be asserted. The advantage of, for example, also asserting a patent right is that this brings the suit within the jurisdiction of the specialised patent court in The Hague.

1.13 Other Legal Theories

It is possible to bring claims relating to trade secrets that do not turn on misappropriation. However, in most cases when there is a legal ground to act upon – such as a contractual breach – this can also be considered trade-secret misappropriation.

1.14 Criminal Liability

Dutch criminal law penalises trade-secret misappropriation with a maximum prison sentence of one year or a maximum fine of EUR21,750. It is possible to combine a civil lawsuit with criminal charges. However, the criminal charges will be handled by the public prosecutor and the injured party has little influence on that process. Also, in order for a criminal conviction to take place, there must have been some form of intent (bad faith) with the misappropriating party.

1.15 Extraterritoriality

Dutch courts have been relatively generous in granting cross-border relief in IP cases. The authors of this section believe that the same will likely apply to trade secret cases. If the trade-secret misappropriation can be tied to the Netherlands (for example, because the misappropriating party is established in the Netherlands or this is where misappropriation takes place) but also to other jurisdictions, it is believed that the Dutch courts are allowed and equipped to grant cross-border relief. Unlike with traditional IP rights, when assessing a trade-secret claim the courts are not limited by Article 24 EEX-II because trade secrets are not registered rights. This means that, unlike for IP rights, cross-border relief should not be limited to preliminary relief proceedings and can also be granted in merits proceedings.

2. MISAPPROPRIATION OF TRADE SECRETS

2.1 The Definition of Misappropriation

Under Dutch law access, the use and/or disclosure of a trade secret can amount to individually punishable unlawful acts. This means that legal action can be taken as soon as someone has gained access through unlawful means. If there is still insufficient proof of misappropriation (access, use or disclosure) it is also possible to request ex parte an evidentiary seizure before starting inter partes injunction and damages proceedings. Based on established Supreme Court case law (*Dow/Organik*), in such a case the claimant must make it plausible – based on the available evidence – that the other party has likely acted unlawfully/misappropriated trade secrets. The courts specifically take into account that an evidentiary seizure is meant to collect evidence and that, therefore, the claimant does not have to prove misappropriation to the extent that it would have to in preliminary relief or merits proceedings to obtain an injunction. The evidentiary seizure action is ex parte: the other party is not heard before a request for seizure is granted and will only learn about it when its facility is dawn-raided by a bailiff, technical expert, IT expert and, when appropriate, with police assistance.

2.2 Employee Relationships

This is the most common scenario in Dutch case law concerning trade-secret misappropriation. The only significant legal difference is the fact that additional statutory provisions (regarding the employer/employee relationship) can be invoked against the misappropriation. This does not usually lead to a material difference in outcome, however. In practice, the courts will scrutinise the agreements that are in force between the employer/employee and the measures that were taken by the employer to prevent misappropriation.

2.3 Joint Ventures

The general rule applies that in the case of a collaboration – joint venture or otherwise – both parties must make clear agreements on which information is considered to be a trade secret and the measures that have to be taken to keep that information secret. No special rules apply.

2.4 Industrial Espionage

There are no unique penalties or remedies against industrial espionage. However, the regular measures that are available can provide sufficient relief. Dutch trade-secret law allows injunctions to be imposed and damages to be awarded (arguably also including moral damages, eg, due to loss or exclusivity or reputation). Likewise, it is possible to remove infringing goods – goods that significantly benefit from the misappropriation – from the market. There are also safeguards in place to keep information confidential during litigation.

3. PREVENTING TRADE SECRET MISAPPROPRIATION

3.1 Best Practices for Safeguarding Trade Secrets

The “best practices” for safeguarding trade secrets will differ significantly across different industries. For computer software, the Dutch courts will likely expect more cybersecurity measures to be taken. For the chemical industry, one can think of relabelling essential ingredients, limited access to formulae, etc. Moreover, which measures must be taken also differs on a case-by-case basis, even within the same industry. It is therefore very difficult to describe best practices on this topic generally. As mentioned in **1.5 Reasonable Measures**, some measures should be taken in any case, such as non-compete and non-disclosure agreements with employees and NDAs with collaborations.

3.2 Exit Interviews

Unfortunately, exit interviews are still a relatively rare, uncommon/unknown phenomenon in the Netherlands. It is highly advisable, however, to conduct an exit interview with any employee who could have had access to trade secrets within the company. In such a conversation, both parties should try to describe clearly which information/knowledge the employee can continue to use and which he or she cannot. This should be formalised in writing and, preferably, another confidentiality obligation is signed at the end of the process.

4. SAFEGUARDING AGAINST ALLEGATIONS OF TRADE SECRET MISAPPROPRIATION

4.1 Pre-existing Skills and Expertise

Dutch trade secret legislation recognises a distinction between an employee's general knowledge and skills and protectable trade secrets. In practice, however, this distinction is very difficult to make and is unpredictable. The crucial question is whether certain information is acquired by the employee during the normal exercise of their function. Hence, the type of information an R&D employee can continue to use will be different from that of other employees. There is very little case law guidance on how to make this distinction and what (legal) considerations play a role. Dutch law does not recognise the doctrine of "inevitable disclosure".

4.2 New Employees

When hiring an employee from a competitor, it is always advisable to make clear written agreements on the competitor's trade secrets before the new employee starts his or her work. By explaining clearly which information the employee should and should not use and why this is the case – eg, placing his or her new employer at risk of trade-secret litigation – the employer can create a situation of good faith and honest commercial practices and prevent unwarranted trade secret misappropriation within the company. Capturing this in writing would help significantly if it were ever to come to litigation.

5. TRADE SECRET LITIGATION

5.1 Prerequisites to Filing a Lawsuit

The key consideration before initiating litigation is how much evidence is available. This means evidence of the existence and ownership of the trade secret as well as misappropriation thereof.

If there is insufficient evidence, Dutch litigation usually starts with an evidentiary seizure. The claimant will then request the court to allow an independent bailiff (assisted by independent experts, such as a technical expert and an IT professional) to take evidence from the defendant, without hearing the defendant prior to the seizure. The claimant will have to specify which documents could serve as evidence of the misappropriation claim and why this evidence will likely be found with the defendant. The bailiff can then copy documents from computers, smartphones, archives, etc. This is not like US discovery, however, where large amounts of documents can be collected for evidence. Also, there is no direct evidence to the seized evidence. The bailiff will hold on to the evidence and once the seizure has taken place, separate access proceedings will have to be conducted in order to obtain access to the seized evidence.

Once sufficient evidence is found/in place, the claimant can choose to initiate preliminary relief proceedings to get a relatively quick preliminary injunction (PI) (which will require there to be an urgent interest) or to initiate merits proceedings to obtain permanent injunctive relief

and establish liability for damages. Both types of proceedings (PI proceedings and merits proceedings) are initiated with a front-loaded writ of summons, containing all relevant arguments and evidence. An important consideration in this regard is whether or not to file a combined claim (with IP rights).

5.2 Limitations Period

The EU Trade Secrets Directive mentions a limitations period of six years. However, the Dutch legislator has chosen to implement a limitations period of five years (both for injunctive relief as well as damages). For injunctive relief, the limitations period starts when the trade secret-holder becomes familiar with the trade-secret misappropriation. For damages, the limitations period starts when the trade secret-holder becomes familiar with the damages and the person or entity liable for those damages.

5.3 Initiating a Lawsuit

See **5.1 Prerequisites to Filing a Lawsuit**.

5.4 Jurisdiction of the Courts

There is no special court for trade-secret claims, nor are there any other limitations on the courts in which a trade-secret claim can be brought. This is different when a claim for trade-secret misappropriation is combined with a claim for patent infringement, in which case the exclusive jurisdiction of the technically savvy patent-specialised Courts of The Hague applies.

5.5 Initial Pleading Standards

The amount of evidence that must be presented is different for evidentiary seizures, preliminary relief proceedings and merits proceedings. In evidentiary seizures – which generally takes place when there is insufficient evidence for preliminary relief – the trade-secret misappropriation must be made plausible on the basis of the available evidence (according to the Dutch Supreme Court in *AIB/Novisem* and *Dow/Organik*). This will be accepted relatively easily. For preliminary relief proceedings, the standard is somewhat higher. The misappropriation must still be made plausible, but the evidence must be more conclusive, comparable to a preponderance of the evidence. In merits proceedings, the evidentiary rules of the Dutch Code of Civil Procedure apply and an even higher threshold applies. It is generally accepted that, in merits proceedings, misappropriation must be proven by clear and convincing evidence.

5.6 Seizure Mechanisms

See **2.1 The Definition of Misappropriation**, **5.1 Prerequisites to Filing a Lawsuit** and **5.5 Initial Pleading Standards**.

5.7 Obtaining Information and Evidence

The primary pre-trial mechanism available to collect evidence is evidentiary seizures. Evidentiary seizures are handled by a court-appointed bailiff. It is also possible to request the court to order the other party to submit evidence, pending proceedings. The type of evidence that can be gathered is not limited in any way. However, the party that tries to obtain evidence must specify which evidence it seeks to obtain (no fishing expeditions are allowed).

5.8 Maintaining Secrecy While Litigating

Although legal proceedings are, in principle, public in the Netherlands, documents and legal briefs that are submitted in those proceedings are not. Furthermore, in cases in which trade-secret legislation applies, confidentiality can be requested, based on Article 1019ib of the Dutch Code of Civil Procedure. This means that relevant parts of hearings will only take place behind closed doors, the court decision can be redacted, and the parties, lawyers or other representatives, witnesses, experts and other persons participating in the proceedings are prevented from using or disclosing the trade secrets that

the judge labelled as confidential at the request of the trade secret-holder.

The confidentiality pools that can be created under this provision are somewhat different from those regularly applied under US law, as it is mandatory also to give access to all information (including the trade secrets) to one natural person of each party. The authors of this section believe that, in most cases, this will be undesirable, as this means that the other side will definitely get access to the trade secrets at issue. This provision is the result of the right to fair proceedings and not wanting to exclude a party from the evidence on the basis of which his or her case is handled. It is unclear whether the parties can contractually agree to deviate from this provision.

If certain information is labelled confidential, pending the proceedings, it will also not be included in the decision and, insofar as the trade secrets are discussed during trial, this will be done behind closed doors.

5.9 Defending against Allegations of Misappropriation

The most common defence is that the asserted information is not a trade secret. If the information is generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question, it is impossible to invoke trade-secret protection. It is also commonly argued that the suing party did not take (sufficient) reasonable measures to protect its information. Likewise, it can be argued that the other party's information was not acquired or used at all, or that this happened in good faith.

5.10 Dispositive Motions

It could perhaps be possible for a party, who fears becoming the defendant in a trade-secret misappropriation case, to take the "initiative" and initiate proceedings to obtain a Declaratory Judgment that certain information does not qualify as trade secrets, or has not been misappropriated. However, this is not really a dispositive motion in that it requires a full trial on its own. The plaintiff will load the "burden of proof" upon itself, and it is likely that the defendant will counterclaim for a finding of misappropriation, injunctive relief and liability for damages. There are no precedents, as far as is known.

5.11 Cost of Litigation

The costs associated with litigating trade secrets are highly dependent on the factual circumstances of the case, as well as the defences raised against a complaint. Very generally speaking, PI proceedings will cost between EUR100,000 and EUR200,000 and merits proceedings will cost between EUR150,000 and EUR350,000. Unlike in IP proceedings, the losing party does not automatically have to compensate for the winning party's legal costs. There is a provision, however, giving the courts the discretionary power to order a full cost order against the losing party. This will depend on the circumstances of the case (and can make litigation significantly more expensive).

No cure-no pay agreements are not allowed under Dutch law. It is, however, possible to agree on contingency fees, fixed fees, or other cost arrangements.

6. TRIAL

6.1 Bench or Jury Trial

In the Netherlands, all legal proceedings are heard and decided by a judge or panel of judges. There are no jury trials.

6.2 Trial Process

In principle, Dutch litigation is based on written submissions. The proceedings are relatively

streamlined, with a front-loaded writ of summons and statement of answer being the main written submissions. It is also possible to submit expert evidence and to hear witnesses. The parties can also bring their experts to trial in order for them to address the court or answer questions. There is no cross-examination of experts or witnesses.

A trial usually takes half a day or a full day, depending on the complexity of the case. Both parties will get two rounds to present their arguments and respond and the judges usually ask questions.

6.3 Use of Expert Witnesses

It is possible to file and rely on expert evidence. There are no strict rules as to how the expert must be approached, what can be the subject of expert evidence and what an expert declaration should look like. It all comes down to an assessment of credibility. As indicated in **6.2 Trial Process**, there is no cross-examination of experts. It is common, however, to have a battle of the experts in writing.

7. REMEDIES

7.1 Preliminary Injunctive Relief

The requirement for obtaining preliminary relief is that there is an urgent interest, that the trade-secret misappropriation (or threat thereof) is made plausible and that a balancing of interests weighs in favour of granting the relief.

There are no specific rules on the duration of an injunction. In theory, it could be infinite (until the information at issue loses its status as a trade secret). This is at the discretion of the court. Another example of how the court could calculate the duration of an injunction is how long it would have taken the defendant – or any other third party – to develop the trade secret at issue independently. If this is impossible to determine, the court can estimate a duration at its own discretion. In any event, it must be long enough to diminish the economic advantages gained by the misappropriation.

The court can demand that the claimant put up a bond before an injunction is granted. Conversely, if a preliminary injunction would harm the interests of the defendant too much, the court can order the defendant to post a bond in order to avoid a preliminary injunction and safeguard a potential damages claim. There is no case law precedent on this.

7.2 Measures of Damages

Dutch trade-secret law provides for quick and effective relief against misappropriation. The measures currently available are:

- injunction for the use or disclosure of the trade secret;
- injunction to manufacture infringing goods, offering or trading them, using them or importing, exporting or storing them;
- returning confidential information;
- seizure, sequestration and (partial) destruction of infringing goods in order to prevent them from entering trade;
- damages (actual damages and moral damages, but not punitive damages), if the misappropriating party knew or should have known that the trade secret was acquired, used or disclosed unlawfully.

In all cases, the court will have to take into account whether the measures are proportionate based on the circumstances of the case and that the measures are not abused or would otherwise impair legitimate trade.

7.3 Permanent Injunction

It is possible to get permanent injunctive relief against a misappropriating party. As discussed under **7.2 Measures of Damages**, the dura-

tion of the injunction will depend on the circumstances of the case. It is also possible for infringing goods to be recalled and destroyed (at the cost of the misappropriating party). Goods are considered to be infringing if the trade secret at issue had a significant influence on the quality, value or price of the goods, or if the trade secret limited costs or eased or quickened the production process or trade thereof. This relatively new definition (stemming from the EU Trade Secret Directive) will likely lead to diverging case law.

It is also possible to request an injunction to be lifted if the trade secret at a later point in time becomes public, for example because its holder makes the information public.

7.4 Attorneys' Fees

In trade secret litigation, cost orders will be based on fixed rates, which are relatively low (in the range of EUR250 to EUR2,500). However, the newly implemented trade-secret legislation gives courts the discretionary power to award full cost orders to the winning party. It remains to be seen whether courts will use this discretionary power as a main rule or as the exception to the rule.

7.5 Costs

See **7.4 Attorneys' Fees**.

8. APPEAL

8.1 Appellate Procedure

Once a first-instance decision is granted, both parties can file an appeal. In preliminary relief proceedings, the appeal must be filed within … In merits proceedings, the appeal must be filed within three months. The writ of summons on appeal is a very short document, basically indicating to the other party and the court of appeal that an appeal is launched. The next step is filing grounds of appeal. These must contain all arguments against the first-instance decision, as well as any new points. Appeal proceedings are de novo proceedings, meaning that the entire debate can be repeated and fine-tuned. In response, the respondent will have to file a statement of answer (and can lodge a counter-appeal simultaneously). The procedural rules on appeal are very strict and these two documents (grounds of appeal and statement of answer) should contain all relevant facts and arguments. There is very little room for second chances and correcting mistakes on appeal. It is also possible to appeal from orders that are not final judgments, but this requires the express permission of the first-instance court.

An appeal usually takes about six to 12 months in preliminary relief proceedings and 12 to 18 months in merits proceedings. Timing may vary somewhat between the different courts of appeal, but, other than that, there are no significant differences.

8.2 Factual or Legal Review

As indicated under **8.1 Appellate Procedure**, in the Netherlands appeal proceedings are de novo proceedings. The court of appeal will review both factual and legal issues. The court of appeal will also hear live arguments. An appeal to the Supreme Court is limited to legal issues.

9. CRIMINAL OFFENCES

9.1 Prosecution Process, Penalties and Defences

See **1.1 Sources of Legal Protection for Trade Secrets**. Criminal offences are handled by the public prosecutor with little to no involvement from the trade secret-owner.

10. ALTERNATIVE DISPUTE RESOLUTION

10.1 Dispute Resolution Mechanisms

Parties are at liberty to initiate any type of ADR mechanism they see fit. This can, for example, be mediation, arbitration or binding advice. The main advantage of ADR – specifically arbitration – is that specialist arbiters can be selected and confidentiality can be tailored to the dispute.

Brinkhof was established as an independent Dutch law firm in 2005. The firm consists of 40 lawyers who are dedicated, experienced litigators, advisers, drafters, and negotiators. They cater to clients from innovative industries, including hi-tech, pharma, medical devices, media, telecoms, retail, food, fashion, and financial. The breadth of knowledge and depth of specialist experience makes Brinkhof a centre of legal expertise for modern markets. Brinkhof's IP practice is one of the broadest in the Netherlands. Its platforms regulation and litigation team advises several of the world's online giants. The competition team is the premier team for the full range of competition and regulatory law advice. The IT team is known for its expertise in the area of sourcing and IT contracting. Brinkhof has dedicated and experienced privacy law specialists providing clients with practical business advice. Seasoned non-contentious IP specialists also deal with licensing, R&D arrangements and similar transactions on a daily basis.

AUTHORS

Alexander de Leeuw is a senior associate and specialises in national and international patent litigation, with a special focus on pharmaceutical inventions, medical devices and consumer goods. He also regularly deals with the protection of know-how/trade secrets and evidentiary seizures. Alexander has gained significant experience litigating in complex patent cases before the courts in The Hague and the EPO, eg, concerning pemetrexed and CRISPR-Cas9. In addition to his litigation practice, Alexander enjoys writing and teaching about patent law and regularly publishes about the developments regarding trade secrets, software patents and artificial intelligence.

Mark van Gardingen is a partner and co-head of the patent and trade secret litigation group and specialises in litigating and co-ordinating patent and trade-secret disputes before national and international courts, as well as the EPO. Mark's litigation experience comprises all technologies (from mobile phones to polymers), but he specifically focuses on (bio-)chemical inventions, electro-technology, and mechanical engineering. Various international practitioners guides recommend Mark as a leading patent specialist. His clients include Heineken, Dow, Synthon, Novozymes and Accord Healthcare Corp. Mark regularly writes articles on patent law in international journals, and is a regular speaker at conferences.

Brinkhof

Grote Bickersstraat 74-78
1013 KS Amsterdam
The Netherlands

Tel: +31203053202
Email: alexander.deleeuw@brinkhof.com
Web: www.brinkhof.com

Trends and Developments

Contributed by:
Alexander de Leeuw and Mark van Gardingen
Brinkhof see p.149

The most prominent development in the field of trade secrets has been the adoption of the EU Trade Secret Directive and its implementation into Dutch national legislation (*Wet Bescherming Bedrijfsgeheimen*) on 23 October 2018. Trade secrets were traditionally protected in the Netherlands under general tort law, employment law and criminal law. There is now specific legislation covering the protection of trade secrets, as well as the more procedural aspects of trade-secret litigation.

Evidentiary Seizures

One of the topics not covered by this new legislation is evidentiary seizures. Trade-secret litigation is all about evidence. In order to claim an injunction or damages successfully, it is necessary to prove that the other party has unlawfully obtained, used and/or disclosed a trade secret. Often, acquiring evidence of trade-secret misappropriation can be difficult as most misappropriating parties will usually have taken careful actions to cover their tracks. Some examples of these actions are computers that were smashed with a sledgehammer, emails and documents that were deleted, hard drives that were overwritten hundreds of times. This is where evidentiary seizures come into play.

Dutch law provides for the possibility to obtain a court order appointing an independent bailiff and a team of technical and (forensic) IT experts to conduct an ex parte (ie, unannounced) evidentiary seizure if it is plausible that the defendant has misappropriated one or more trade secrets. Although evidentiary seizures were traditionally only applied in civil litigation and later also in IP litigation, recent Supreme Court case law (*Dow/Organik*) confirms that evidentiary seizures can also be used in trade-secret litigation. The burden of proving (a reasonable suspicion of) trade-secret misappropriation for getting an evidentiary seizure order granted is relatively low. After all, this is a tool to be used for the collection of evidence, which naturally implies that the claimant does not yet have a complete case.

The bailiff will be instructed by the claimant before the seizure starts as to which specific documents/data to look for and seize. Evidence that can be seized is not limited to information contained in (electronic) documents, such as emails, process descriptions, recipes, client lists, etc, but can also be a detailed description of a manufacturing process that takes place in the factory, or samples of ingredients, intermediate products or end products. Regarding electronic documents, the bailiff's possibility to seize evidence is not necessarily limited to data physically stored in the Netherlands, but may also get access to data stored in the cloud or on foreign servers, provided that the data is (also) normally accessible in/via the Netherlands (hence, if a Dutch branch of an international group of companies also has access to documents within foreign group members, this evidence may be seized in the Netherlands).

The bailiff and his team will take evidence from the seizure location and make copies, or make copies directly on site. These copies will be stored by the bailiff, and the claimant can get access to these documents via separate inter partes access proceedings (which can be done in summary proceedings – a decision will be available within a couple of months after the seizure).

The evidence obtained through an ex parte evidentiary seizure and subsequent inter partes access proceedings can be used in Dutch litigation, but can also be used for trade-secret misappropriation litigation in foreign courts.

Confidentiality Club

Another important issue relates to confidentiality pools. For many years, Dutch procedural law accommodated a limited form of confidentiality for trade secrets that were disclosed pending litigation (eg, hearing a case behind closed doors and redacting decisions). However, legal options on the protection of confidentiality were limited to excluding third parties getting access to information, and there was no uniform practice and no clear guidance on how to establish confidentiality pools. The implementation of the EU Trade Secret Directive led to a new provision governing confidentiality pools in trade-secret litigation. The confidentiality pools that can be created under this provision are somewhat different from those regularly applied under US law, as it is mandatory also to give access to all information (including the trade secrets) to at least one natural person of each party. The rule is not "attorney's eyes only".

This may seem logical at first sight. After all, a party to litigation should have access to all relevant evidence in order to have a fair chance of bringing a defence (ie, the right to a fair trial). At the same time, however, it seems somewhat strange that a claimant should give the defendant access to their trade secrets pending litigation that should determine whether the defendant actually even had (and used/disclosed) the trade secret in the first place. This may not be a big issue for large companies with in-house legal teams. In that case, one of the members of the legal team can simply gain access to the confidential evidence and keep the information away from those dealing with the information at issue (such as R&D employees). However, when dealing with small- (and potentially also medium-) sized companies, this can become a problem.

For instance, what if an employee leaves the company, starts his or her own company and is subsequently accused of trade secret misappropriation by his or her former employer. Pending litigation, the ex-employee may get access to his or her ex-employer's trade secrets – based on the newly implemented provision – but what if the court then ultimately decides that misappropriation cannot be established? The ex-employee has then had access to the trade secrets through the litigation – how does one ensure that the ex-employee does not subsequently use that for his or her own business after all? This may lead to some further interesting case law, or creative lawyers avoiding getting into such a situation in the first place.

Brinkhof was established as an independent Dutch law firm in 2005. The firm consists of 40 lawyers who are dedicated, experienced litigators, advisers, drafters, and negotiators. They cater to clients from innovative industries, including hi-tech, pharma, medical devices, media, telecoms, retail, food, fashion, and financial. The breadth of knowledge and depth of specialist experience makes Brinkhof a centre of legal expertise for modern markets. Brinkhof's IP practice is one of the broadest in the Netherlands. Its platforms regulation and litigation team advises several of the world's online giants. The competition team is the premier team for the full range of competition and regulatory law advice. The IT team is known for its expertise in the area of sourcing and IT contracting. Brinkhof has dedicated and experienced privacy law specialists providing clients with practical business advice. Seasoned non-contentious IP specialists also deal with licensing, R&D arrangements and similar transactions on a daily basis.

AUTHORS

Alexander de Leeuw is a senior associate and specialises in national and international patent litigation, with a special focus on pharmaceutical inventions, medical devices and consumer goods. He also regularly deals with the protection of know-how/trade secrets and evidentiary seizures. Alexander has gained significant experience litigating in complex patent cases before the courts in The Hague and the EPO, eg, concerning pemetrexed and CRISPR-Cas9. In addition to his litigation practice, Alexander enjoys writing and teaching about patent law and regularly publishes about the developments regarding trade secrets, software patents and artificial intelligence.

Mark van Gardingen is a partner and co-head of the patent and trade secret litigation group and specialises in litigating and co-ordinating patent and trade-secret disputes before national and international courts, as well as the EPO. Mark's litigation experience comprises all technologies (from mobile phones to polymers), but he specifically focuses on (bio-)chemical inventions, electro-technology, and mechanical engineering. Various international practitioners guides recommend Mark as a leading patent specialist. His clients include Heineken, Dow, Synthon, Novozymes and Accord Healthcare Corp. Mark regularly writes articles on patent law in international journals, and is a regular speaker at conferences.

Brinkhof

Grote Bickersstraat 74-78
1013 KS Amsterdam
The Netherlands

Tel: +31203053202
Email: alexander.deleeuw@brinkhof.com
Web: www.brinkhof.com

PORTUGAL

Law and Practice

Contributed by:
Marta Alves Vieira and Sara Nazaré
VdA see p.164

CONTENTS

1. LEGAL FRAMEWORK

1.1 Sources of Legal Protection for Trade Secrets

Trade secrets are governed by the Industrial Property Code (IP Code).

A new legal framework entered into force in January 2019 through Decree-Law No 110/2018, of 10 December 2018, which approved the new IP Code and transposed Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (the Trade Secrets Directive).

1.2 What Is Protectable as a Trade Secret

Protection as a trade secret may cover all types of information relating to corporate activities, provided it meets the legal requirements.

Scholars exclude personal data, obvious information, information that is in the public domain and information whose content is unlawful by nature from the scope of protectable information.

1.3 Examples of Trade Secrets

The IP Code does not provide for an enumeration of the types of information that are protectable as trade secrets.

In recent case law, protectable objects have been given a wide categorisation, with the courts including the following as examples of information that is suitable to be protected as trade secrets:

- customer and distributer lists;
- market studies;
- salary statements;
- product launch dates;
- source codes;
- formulas and manufacturing processes, mainly in the food industry;
- algorithms;
- methods of assessment of manufacture and distribution costs;
- sources of supply;
- quantities produced and sold;
- market shares;
- distributor lists;
- commercial strategies;
- structure of the cost price;
- sales policies; and
- techniques used in a company (even if they are devoid of inventiveness).

1.4 Elements of Trade Secret Protection

To be protected as a trade secret, the information must cumulatively:

- be secret in the sense that it is not generally known or readily accessible, as a body or in the precise configuration and assembly of its components, to persons within the circles that normally deal with the kind of information in question;
- have commercial value because it is secret; and
- have been subject to reasonable steps to keep it secret under the circumstances, by the person lawfully in control of the information.

The required elements are very close to those established in Article 39 of the TRIPS Agreement and Article 2 (1) of the Trade Secrets Directive.

1.5 Reasonable Measures

The trade secret owner has the burden of showing that it took measures to keep the information secret.

According to the doctrine, reasonable measures may include both substantial measures (eg, lim-

iting access to digital documents through passwords or to physical documents through safes, classifying the information, carefully handling rubbish and the destruction thereof) and legal measures (eg, non-disclosure agreements).

However, so far there is no case law defining the reasonable extent of such measures.

1.6 Disclosure to Employees

Where disclosure of information to employees is controlled and secrecy is kept, said disclosure does not necessarily affect the protection of the trade secret.

In the context of an employee relationship, the employer may agree several undertakings with the employees and/or take actions to inform employees of their obligation of non-use and/or disclosure of specified confidential information in order to safeguard its secrecy.

1.7 Independent Discovery

In line with the Trade Secrets Directive, the IP Code establishes certain acts where the acquisition, use and disclosure of a trade secret is lawful.

This is the case, for instance, when the trade secret is obtained by independent discovery or creation, or by observation, study, disassembly or testing of a product or object that has been made available to the public (reverse engineering) or that is lawfully in the possession of the acquirer of the information who is free from any legally valid duty to limit the acquisition of the trade secret.

1.8 Computer Software and Technology

There are no specific provisions for the protection of trade secrets that are unique to computer software and/or technology.

1.9 Duration of Protection for Trade Secrets

The trade secret protection lasts as long as the legal elements required for trade secret protection are fulfilled. As long as the disclosure is controlled, and the information keeps its value and secrecy, the protection will last.

It is perhaps more difficult to understand the implications of an accidental disclosure. There is no case law on this, and assessment should be made on a case-by-case basis, but the major concern would be whether the information was generally disclosed to the public or not and whether or not it is still secret, valuable and controlled. In theory, it may be possible that people who have become aware of a trade secret by accident are willing to undertake not to disclose said information and to keep it secret.

1.10 Licensing

It is possible to share trade secrets, provided said sharing is made in a controlled way in order to keep the information secret (namely by non-disclosure agreements with clear terms and conditions) and valuable. Under the IP Code, licences are only established for industrial property rights (patents, utility models and registrations), which means that any licence to be granted will follow the general civil law regime.

There is no case law on this matter.

1.11 What Differentiates Trade Secrets from Other IP Rights

Trade secrets are not recognised as industrial property rights but rather as sui generis exclusive rights.

Contrary to other types of intellectual property rights, trade secrets:

- are not disclosed to the public;
- are not registered rights (quite the opposite);

- are more challenging in terms of evidence of their existence;
- have a very wide object and generally cover information that is not protectable under IP rights; and
- are harder to sell and transfer.

They are, however, close in many aspects to industrial property rights and to their respective means of enforcement and remedies.

1.12 Overlapping IP Rights

Trade secret rights may coexist with other IP rights, provided that the requirements necessary for both rights to be asserted are met in relation to the same information. As these tend to be mutually exclusive, there are very few cases where such an overlap will occur.

However, it is possible for a plaintiff to assert the same trade secret rights together with other types of intellectual property rights. For the court jurisdiction, see **5.4 Jurisdiction of the Courts**.

1.13 Other Legal Theories

It is possible to bring claims relating to trade secrets that do not derive solely from the trade secret misappropriation legal framework under the IP Code.

For instance, it is also possible to bring a claim related to trade secrets based on the following:

- unfair competition (when there is an act of competition contrary to honest practices in industrial or commercial matters) under the IP Code;
- contractual liability (eg, breach of a non-disclosure agreement), under the Civil Code (and the Labour Code if the breach is conducted by an employee);
- disciplinary liability (in cases of a breach of fiduciary duty of an employee) under the Labour Code; and
- criminal liability (see **1.14 Criminal Liability**).

Under the IP Code, the acquisition, use or disclosure of a trade secret shall also be considered unlawful whenever a person, at the time of the acquisition, use or disclosure, knew or ought to have known, under the circumstances, that the trade secret had been obtained directly or indirectly from another person who was using or disclosing the trade secret unlawfully. This may apply to a case where a third party (eg, a future employer) induces the employee to breach a contractual confidentiality obligation to the owner/employer. Both the employee and the third party would be liable for the trade secret infringement.

There is also a general civil provision according to which the instigators and assistants are also liable for the injury arising from an unlawful act.

1.14 Criminal Liability

Trade secret theft is not established in Portuguese Law as a criminal offence, but only as a misdemeanour. The unlawful acquisition, use and disclosure of trade secrets is qualified as a misdemeanour, according to the IP Code. The penalty fines range from EUR1,000 to EUR30,000 for a natural person, or from EUR5,000 to EUR100,000 for a legal person.

The disclosure of a secret can also be framed as a criminal offence, whenever a secret of a third party is revealed by someone who took knowledge of the secret in the context of their job, profession or art. The crime is punishable with imprisonment of up to one year or a fine of up to 240 days. If the disclosure of the secret is rewarded or aimed at causing damage to a third party, or if it was made through the media, the crime may be punished with imprisonment of up to one year and four months, or with a fine of up to 320 days.

Taking advantage of a secret known in the context of one's job, profession or art (in relation to the commercial, industrial, professional or artistic activity of a third party) is also framed as a crime, punishable with imprisonment of up to one year or a fine of up to 240 days.

These may be cumulated with civil claims, but care must be taken in preparing such a combined strategy since filing first a civil claim on the basis of the facts that will ground the criminal one will generally be considered a waiver of the right to pursue criminal offences.

1.15 Extraterritoriality

The Portuguese courts are only competent to assess a claim based on misappropriation that happens outside the Portuguese territory if any infringing act occurs in Portugal, under the relevant European and national civil procedural legislation.

2. MISAPPROPRIATION OF TRADE SECRETS

2.1 The Definition of Misappropriation

In line with the Trade Secrets Directive, the unlawful acquisition of trade secrets includes:

- unauthorised access to or appropriation or copying of any documents, objects, materials, substances or electronic files that are lawfully under the control of the trade secret holder and contain the trade secret or from which the trade secret can be deduced; and
- any other conduct which, under the circumstances, is considered contrary to honest commercial practices.

Likewise, the use or disclosure of a trade secret is unlawful when a person:

- acquired the trade secret unlawfully;
- breached a confidentiality agreement or any other duty not to disclose the trade secret; or
- breached a contractual or any other duty to limit the use of the trade secret.

For a claim of trade secret misappropriation, the law does not require the trade secret to be actually used nor the respective access to be gained through unlawful means. The acquisition of a trade secret without the consent of the trade secret holder is considered sufficient to be unlawful.

2.2 Employee Relationships

The elements of a trade secret misappropriation claim under the IP Code do not differ where the misappropriation involves an employee of the owner.

Furthermore, employees are bound to special obligations – if not through a written agreement – by the Labour Code, the provisions of which may also be breached by an employee, such as:

- to be loyal to the employer – ie, not carry out any business in competition with the employer, nor disclose information related to the organisation, methods of production or business; or
- to act in good faith.

2.3 Joint Ventures

The law does not make any reference to any obligations between joint ventures with respect to trade secrets.

2.4 Industrial Espionage

There are no specific provisions nor claims or penalties/remedies in relation to industrial espionage.

3. PREVENTING TRADE SECRET MISAPPROPRIATION

3.1 Best Practices for Safeguarding Trade Secrets

The trade secrets legal framework was approved by the new IP Code, which has been in force since January 2019, and is still very recent in Portugal. There are no clear recognised "best practices" for safeguarding trade secrets.

Given the uncertainty on how the courts will apply the trade secrets legal provisions, it is advisable for companies to have a strong plan for the protection of trade secrets, where the secret information is classified and clear measures of protection of secrecy are established and under surveillance, following the best practices adopted in those countries where the matter has been more developed.

For instance, the employer may take reasonable steps to educate employees on the importance of keeping confidential information secret and to adopt internal rules and codes of behaviour in relation to trade secrets. Careful actions in relation to the exit and hiring of employees are also advisable.

3.2 Exit Interviews

Where the employees have already provided non-disclosure undertakings (eg, in the employment contract), the protection of a trade secret may already be safeguarded.

If that was not the case, employers and employees are able to jointly agree on confidentiality assurances during the exit process, provided those assurances are in accordance with the law.

However, employers cannot unilaterally require employees to provide written assurances with respect to confidentiality and/or trade secrets, nor can they force employees to provide details of a new position.

Regardless, there is still a loyalty duty in respect to trade secrets (and potential information) after the employee's departure.

Although the extent of said duty is not entirely clear, the non-disclosure obligation cannot be so severe that it would prevent employees from working after their departure, nor can employees be bound to a non-competition obligation that does not comply with the legal requirements under the Labour Code.

Therefore, employers can expressly inform the employees about which information is considered confidential and/or is protected as trade secrets, and about the employees' legal duties in that respect.

4. SAFEGUARDING AGAINST ALLEGATIONS OF TRADE SECRET MISAPPROPRIATION

4.1 Pre-existing Skills and Expertise

Considering the legal definition of trade secret and in accordance with the recitals of the Trade Secret Directive, trivial information and the experience and skills gained by employees in the normal course of their work are excluded from the scope of trade secret protection, as is information that is generally known among, or readily accessible to, persons within the circles that normally deal with the kind of information in question.

There is no relevant case law in Portugal addressing the doctrine of "inevitable disclosure".

However, the Portuguese courts have been interpreting freedom to work more restrictively, as this is a constitutional right that cannot be seriously restrained. This may constitute a serious objection for the doctrine of "inevitable disclosure" in Portugal.

4.2 New Employees

There is no case law nor doctrine guidance on best practices for employers to use to minimise the likelihood of a trade secret misappropriation claim.

However, it seems that the new employer may ask the new employee to provide some assurances in relation to potential trade secret misappropriation (eg, to undertake that all the electronic devices and accounts were closed and returned to the former employer, and that no confidential information and/or trade secrets of the former will be used by the new employee).

This may be scrutinised while drafting the employment contract.

5. TRADE SECRET LITIGATION

5.1 Prerequisites to Filing a Lawsuit

No prerequisites nor preliminary steps are needed to bring a civil lawsuit based on trade secrets.

5.2 Limitations Period

The limitation period for filing a trade secret claim is five years, starting on the day when the right (trade secret claim) can be enforced – ie, the period starts when the rights holder becomes aware of the infringement and is able to identify the infringer(s) even if he/she is not yet aware of the details and the extent of the losses suffered.

When the claim is based on contractual liability (eg, infringement of a non-disclosure agreement), an ordinary 20-year limitation period is applicable. Likewise, specific deadlines are applicable in relation to criminal complaints.

5.3 Initiating a Lawsuit

The steps that an owner must take to initiate a trade secret lawsuit in Portugal are no different from those needed to file any other civil lawsuit.

The owner must file a statement of claims, invoking the right it intends to assert (see **5.5 Initial Pleading Standards** regarding proof of right) and the facts that substantiate an infringement. A judicial fee needs to be paid, the amount of which varies depending on the value of the claim (see **5.11 Cost of Litigation**).

5.4 Jurisdiction of the Courts

The Intellectual Property Court (IP Court) is a specialised state court, with jurisdiction at a national level, and is competent to handle all actions concerning industrial property in all forms as provided in law, as well as unfair competition acts and infringement of trade secrets in industrial property matters. Its jurisdiction to try claims based solely on trade secrets is still under discussion due to this dubious legal provision (in which case, the general civil courts would be competent). Non-civil claims (labour, criminal, etc) shall be tried before the relevant competent courts.

5.5 Initial Pleading Standards

According to the IP Code, trade secrets are considered as such under the same definition as Article 2(1) of the Trade Secrets Directive. The initial pleading must contain an allegation and demonstration by the claimant of the existence and ownership of such a right (ie, by alleging and demonstrating – adding evidence – the requirements set forth in the law: the fact that the information is secret, that it has commercial value because it is secret and that it has been subject to reasonable steps under the circumstances, by

the person lawfully in control of the information, to keep it secret) (see **5.8 Maintaining Secrecy While Litigating**).

5.6 Seizure Mechanisms

As a result of the transposition of the Enforcement Directive (Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004), it is possible to seize the infringing goods and materials, and the instruments used in producing and distributing said goods, as well as documentation pertaining to them. Such seizures are usually not conducted via ex parte proceedings, as these are very scarce in Portugal.

In order to successfully obtain an order for seizure, the owner must demonstrate that its right is/was infringed or that there is a reasonable fear that it will be infringed and that such infringement causes a severe injury that will be difficult to repair (close to the irreparable harm requirement).

The seizure can be requested as a pre-emptive action, or as a claim within the civil preliminary injunction/main infringement action.

Customs seizures are also available.

5.7 Obtaining Information and Evidence

The IP Code provides for the same measures as enabled in the Enforcement Directive, notably the following measures for obtaining information and evidence:

- presentation of evidence and information in the possession of, held by, or under the control of the opposing or a third party; and
- presentation of banking, financial, accounting or commercial documents.

The evidence and information measures might also be asked as a pre-emptive action, or as a claim within the preliminary injunction/civil main infringement action.

5.8 Maintaining Secrecy While Litigating

The IP Code contains a provision similar to Article 9 of the Trade Secrets Directive.

Upon a grounded request (the court cannot act on its own initiative), the court can determine that any procedural intervenient who has access to documents that form part of legal proceedings is not permitted to use or disclose any trade secret or alleged trade secret that is identified as confidential, of which they became aware as a result of such participation or access. This obligation to maintain secrecy remains in force after the legal proceedings have ended, but will cease to exist in the following circumstances, as provided in the Directive:

- where the alleged trade secret is found, by a final decision, not to meet the requirements to be considered a trade secret; and
- where, over time, the information in question becomes generally known among or readily accessible to persons within the circles that normally deal with that kind of information.

On the basis of a duly reasoned application by a party, the court can also take specific measures that are necessary to preserve the confidentiality of any trade secret or alleged trade secret used or referred to in the course of legal proceedings relating to the unlawful acquisition, use or disclosure of a trade secret (again, the court cannot make this decision on its own motion).

5.9 Defending against Allegations of Misappropriation

There are two main defence routes against a trade secret claim:

- the rebuttal of the existence of a trade secret by demonstrating that at least one of the

three requirements for the information to be considered as trade secret is not met; and
- the demonstration that either the acquisition, use or disclosure of the trade secret is not unlawful (under the same terms as those provided in Article 4 of the Trade Secrets Directive) or that it falls under the lawful acquisition, use and disclosure rule (very similar to Article 3 of the Directive).

5.10 Dispositive Motions

Although these are not considered dispositive motions (which are not a procedural figure in Portugal), a case can be immediately resolved without entering the assessment of the merits or pursuing to trial if a procedural objection is ruled favourably (lack of jurisdiction, lack of legal standing, expiry of the right) or if the defendant confesses the facts alleged in the statement of claims (either explicitly or by failing to file a defence).

5.11 Cost of Litigation

Several aspects must be considered when calculating predictable costs.

- The value of the proceedings – typically set at EUR30,000.01 in cases where exclusive rights (as immaterial rights) are at stake. In such a case, each party will have to pay EUR1,224 (paid in different phases of the proceedings, and the judicial fee of the appeal is EUR306). However, the court may set a different value for the case, considering different aspects, such as the amount of pecuniary interest of the claimant and the complexity of the case, which may lead to a substantial increase in the costs. It is, therefore, hard to predict the costs of a patent lawsuit.
- The amount that each party shall pay at the end of the proceedings – according to Portuguese civil procedural law, at the end of the proceedings, the court will fix the responsibility of the parties for the costs to the extent to which the action was unsuccessful, being the due amount paid by the losing party directly to the court.
- Other administrative costs – for translators, advisers to the court and experts.

6. TRIAL

6.1 Bench or Jury Trial

Civil disputes are always decided by a single judge in the first instance, who conducts the entire trial. In appeal, the higher courts' decisions are usually handed down by a panel of at least three judges.

6.2 Trial Process

The parties or their representatives, if they wish to, may attend the hearing. The parties' lawyers may appoint technical advisers to assist them during the hearing (being granted the same powers, notably posing questions to the witnesses). It is also common for the judge to be assisted by technical advisers during the trial, who are appointed by the court, upon the recommendation of the Portuguese public institution agreed between the parties to that effect, based on a discussion between the parties on the characteristics that such advisers should have in order to assist the court in technical matters.

The following acts are conducted during the trial phase:

- the parties' deposition (if it was requested by any of the parties);
- clarifications of the experts about the written report provided (if expert evidence was conducted and clarifications about the final report were requested by the parties or ordered by the judge); and
- the questioning of witnesses and expert witnesses, which is generally conducted in person at the hearing or by means of telecon-

ference, by the parties and generally also the judge and the technical adviser assisting the judge, with cross-examination permitted but limited to the examination scope.

Documents, legal opinions and expert opinions can also be submitted in first instance as evidence, and can be discussed during the trial. Exceptionally, documents conveyed by the witnesses during the trial may be attached to the proceedings.

Taking into consideration the evidence that was produced in the proceedings, both parties' lawyers convey their conclusions on the facts and on the law. Each lawyer may reply to the opposing side's oral pleadings only once. It is very common for the parties to jointly request and for the judge to accept the submission of the final pleadings in writing in complex patent cases.

A trial typically lasts between two days and two weeks, depending on the court's agenda and on the number of witnesses appointed by the parties and heard at the trial. If any of the witnesses are foreign and require an interpreter, this may delay the trial.

6.3 Use of Expert Witnesses

Expert witnesses can act in a trial in two different ways:

- witnesses can be appointed by the parties to be examined before the court during the hearing (where they need to take an oath), although they can also give formal written testimonies (affidavit), which is less common; cross-examination is always permitted, but is limited to the scope of the deposition that was given when examined by the party that appointed them; the witnesses shall be independent and have no direct or indirect interest in the dispute; the Bar Association deontological rules prevent lawyers from instructing the witnesses/manipulating their deposition; their oral declarations are recorded; or
- experts can also provide written opinions (not an affidavit) prior to being heard in a hearing before the court or instead of deposing orally; these written expert opinions can be attached as evidence at any time in first instance prior to the delivery of the decision.

The costs of experts are difficult to predict, as they depend on the experience/background of the expert, the technical field in question, and the level/time of assistance required. Costs are paid by the party who instructs the expert.

7. REMEDIES

7.1 Preliminary Injunctive Relief

Preliminary injunctions can be applied for at any time; although there is no urgency requirement, it is advisable to file for preliminary injunctions as soon as possible.

They can be filed before the main action or pending it. If they are filed before the main action is brought, the main action needs to be filed within 30 days of the day the preliminary injunction became res judicata. Once decreed, a preliminary injunction can stay in place for as long as the right in question is in force and/or the corresponding main action is not dismissed.

Preliminary injunctions can be decreed on the basis of a threat of infringement or actual infringement, to avoid an imminent future violation or to obtain an order for the infringement to cease. The trade secret owner must demonstrate the he/she holds the right, that is being or will be infringed. If the injunction is applied for on the basis of a threat of infringement, the holder must also demonstrate the irreparable harm. The court must take into consideration the existence

of any of the circumstances provided in Article 13(1) of the Trade Secrets Directive.

The provision of a bond is not required in order for a preliminary injunction to be granted but can be fixed by the court; it is usually calculated based on the market value of the products/rights in question.

7.2 Measures of Damages

In determining the amount of compensation for losses and damages, the court shall consider the profits obtained by the infringer, the resulting damages and lost profits suffered by the injured party, the costs borne in the protection of the right in question, the investigation and termination of the harmful conduct and the importance of the revenue resulting from the infringer's unlawful conduct.

The court should also take the moral damages caused by the infringer's conduct into account.

If it is impossible to quantify the losses effectively suffered by the injured party, the court may – provided this is not opposed by the injured party – define a fixed amount on the basis of equity (based, as a minimum value, on the payment that the injured party would have received if the violator had been authorised to use the intellectual property rights in question, as well as the costs borne in the protection of the intellectual property right and the investigation and termination of the harmful conduct).

No punitive damages can be claimed.

The case law on the calculation of royalties is not plentiful. Such royalties are usually calculated based on the average amount of the royalties received by the claimant in the position of a licensor, in a licence contract, or on the average amount of royalties practised in the industrial or commercial sector at stake.

According to a decision of the Lisbon Court of Appeal, the liability for ungrounded preliminary injunctions should be considered a strict liability (ie, the fault of the applicant must be established).

7.3 Permanent Injunction

Main (final) injunctions are the most typical claims formulated by exclusive rights holders (notably for the infringers to be ordered to cease the infringing conduct) and can be claimed on the basis of actual infringement (reactive action) or threat of infringement (pre-emptive action). Their duration is not limited.

The court may also order the infringer to pay a recurring penalty payment and corrective measures, such as the ones provided in Article 10 of the Enforcement Directive (recall from the channels of commerce, definitive removal from the channels of commerce or destruction). Where a judicial decision was taken on the merits of the case, the court may also impose other measures on the infringer aimed at preventing the continuation of the infringement conduct. These measures may include the temporary prohibition of carrying on certain activities or professions, for instance, but there is no case law on the matter. Where freedom of work is a constitutional right, it is not yet clear how this provision may be applied.

7.4 Attorneys' Fees

The final award will determine the responsibility for the judicial fees (see **7.5 Costs**).

The winning party may ask the losing party (in total or the corresponding percentage) to proceed with the payment of an amount that corresponds to the sum of the court fees paid by the wining party, plus 50% of all judicial fees paid by all the parties as a fictional compensation for the attorney fees incurred.

This is done by sending a notification letter to the losing party, detailing and demonstrating the costs incurred.

7.5 Costs

The winning party may claim for the payment of the legal and attorney fees (see **7.4 Attorneys' Fees**).

The wining party can also claim the costs incurred for translations, witnesses' travel expenses, the court's adviser, experts (when this is ordered by the court) and certificate fees (when ordered by the court).

Again, this will be decided in the final award (that will fix the fees liability) and claimed by sending a notification letter to the losing party.

8. APPEAL

8.1 Appellate Procedure

All court decisions (final and not final) are, in principle, subject to appeal in one or two degrees, by any losing party. A party can file an independent or a cross-appeal.

The appeal against a decision of the IP Court (first instance) is to be filed to the Lisbon Court of Appeal (LCA). The decision of the LCA may be subject to an appeal to the Supreme Court of Justice (SCJ), depending on the circumstances of the case. Should any issue of unconstitutionality arise, appeals may be filed to the Constitutional Court, subject to some formal requirements being met.

In the LCA and SCJ, the appeal is mostly assessed by a panel of three judges and, as a rule, the appeal does not have a suspensive effect.

Most interim decisions are appealable along with the final decision, although some interim decisions may be subject to an autonomous immediate appeal in certain cases expressly provided in the law.

Preliminary injunctions follow the same regime, although it is generally not possible to appeal to the SCJ except in very special and rare cases.

Most of the appeals are filed within 30 days of the notification of the final award, although final preliminary injunction decisions and some other types of interim decisions (not decisions on the merits) need to be filed within 15 days.

An appeal can take around one to two years for preliminary injunctions and two to four years for main actions.

8.2 Factual or Legal Review

All appeal courts decide mostly on the papers.

While the LCA hears matters both of fact and of law, the SCJ and the Constitutional Court only hear on law. For an unconstitutionality matter to reach the Constitutional Court, the interested party must have raised it in the lower courts and, once raised, it can no longer be abandoned (the matter must be repeatedly brought again in further appeals).

The early waiver to the right to appeal is only possible if done by both parties.

9. CRIMINAL OFFENCES

9.1 Prosecution Process, Penalties and Defences

See **1.13 Other Legal Theories** regarding the definition of misdemeanour and crimes.

Although these routes are not common, to pursue a misdemeanour process, the injured party must file a complaint before the Economic and Food Safety Authority (ASAE), which will be in charge of the investigation.

Only natural persons may be punished for the crimes. To pursue a criminal offence, the offended party must make a complaint to the police, to the Public Prosecutor or to another criminal entity. The Public Prosecutor will be in charge of the investigation.

In the context of a criminal file, the trade secret owners may request to be made assistants (*assistente*) of the Public Prosecutor, being therefore entitled to access the file, request new evidence, and appeal decisions taken in the file.

The typical defences available are the same as those used in a civil lawsuit, together with the criminal liability requirements rebuttal.

10. ALTERNATIVE DISPUTE RESOLUTION

10.1 Dispute Resolution Mechanisms

Mediation is very rare in Portugal.

Arbitration can be considered (for both preliminary injunctions and main actions), with one of the main advantages being the swiftness and flexibility of the procedural rules. However, since the arbitral tribunal is not empowered to grant orders to third parties, the enforcement of relevant measures such as seizures of the infringing goods would have to be performed by a judicial court upon request.

The authors would like to acknowledge the contribution of their colleagues Tiago Cochofel de Azevedo (Labour Practice) and Joana Bernardo (Investigations & White Collar).

VdA is a leading international law firm with more than 40 years of history, and is recognised for its impressive track record and innovative approach in corporate legal services. The firm offers specialised legal services covering several sectors and practice areas, enabling it to handle the increasingly complex challenges faced by clients. VdA offers robust solutions grounded in consistent standards of excellence, ethics and professionalism. Through the VdA Legal Partners network, clients have access to 12 jurisdictions, with a broad sectoral coverage in all Portuguese-speaking and several French-speaking African countries: Angola, Cabo Verde, Cameroon, Chad, Republic of Congo, Democratic Republic of Congo, Equatorial Guinea, Gabon, Mozambique, Portugal, São Tomé and Príncipe, and Timor-Leste. The firm is recognised as a leader in the provision of legal services and has received the industry's most prestigious international accolades and awards.

AUTHORS

Marta Alves Vieira joined VdA in 2012. She has approximately 18 years' experience as a litigator and is of counsel in the IP Litigation and IP Transactions practice areas, where she has been actively involved in intellectual property litigation and arbitration, notably in disputes involving pharmaceutical patents, regularly providing legal and strategic advice to companies in all intellectual property matters.

Sara Nazaré joined VdA in 2010, and is managing associate of the IP Litigation and IP Transactions practice areas. She has been providing legal advice in litigation involving patents (mostly in the pharmaceutical industry), trade marks and designs, in the context of judicial and arbitral proceedings for the infringement of industrial property rights (including damage claims), invalidity/revocation proceedings, administrative actions and assisting with the prosecution of supplementary protection certificates before the Portuguese Patent Office.

VdA

Rua Dom Luis I 28
1200-151 Lisboa
Portugal

Tel: +351 21 311 3400
Fax: +351 21 311 3406
Email: lisboa@vda.pt
Web: www.vda.pt

VIEIRA DE ALMEIDA

SOUTH KOREA

Law and Practice

Contributed by:
Wonil Kim, Sejung Lee, Chang Woo Lee and Yoon Sun Kim
Yoon & Yang LLC see p.181

CONTENTS

1. LEGAL FRAMEWORK

1.1 Sources of Legal Protection for Trade Secrets

In Korea, trade secrets are protected under the Unfair Competition Prevention and Trade Secret Protection Act (UCPA). The UCPA defines trade secrets and trade secret misappropriation, among others, and provides remedies for trade secret misappropriation, including injunction, damages, restoration of reputation of a trade secret owner/holder and criminal penalties.

If a trade secret constitutes "industrial technology" under the Act on Prevention of Divulgence and Protection of Industrial Technology (ITPA), it would additionally be protected under such Act. Further, other laws may apply to trade secrets depending on the nature and relations between a trade secret owner and misappropriator and the form of misappropriation, including:

- the Act on Support for Protection of Technologies of SMEs;
- the Monopoly Regulation and Fair Trade Act;
- the Fair Transactions in Subcontracting Act;
- the Act on the Promotion of Mutually Beneficial Cooperation between Large Enterprises and SMEs; and
- the Act on the Investigation of Unfair International Trade Practices and Remedy against Injury to Industry.

1.2 What Is Protectable as a Trade Secret

The UCPA defines a trade secret as "a production method, sales method or any other useful technical or business information in other business activities which is unknown to the public, has independent economic value and has been managed as a secret" (Article 2(ii)).

Any type of useful technical or business information may be protected as a trade secret as long as it satisfies the foregoing requirements under the UCPA.

1.3 Examples of Trade Secrets

Examples of technical information include methods of manufacturing objects, such as methods for mixing raw materials, and methods of using objects for new uses. Examples of business information include customer lists; business plans, such as investment plans; and organisational management techniques, such as personnel management techniques.

1.4 Elements of Trade Secret Protection

For trade secret protection under Article 2(ii) of the UCPA, information should be unknown to the public, have independent economic value and be managed as a secret.

Information is unknown to the public if it cannot normally be obtained without obtaining it through the information owner as the information is unknown to many unspecified persons, which would otherwise be the case as in a publication or other published form.

Information has independent economic value if the information owner can gain competitive advantage over the competitors by using the information, or if significant cost or effort is required to obtain or independently develop the information.

Information has been managed as a secret if it is objectively recognised that the secrecy of information is maintained or managed, such as by indicating or notifying the information so that it could be recognised as a secret, restricting who can access it or the method of access, or imposing a confidentiality obligation on those who access such information.

1.5 Reasonable Measures

With respect to the "secrecy" requirement, the UCPA has amended the clause "maintain secrecy by reasonable efforts" to "manage the information as secret" to set the bar lower for the "secrecy" requirement of trade secrets in 2019. Therefore, under the amended UCPA, a trade secret owner is not required to show that it took reasonable measures to protect its trade secrets, and the "secrecy" requirement would still be met if information was managed as a secret even without reasonable efforts.

Although under the amended UCPA, the term "reasonable efforts" was removed from the "secrecy" requirement and the term "maintain" was changed to "manage", the current UCPA still requires the "secrecy" of information. Since the trade secret owner needs to exert efforts in whatever form to satisfy this requirement, the prevailing view in academia is that even under the current UCPA, a certain level of effort is required to meet the "secrecy" requirement (Sang Jo Jong, Annotation to Unfair Competition Prevention Act, Pakyoungsa 2020 at 315 – 316).

1.6 Disclosure to Employees

The disclosure of a trade secret to employees could undermine the possibility of protection for the trade secret since it could increase the risk of making the information known to the public and/or undermining the "secrecy" requirement. To maintain trade secret protection, it would be recommendable for the employer to advise employees that the information is confidential and proprietary and constitutes a trade secret, regularly hold education for employees and obtain confidentiality or non-disclosure agreements from the employees.

1.7 Independent Discovery

Trade secrecy of the information cannot be denied merely because independent discovery or reverse engineering is possible. However, independent discovery or reverse engineering of a publicly available product does not constitute a trade secret misappropriation. The entity engaged in an independent discovery or reverse engineering actually bears the burden to present concrete proof that it obtained the relevant information by independent discovery or reverse engineering as a defence in the trade secret misappropriation lawsuit.

1.8 Computer Software and Technology

In Korea, there are no protections for trade secrets that are unique to computer software or technology.

1.9 Duration of Protection for Trade Secrets

Theoretically, information is protectable as a trade secret for an unlimited period as long as the requirements of a trade secret are met. However, in practice, courts limit the time period for trade secret protection by comprehensively considering various factors, including the content and difficulty of technical information; whether misappropriators or other fair competitors were able to obtain trade secrets in a legitimate way, such as independent development or reverse engineering; the time taken for the owner to acquire technical information; the time taken for the acquisition of technical information; the speed of development of relevant technologies; the personnel/physical facilities of the misappropriator; and the former employee's freedom of job selection and business (see Supreme Court Decision No 2018Ma7100).

Meanwhile, once the information becomes known to the public, it is no longer protectable as a trade secret, and this also applies to the case of accidental disclosure.

1.10 Licensing

A trade secret owner is entitled to grant a licence to use its trade secret. As long as the person

with the proper licence to use the trade secret maintains/manages the relevant information as a secret, the "secrecy" requirement would continue to be met. Therefore, when granting a licence to a third party to use the relevant information, the trade secret owner needs to require the third party to maintain or manage the information as a trade secret by imposing a non-disclosure or confidentiality obligation, and the like.

1.11 What Differentiates Trade Secrets from Other IP Rights

Most industrial property rights, including patent, design, trade mark and variety protection rights, are registered after a deliberation process. The registration presumes the existence, scope and ownership of these rights, and the misappropriator's wilfulness or negligence. However, the subject of industrial property rights and their requirements are strictly limited by law, and significant costs are incurred in the application, registration and maintenance of these rights.

This being said, trade secrets do not involve a registration process requiring the disclosure of information. A disadvantage of this is that the entity protecting trade secrets must prove the existence and characteristics of the relevant information; the fact that the information meets trade secret protection requirements; and the existence of trade secret misappropriation to receive protection. However, an advantage of this is that a wide range of information that meets the trade secret protection requirements are protectable and a smaller cost is incurred to maintain and protect trade secrets relative to industrial property rights.

1.12 Overlapping IP Rights

Industrial property rights, including patent rights, are triggered after an application submission to the Korean Intellectual Property Office, disclosure of information and a deliberation process. As such, trade secret protection rights, requiring information to be "unknown to the public", cannot, in principle, be asserted in combination with industrial property rights for the misappropriation/infringement of the same information.

However, for patent rights, there are many cases where additional information managed as trade secrets aside from the information disclosed in the patent specifications are necessary for the specific and actual practice of the relevant invention. Therefore, a plaintiff could assert trade secret rights in combination with patent rights for the misappropriation/infringement.

1.13 Other Legal Theories

Where a corporate employee divulges a trade secret or major business asset, during their employment, to the employer's competitor or removes the same without authorisation for the purpose of exploiting it for personal interest, such act constitutes unauthorised divulgence or removal in violation of their occupational duties as a person administering another's business. Thus, the crime of occupational breach of trust is consummated at the time of such unauthorised divulgence or removal (see Supreme Court Decision No 2017Do3808).

A third party who is privy to and actively conspires in or assists in the corporate employee's occupational breach of trust may be recognised to have committed a breach of trust. Further, the third party may be subject to tort liability under Article 750 of the Korean Civil Code for their inducement of the employee's violation.

1.14 Criminal Liability

A trade secret owner can pursue both civil and criminal claims. The UCPA provides criminal penalties for trade secret misappropriation.

Under the UCPA, any person who commits any of the following may be punished by an impris-

onment of no more than ten years and/or a criminal fine not exceeding KRW500 million:

- for the purpose of obtaining improper benefits or damaging the trade secret owner, ie:
  (a) acquiring, using, or leaking to any third party, trade secrets;
  (b) leaking trade secrets out of a designated place without authorisation; or
  (c) continuing to possess another's trade secret even after the trade secret owner's request to delete or return it;
- acquiring trade secrets through theft, deception, threat or other improper means; or
- acquiring or using trade secrets while knowing that an act set forth in bullet points one and two is involved (Article 18(2)).

Any person who commits the above acts with knowledge of the fact that the trade secret will be used overseas may be punished by imprisonment of no more than 15 years and/or a criminal fine not exceeding KRW1.5 billion (Article 18(1)).

Further, the UCPA provides penalties for attempted crime, criminal intent and conspiracy, consent or abetting with respect to the crime of trade secret misappropriation (Articles 18-2 and 18-3). Additionally, the UCPA has a joint penalty provision providing that if the representative of a company, etc, commits the crime of trade secret misappropriation, the company in addition to the violator may be subject to a criminal fine (Article 19).

1.15 Extraterritoriality

If a trade secret owner is a Korean entity (whether company or person), the trade secret owner can bring a civil claim in Korea based on misappropriation that happened overseas. Moreover, when a Korean committed the crime of trade secret misappropriation overseas, they may be subject to criminal proceedings in Korea. However, when a foreigner committed such crime against any Korean entity overseas, they may be subject to criminal proceedings in Korea, unless the act is not subject to criminal penalties according to the law of the place of misappropriation.

2. MISAPPROPRIATION OF TRADE SECRETS

2.1 The Definition of Misappropriation

The UCPA prohibits each of the various acts in the acquisition and use or disclosure of trade secrets. The UCPA defines trade secret misappropriation as any of the following six acts (Article 2(iii)):

- acquiring trade secrets by theft, deception, coercion, or other improper means ("improper acquisition") or subsequently using or disclosing such trade secrets improperly acquired (including informing any specific person of the trade secret while maintaining secrecy);
- acquiring trade secrets with knowledge of the fact that an improper acquisition of trade secrets has occurred or without such knowledge due to gross negligence or thereafter using or disclosing the trade secrets so acquired;
- using or disclosing trade secrets, with the knowledge of the fact that an improper acquisition of the trade secrets has occurred or without such knowledge due to gross negligence after acquiring them;
- using or disclosing trade secrets to obtain improper benefits or to damage the trade secret owner while under a contractual or other duty to maintain secrecy of the trade secrets;
- acquiring trade secrets with the knowledge of the fact that they have been disclosed in the manner provided in the fourth bullet point above or that such disclosure has been

involved, or without such knowledge due to gross negligence or, thereafter, using or disclosing the trade secrets so acquired; or
- using or disclosing trade secrets, with the knowledge of the fact that they have been disclosed in the manner provided in the fourth bullet point above or that such disclosure has been involved or without such knowledge due to gross negligence after acquiring them.

To claim trade secret misappropriation under the UCPA, a trade secret owner should argue or prove that the alleged act meets the requisite elements of the relevant trade secret misappropriation.

2.2 Employee Relationships

No separate requirement is necessary to establish a claim of trade secret misappropriation by or involving an employee. The applicable law also does not impose any particular obligations on an employee with respect to trade secrets. However, an employee generally signs agreements with their employer where they bear obligations of non-disclosure, confidentiality or non-competition, and the employee, in principle, bears such obligations to the extent stated in the relevant agreement. Consequently, where a claim of trade secret misappropriation is by or involves an employee, the acts of misappropriation related to the violations of confidentiality obligations Article 2(iii) of the UCPA (as mentioned in bullet points four to six in **2.1 The Definition of Misappropriation**) may particularly pose issues.

Meanwhile, if the information to be maintained under such agreements is deemed unworthy of protection, the court may determine that the employee's confidentiality obligation under such agreements is null and void. In addition, the court may shorten the term of the obligation provided in the agreement if it considers it to be unreasonably long considering the employee's freedom to select jobs and transfer to another employer.

2.3 Joint Ventures

The applicable laws, including the UCPA, do not separately stipulate rights or obligations between parties to a joint venture with respect to trade secrets. However, parties may sign an agreement that includes confidentiality obligations with respect to trade secrets.

2.4 Industrial Espionage

As mentioned in **1.14 Criminal Liability**, the UCPA imposes criminal penalties for trade secret misappropriation.

Moreover, industrial espionage is strictly punished, as exemplified in the case where the relevant information constitutes "national core technology" under the ITPA. Any entity that divulges and misappropriates national core technology for the purpose of using the national core technology or having it used abroad may be punished by a limited penal servitude for at least three years and/or a criminal fine not exceeding KRW1.5 billion (Article 36(1)).

If the relevant information constitutes "industrial technology" under the ITPA, the violator may be punished by an imprisonment of no more than 15 years and/or a criminal fine not exceeding KRW1.5 billion (Article 36(2)).

3. PREVENTING TRADE SECRET MISAPPROPRIATION

3.1 Best Practices for Safeguarding Trade Secrets

Safeguarding

To safeguard trade secrets, it would be advisable to develop and implement security procedures that would reduce the risk of improper disclosure

of trade secrets and provide evidentiary support for remedies for trade secret misappropriation. For example, a company may identify and classify trade secrets and mark them as confidential.

Also, a company may limit access to confidential information by controlling information on a need-to-know basis, and keep electronic information secure by using methods that prevent unauthorised access to trade secrets, including firewalls, passwords, encryption and digital signatures, and tracking or keeping logs of access to the information. It is also important to conduct regular education for employees and secure agreements on non-disclosure and confidentiality from employees, vendors and independent contractors.

The Original Certificate System

The UCPA introduced the original certificate system for electronic documents containing trade secrets to ease the trade secret owner's burden of proof regarding ownership in the trade secret misappropriation lawsuit. Once the original electronic document including trade secrets is registered and the original certificate is issued, the recipient of the original certificate is presumed to have possessed the information as stated in the relevant electronic document at the time of registration.

However, receiving the original certificate for a certain technology or data merely means that the recipient is presumed to possess the registered information at such time, and does not necessarily mean that the electronic document is automatically recognised as a trade secret.

The original certificate system for trade secrets:

- reduces and eases the burden of proof on the trade secret owner that it "owns the relevant trade secret at a certain point in time";
- forestalls trade secret misappropriation by systematically placing a time stamp on an R&D outcome so that employees recognise that the information is being managed as a trade secret;
- may positively influence the court to recognise that the relevant information has been managed as a secret when a legal dispute occurred; and
- may be used to prove prior use right or prior invention with respect to another person's patent rights.

3.2 Exit Interviews

During exit interviews, an employer reminds departing employees of the confidentiality or post-employment restrictive covenants and demands the return of all proprietary information. An employer commonly has departing employees sign a certification during the exit interview acknowledging that they received copies of executed post-employment restrictive covenants and certifying that all confidential or proprietary company information and property have been returned.

Departing employees often execute written confidentiality agreements with respect to trade secrets acquired or used during the employment period, normally together with non-compete agreements prohibiting the employment of the departing employees in the same industry for a certain time period.

The non-compete agreement goes beyond merely imposing a confidentiality obligation on an employee and prohibits the employee from engaging in any competitive acts, such as joining the employer's competitor or establishing and operating a competing company on their own. Therefore, a concern is that the agreement would harm general consumer welfare by directly restricting the employee's freedom of job selection as well as restraining free competition

and especially by being directly linked to the employee's livelihood. Thus, the court basically views the non-compete agreement as unacceptable.

However, the court may accept the employer's claim to prohibit an employee's transfer to another employer in the exceptional cases where the content and term of the non-compete agreement is found reasonable or where it is recognised that a company's trade secrets cannot be protected without such prohibition.

4. SAFEGUARDING AGAINST ALLEGATIONS OF TRADE SECRET MISAPPROPRIATION

4.1 Pre-existing Skills and Expertise

Confidential information created, developed or accumulated in the course of the employment under the employer's supervision may include the employee's general knowledge, skills and experience that should be treated as belonging to the employee.

In Korea, courts distinguish between an employee's general knowledge/skills/experience and protectable trade secrets. Utilising the employee's "general" knowledge, skills or experience gained in their employment with the prior employer is not construed as trade secret misappropriation. However, using the "special" knowledge, skills or experience gained by the employee in their employment with the prior employer, while bearing the confidentiality obligation, at the subsequent employer would constitute trade secret misappropriation.

Further, courts have ruled to the effect that using the information and know-how acquired in the employee's professional line of work in a similar line of work does not violate the UCPA (see Supreme Court Decision No 2008Ma701). This suggests that the doctrine of inevitable disclosure does not appear to be broadly accepted in Korea.

4.2 New Employees

When a company hires employees from competitors (prior employers), it would be recommendable for the company to ensure that the employees are aware of the actions that should not be taken, such as copying the prior employer's files, before being hired and to request them to provide a written pledge to confirm that they neither possess, nor will disclose, any trade secret information they learned in their prior employment. Additionally, it would be recommendable for the company to require the new employees to sign a statement that they are not violating the terms of any restrictive covenants signed with their prior employers by taking on the new job.

Further, it would be advisable for the company to take physical/technical measures to prevent the inflow of the prior employer's confidential information within the company, if possible. It would also be recommendable to prevent the employee from engaging in the same type of work as their work with the prior employer for a reasonable non-compete period; ie, usually six months to two years. The foregoing efforts will help minimise the likelihood that the company will be subject to a trade secret misappropriation claim.

5. TRADE SECRET LITIGATION

5.1 Prerequisites to Filing a Lawsuit

There are no prerequisite or preliminary steps that must be taken before a trade secret misappropriation lawsuit can be filed.

5.2 Limitations Period

Claims for trade secret misappropriation are subject to the statute of limitations. Under the UCPA, when the trade secret misappropriation continues, the right to claim injunction against or prevention of the misappropriation expires unless the right is exercised within three years from the date on which the trade secret owner becomes aware of the misappropriator's identity and the fact that business interests were infringed or threatened to be infringed due to such misappropriation. Such right also expires when ten years have elapsed after the date on which the misappropriation first occurred (Article 14).

Furthermore, the right to claim for damages resulting from a trade secret misappropriation is also subject to three-year and ten-year statutes of limitations. The three-year period begins to run when the trade secret owner becomes aware of such damage and the misappropriator's identity, and the ten-year period begins to run when the misappropriation occurred (Article 766 of the Civil Act).

5.3 Initiating a Lawsuit

The applicable laws do not provide any steps that a trade secret owner must take to initiate a trade secret lawsuit.

5.4 Jurisdiction of the Courts

There are no limitations on the courts in which a trade secret owner may bring a claim for trade secret misappropriation. There are no specialised courts handling civil or criminal trade secret lawsuits.

Under the Civil Procedure Act (CPA), a trade secret owner (plaintiff) may file a trade secret misappropriation lawsuit in a court having the jurisdiction over the place where the defendant has a domicile, where the misappropriation occurred, or where the plaintiff has a domicile (Articles 3, 8, 18 and 25).

5.5 Initial Pleading Standards

The CPA and other applicable laws and regulations do not provide initial pleading standards for civil trade secret lawsuits. In this regard, the trade secret owner may choose to file such lawsuits by alleging facts on "information and belief" as in other civil lawsuits and may additionally submit concrete evidence of misappropriation in the later stages of litigation.

However, a party's filing of the civil lawsuit would constitute a tort if it is filed in order to infringe on the counterparty's rights or interests or to inflict harm on the counterparty without reasonable cause, and the filing contravenes public order and morality (see Supreme Court Decision No 2011Da91876).

5.6 Seizure Mechanisms

By successfully obtaining the preliminary injunction and executing the preliminary injunctive relief, the trade secret owner may obtain ex parte civil seizure of accused products in a trade secret case. The court may order necessary measures to prohibit or prevent misappropriation, and such necessary measures include a seizure order ex parte. For the execution of the order, the bailiff would be dispatched to seize the accused products and/or the equipment provided in such misappropriation. The requirements for preliminary injunction are explained in **7.1 Preliminary Injunctive Relief**.

5.7 Obtaining Information and Evidence

Korea does not have a discovery process where parties are subject to the general document preservation and provision (production) requirements. The party bearing the burden of proof in the adversarial system is responsible for fact-gathering, including evidence collecting and submission. Parties may collect evidence even

before the lawsuit's filing and submit evidence to the court until the end of hearings.

The CPA has a principle of free evaluation of evidence. In this regard, there is no limit on the admissibility of evidence for all evidentiary methods. For example, documents prepared to prove the disputed issues after filing the lawsuit, hearsay evidence and written unconfirmed judgments are admissible.

Examining Evidence in Advance

Under the CPA, even before the lawsuit's filing, a party may request the court to conduct the examination of evidence in advance if using such evidence would be difficult unless the examination of evidence is conducted (Article 375). All types of evidentiary methods, including witness examination, expert examination, appraisal, documentary evidence, inspection and examination of parties, are subject to such examination in advance; ie, preservation of evidence.

Document Production

Under the CPA, a party may apply to the court for an order for document production. The application should specify the document label and its purport, the document holder and the facts to be proven and the reason why such document should be submitted (Articles 345 and 347). Further, upon the party's application, the court may order the document holder to state the document label and purport, etc (Article 346). The document holder should submit documents under the court order only in any of the following cases:

- when the holder has the documents cited in the lawsuit;
- when the applicant holds a judicial right to demand the document holder to send or show such documents; and
- when the documents have been prepared for the benefit of the applicant, or prepared with respect to a legal relationship between the applicant and the document holder (Article 344).

Moreover, the UCPA stipulates that the court may, at a party's request, order the other party to submit materials necessary for the assessment of damage caused by the infringement of business interests in trade secret misappropriation lawsuits (Article 14-3).

5.8 Maintaining Secrecy While Litigating

Under the UCPA, in trade secret misappropriation lawsuits related to the infringement of business interests, the court, at a party's request, may order the other party, its legal counsel, or any other entity that has acquired the trade secret due to such lawsuit not to use such trade secrets for purposes other than for continuing the lawsuit nor to disclose these trade secrets to others, provided that the applicant shows or vindicates that the evidence contains or would contain trade secrets and there is a risk of business disruption without such confidentiality order (Article 14-4).

Furthermore, under the CPA, if the court record contains trade secrets owned by a party, the court, at the party's request, may restrict others' access to the portions containing these trade secrets among the court records (Article 163).

5.9 Defending against Allegations of Misappropriation

Many defences are available against a claim for trade secret misappropriation.

Specificity

The defendant may argue that the alleged trade secret lacks specificity. Since trade secrets are not disclosed to the public, the exact contents thereof are often not specific, and the alleged trade secrets are fundamentally broad and ambiguous. However, trade secrets should be

as specific as possible to the extent that secrecy is not lost so that it does not interfere with the court hearing and the defendant's exercise of defence rights.

The extent of specificity of a trade secret should be determined by considering various factors, including the content and nature of the individual information alleged as a trade secret; the content of information known in the relevant field; specific aspects of trade secret misappropriation and the content of the claim for injunction; and the relationship between the trade secret owner and the other party. If the trade secret is not specific enough, the court will dismiss the plaintiff's claim (see Supreme Court Decision No 2011Ma1624).

Information Not Protectable

The defendant may argue that the alleged information does not qualify as a protectable trade secret. Possible arguments would be that the alleged information has been disclosed or available to the public or the plaintiff failed to manage the information as a secret.

Misappropriation

The defendant may target the misappropriation element. It may raise a defence contending that it independently developed or reverse engineered the information, or obtained the information under licences, among others.

Accidental Acquisition

The defendant may argue and prove that it acquired trade secrets without the knowledge and without gross negligence that trade secrets were improperly disclosed or that an act of improper acquisition or improper disclosure of trade secrets has occurred when it acquired such trade secrets. In such case, the defendant may be exempt from liability for the plaintiff's claims for injunction, damages or restoration of reputation (Article 13 of the UCPA).

Statute of Limitations

The defendant should check whether the statute of limitations has expired before the lawsuit's filing.

5.10 Dispositive Motions

Under the CPA, in the case of a deficient lawsuit whose deficiencies are not rectifiable, such lawsuit may be dismissed by a judgment without holding any pleadings (Article 219). This is exemplified in the case where a lawsuit is filed even though the parties have an agreement not to file one. Furthermore, the court may render a judgment without holding any pleadings when a defendant fails to submit a written defence until the judgment has been rendered (Article 257).

However, this is at the court's discretion, and the CPA does not provide any application procedure for parties to demand the court to render such judgment.

5.11 Cost of Litigation

It is difficult to provide a general estimate of the costs for trade secret litigation as the costs are dependent on various factors, including the content, type and complexity of alleged information and relevant technology and the complexity of the relevant case at hand.

Most of the costs for trade secret litigation would be attorneys' fees and technical expert fees. Contingency-based fees are permitted in civil cases.

Litigation financing is not prohibited, but is rarely used in Korea. However, applicable laws prohibit a voluntary litigation trust, where an entity entitled to be a party to a lawsuit or dispose legal matters entrusts such lawsuit to a third party for litigation financing.

6. TRIAL

6.1 Bench or Jury Trial

In Korea, judges decide trade secret trials, and there is no jury trial system for civil lawsuits.

6.2 Trial Process

In Korea, the trial proceeds through several hearings designated by the court.

First Hearing

At the first hearing, the plaintiff states its purpose of claim and grounds of claim in the complaint. Then, the defendant states its written answer/defence or makes an oral response. In such response, the defendant requests the dismissal of suit or claim and states whether it accepts each of the claims provided in the complaint. The plaintiff may respond whether it accepts the defendant's answer and/or submits a rebuttal brief to the defendant's answer.

Each party commonly submits evidence supporting its arguments together with the briefs. In this regard, the relevant facts in the case are argued based on the written and oral statements of the plaintiff and defendant. The court decides whether to accept the parties' applications for examination of evidence considering the relevance of the evidence with the factum probandum in the case. After the court notifies the decision on such applications for examination of evidence to the parties, it designates a next hearing for pleadings and examination of evidence.

Examination of Evidence

At the hearings for the examination of evidence, a witness should attend the hearing, swear an oath and make testimonies (Article 303 of the CPA). Further, the court may hold an explanatory session at the hearing that normally lasts for one to two hours to understand the case, including alleged trade secrets and relevant technical information.

As such, the court holds several hearings where it reviews and examines information/evidence to render judgment and when it considers that it has sufficiently examined it, hearings are closed and the court schedules the date when it will announce its judgment. The first instance proceedings usually last for around eight months to a couple of years depending on the complexity of the case, among others.

6.3 Use of Expert Witnesses

As explained in **5.7 Obtaining Information and Evidence**, the examination of evidence includes the examination of expert witnesses. Under the CPA, parties may apply for expert witnesses who report on facts obtained on the basis of specialised knowledge and experience, and the expert witness examination is based on the witness examination procedure (Article 340).

An expert witness, in principle, should make oral testimony and thus cannot testify by documents, unless permitted by the court. In other words, the expert witness, in principle, cannot testify while looking at any notes or documents prepared in advance, and thus such written notes/documents cannot replace the witness's oral testimony (Article 331). If an expert witness has difficulty in appearing before the court because they reside in a remote or barely accessible area or due to other circumstances, the court may examine such witness through video or other transmission system after hearing the parties' opinions (Article 327-2).

The expert witness examination differs by each case, but usually lasts no more than an hour.

7. REMEDIES

7.1 Preliminary Injunctive Relief

Under the Civil Execution Act, a trade secret owner may request for a preliminary injunction aside from the civil trade secret lawsuit to establish a temporary position on the disputed rights relationship in order to avoid potential material damage on the rights relationship, prevent imminent harm, or for another justifiable reason (Article 300). In order to obtain a preliminary injunction, the applicant should demonstrate that it is entitled to claim for trade secret misappropriation and the preliminary injunction is necessary to avoid significant harm or prevent imminent risk to the applicant. Such necessity is determined by comprehensively considering various factors, including the likelihood of success on the merits and the balance of hardships/benefits between the parties.

The courts limit the duration of a permanent injunction to the duration of trade secret protection, which is limited to the period explained in **1.9 Duration of Protection for Trade Secrets**.

The court may order collateral provision with respect to the respondent's damages that could incur from the preliminary injunction (Articles 301 and 280 of the Civil Execution Act). The party should either submit a copy of the deposit to the court after depositing the collateral amount ordered by the court or submit the original of the guarantee as collateral after executing a payment guarantee entrustment contract with a financial institution or insurance company.

The standard for calculating the collateral amount differs for each court, but usually it is equivalent to 10% to 20% of the amount or value of the subject matter in the litigation.

7.2 Measures of Damages

Under the UCPA, the misappropriator that damaged the trade secret owner's business interests by wilfulness or negligence is liable to compensate for such damages; if the misappropriation is found wilful, the court may award up to treble damages (Articles 11 and 14-2).

Misappropriation and Actual Damages

However, as it is difficult for the claimant (owner) to prove a causal relation between the misappropriation and actual damages, the UCPA provides damage calibration rules based on the following legal presumptions.

In measuring damages, the amount of damage may be calculated by multiplying "the volume of the goods transferred by the misappropriator" by "the claimant's presumed profit per unit of good". In such cases, the compensation should be determined between the volume of goods that the claimant could have produced as a maximum and the amount that the claimant has actually sold under the circumstance of misappropriation.

Where the respondent successfully proves the amount that the claimant would not have obtained even without misappropriation, such amount should be deducted from the foregoing damage amount if the misappropriator has gained any profit by misappropriation; the relevant amount of profit should be presumed as the amount of damages sustained by the claimant.

The claimant may choose the amount of reasonable royalty as damages against misappropriation, and the reasonable royalty denotes the objective amount that would have been paid for the trade secret if the misappropriator had gone into a licence contract with the claimant. The reasonable royalty is guaranteed as the base amount of damages for every misappropriation, and if the actual damages amount exceeds the

royalty amount, such excess amount may also be claimed as compensation.

Further, where the court recognises the extreme challenge of proving the amount of damages incurred with respect to the misappropriation in litigation owing to the nature of the case, the court may determine a reasonable amount on the basis of the entire purpose of oral proceedings and the outcome of examination of evidence (Article 14-2).

Punitive Damages

As explained above, punitive damages (treble damages) are available and the UCPA provides that the court should consider the following in determining damages:

- whether the misappropriator has a superior bargaining position;
- the degree of the misappropriator's knowledge about the risk of damages or wilfulness;
- the scale of damages suffered by the owner due to the misappropriation;
- the economic benefits obtained by the misappropriator from the misappropriation;
- the period and frequency of the misappropriation;
- the penalties pursuant to the misappropriation;
- the misappropriator's asset status; and
- the degree of efforts by the misappropriator for damage relief (Article 14-2).

In trade secret misappropriation lawsuits related to the infringement of business interests, the court may, at a party's request, order the other party to submit materials necessary for the assessment of damage caused by the misappropriation (Article 14-3).

7.3 Permanent Injunction

The trade secret owner (claimant) is entitled to claim for injunction against or prevention of misappropriation by the entity that misappropriated or is intending to misappropriate trade secrets; and necessary measures to prohibit or prevent misappropriation, such as the destruction of the object that created the act of misappropriation, the removal of equipment provided in such misappropriation or any other such necessary measures (Article 10 of the UCPA).

Courts have ruled that a permanent injunction in a trade secret misappropriation case is unacceptable as it not only has a sanctioning effect, but also runs contrary to the public interest of promoting free competition and enabling employees to extract their knowledge and abilities. Thus, courts impose a time limit on the permanent injunction, as explained in **1.9 Duration of Protection for Trade Secrets** and **7.1 Preliminary Injunctive Relief**.

Further, as explained in **3.2 Exit Interviews**, in exceptional cases where the parties have a non-compete agreement, the agreement is construed to be valid where the content and term of the agreement is recognised as reasonable or where it is found that a company's trade secrets cannot be protected without such agreement.

7.4 Attorneys' Fees

In principle, the losing party should pay the litigation costs. Attorneys' fees should be the cost of the lawsuit up to the limit of the amount as determined by the Supreme Court Rules (Article 109). Therefore, only a part of the winning party's attorney fees should be directly reimbursed by the losing party.

The litigation costs, including attorneys' fees, are determined in proportion to the amount in controversy. For example, if the amount in controversy is KRW100 million, the litigation costs would be about KRW7 million.

7.5 Costs

Under the Costs of Civil Procedure Act, the losing party bears all civil litigation costs, including daily and travel expenses for witnesses, appraisers, etc; daily allowances required for the court clerk's evidentiary examination; special charges for appraisal; communication costs; and notification costs. This amount is not significant as it is limited by the Supreme Court Rules.

8. APPEAL

8.1 Appellate Procedure

The appeal mechanism is available to the losing (aggrieved) party in the first instance trial that has a legitimate interest in the appeal. Under the CPA, an appeal should be filed within two weeks from the date on which the written judgment has been served, and such period is invariable (Articles 390 and 396).

Although the appeal period differs by case based on the complexity of case, it usually takes six months to two years to pursue an appeal.

It is impossible to appeal orders that are not final judgments (Article 390).

Since the same laws apply to all appellate courts, the appeal process does not differ depending on the first instance court where the case was filed.

8.2 Factual or Legal Review

The appellate proceeding is a continuation of the first instance trial where there is a substantive review of the claim. The appellate proceeding is a second factual trial and the case is decided again by reviewing both factual and legal issues. As a continuation of the first instance trial rather than repeating the content and process thereof, new allegations or submissions in the appellate proceeding should be considered. Therefore, the parties have a right to renewal in the appellate proceeding.

As a continuation, the parties do not need to separately take measures to preserve issues for appeal. However, considering that the appeal was initiated to reverse the judgment in the first instance court, the case is re-examined to the extent of such appeal and determined as to whether the appeal has grounds.

9. CRIMINAL OFFENCES

9.1 Prosecution Process, Penalties and Defences

A trade secret owner can bring a criminal claim for trade secret misappropriation. The law enforcement authorities investigating trade secret misappropriation can commence their investigation when they have received such criminal claim or when they have become aware of the trade secret misappropriation even without such claim.

The types of trade secret misappropriation subject to criminal penalties and details of criminal penalties have already been explained in **1.14 Criminal Liability** and **2.4 Industrial Espionage**.

The defendant's defence methods in a criminal trade secret lawsuit are similar to those in a civil trade secret lawsuit.

The trade secret owner could be investigated as a criminal complainant or witness by the law enforcement authorities. Further, the trade secret owner could be subject to a cross-examination investigation interview alongside the suspected misappropriator. The trade secret owner could make statements during the investigation, such as the fact that the information at issue constitutes trade secrets or the conduct at issue con-

stitutes trade secret misappropriation, and could also submit written opinions to this effect.

10. ALTERNATIVE DISPUTE RESOLUTION

10.1 Dispute Resolution Mechanisms

In regard to alternative dispute resolution (ADR) mechanisms, there are settlement, mediation and arbitration procedures.

Settlement

The settlement procedures include court-led settlement and out-of-court settlement. In an out-of-court settlement, parties sign a settlement agreement to make mutual concessions and end the dispute. The content and method of settlement agreement follows the principles of contractual freedom and is not subject to any limits. However, court-led settlement is under the court's supervision and carries the effect of a final judgment, unlike an out-of-court settlement.

Mediation

Mediation refers to the process by which a judge or mediator intervenes between disputed parties to prepare a forum for dialogue and compromise, and, ultimately, settlement. Once the mediation is established and mediation protocol is prepared, this would carry the same effect as court-led settlement.

Arbitration

Arbitration refers to the process where the appointed arbitrator based on the parties' agreement resolves the dispute by an arbitral award. Under the Arbitration Act, the arbitral award has the same effect as a court's final judgment (Article 35). However, the arbitral award may be enforced only by the court's decision to enforce it upon the request of the parties (Article 37).

Carrying Out Proceedings

Contrary to judicial proceedings, ADR proceedings are not open to the public. Thus, the risk of losing secrecy of the parties' trade secrets may be reduced. Aside from this, however, it is difficult to find any particular advantages or disadvantages to using ADR in trade secret cases relative to other cases.

Under the Arbitration Act, a party to an arbitration agreement may request interim measures of protection from a court, before the commencement or during arbitral proceedings (Article 10). In addition, unless otherwise agreed by the parties, the arbitral tribunal may grant interim measures as found necessary at a party's request whereby the tribunal orders a party to perform any of the following:

- maintain or restore the status quo pending determination of the dispute;
- take action that would prevent current or imminent harm or prejudice to the arbitral proceeding or prohibit action that may cause such harm or prejudice;
- provide a means of preserving assets subject to the execution of an arbitral award; or
- preserve evidence that may be relevant and material to the dispute resolution (Article 18).

Yoon & Yang LLC is a full-service law firm with more than 450 attorneys and other professionals based in Seoul, South Korea, with overseas offices in Tashkent, Uzbekistan, and Ho Chi Minh City and Hanoi, Vietnam. The firm's trade secret practice team has over 20 attorneys and other professionals, including IP, antitrust, criminal defence and labour attorneys, who demonstrate world-class professionalism and expertise to provide top-notch legal services based on the clients' needs. The trade secret practice team has accumulated litigation expertise as Korean companies have increasingly initiated or been subject to litigation in US court and ITC proceedings. The team successfully represented SK Innovation in a trade secret infringement lawsuit brought by its competitor before the US courts, ITC and Korean courts. It also represented SK Hynix against its competitor in trade secret infringement cases in the USA and Japan and OTO Melara in ICC arbitration proceedings regarding trade secret infringement.

AUTHORS

Wonil Kim is a partner and head of Yoon & Yang's intellectual property practice group and trade secret team. He has been practising in Korea for over 25 years, advising numerous domestic and multinational corporations on IP and trade secret matters intertwining IP and antitrust laws. He has been recognised by leading ranking publications. He has contributed to numerous international publications relating to IP laws since 2010, including The In-House Lawyer's "Brand and reputation management for general counsel in South Korea".

Sejung Lee is a partner at Yoon & Yang LLC. She specialises in legal advice and litigation in a wide range of intellectual property and antitrust matters. She has successfully represented major domestic and multinational companies in numerous trade secret, patent and copyright cases. Furthermore, she has worked on prominent cases involving the intersection of intellectual property and antitrust issues, including several abuse of dominance cases involving standard essential patents. She is a member of the Korean and New York Bars.

Chang Woo Lee is a partner at Yoon & Yang LLC. His main practice area is intellectual property. Prior to joining the firm, he was a patent attorney and also served as the deputy director at the Korean Intellectual Property Office. He has successfully represented numerous domestic and multinational companies in trade secret dispute and patent litigations. He co-authors various international publications relating to trade secrets and intellectual property. He is a member of the Korean and New York Bars.

Yoon Sun Kim is a US-licensed foreign attorney at Yoon & Yang LLC. Her main practice areas are intellectual property and antitrust, and she has handled various IP and antitrust matters for major domestic and multinational corporations. She earned her JD at University of Pennsylvania Law School and BA and MA at Stanford University. She is a member of the New York Bar.

Yoon & Yang LLC

ASEM Tower
517 Yeongdong-daero
Gangnam-gu
06164
Seoul
South Korea

Tel: +82 2 6003 7000
Fax: +82 2 6003 7800
Email: yoonyang@yoonyang.com
Web: www.yoonyang.com

YOON & YANG
법무법인(유) 화우

SWEDEN

Law and Practice

Contributed by:
Björn Rundblom Andersson, Hans Eriksson and Axel Seger
Westerberg & Partners ***see p.202***

CONTENTS

1. LEGAL FRAMEWORK

1.1 Sources of Legal Protection for Trade Secrets

The primary source of legal protection for trade secrets in Sweden is legislation. The Trade Secrets Act (SFS 2018:558) came into force 1 July 2018 and implemented Directive 2016/943/EU of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (Trade Secrets Directive). The previous legislation governing trade secrets in Sweden, the Trade Secrets Act (SFS 1990:409), remains applicable to the misappropriation of trade secrets that took place prior to 1 July 2018.

The Trade Secrets Directive will be an important source for interpreting the Trade Secrets Act, as well as the CJEU's preliminary rulings on the Directive.

The secondary source of legal protection for trade secrets in Sweden is case law, mainly from the Supreme Court, the Patent and Market Court of Appeal and the Labour Court, as well as the preparatory works. However, the latter may be expected to be less relevant than normally in Swedish legal tradition as it is ultimately the Trade Secrets Directive and the CJEU that will have an impact on the construction of the Trade Secrets Act.

1.2 What Is Protectable as a Trade Secret

There are many different types of information that may be protected as trade secrets under the Trade Secrets Act. This information may consist of complex information of a technical nature, or even simple facts of a commercial or administrative nature. The information is often documented, but undocumented information (ie, the knowledge of a person) may also be protected as a trade secret.

Two "types" of information may explicitly not be protected as a trade secret according to the legal definition in Section 2 of the Trade Secrets Act:

- experience and skills which an employee has gained in the normal course of their employment; and
- information regarding a matter that constitutes a criminal offence or other serious wrongdoing.

All other types of information may, in principle, qualify for trade secret protection, as long as the information fulfils the requirements for protection in Section 2.

1.3 Examples of Trade Secrets

No specific types of information are enumerated as examples of protectable trade secrets in the Trade Secrets Act.

However, as Sweden has had trade secret legislation since 1919, there is a significant body of case law on what specific types of information are generally protectable as trade secrets – for example, a bank's internal documents concerning when to issue credits to customers (NJA 1999 s. 469), a business plan, marketing plan and financial plan for a new business (NJA 1998 s. 663) and the technical design documents for a boat (RH 2002:11).

Modern Swedish trade secret jurisprudence has granted a wide variety of different types of information protection as a trade secret. Customer information broadly speaking appears to be the most common type of trade secret being litigated in Sweden currently – eg, customer databases with contact information (NJA 2001 s. 362). The preparatory works to the Trade Secrets

Act also specifically mention market research, market planning, pricing calculations and plans for advertising campaigns as typical examples of information that commonly constitutes trade secrets. Source codes and computer programs may also constitute trade secrets.

1.4 Elements of Trade Secret Protection

The Trade Secrets Act offers trade secret protection to information that qualifies for protection according to Section 2.

- The information must concern the business or operational circumstances of a trader's business or a research institution's activities – the definition of business is broad and covers all natural and legal persons that professionally run an operation of an economic nature, regardless of whether or not it aims to make a profit. The definition of research institution covers both public and private research institutions and is assumed to be broad but has not yet been the subject of case law (following the implementation of the Trade Secrets Directive in 2018).
- The information must, either as a body or in the precise configuration and assembly of its components, not be generally known or readily accessible to persons who normally have access to information of the type in question – information unrelated to the business or institution can thus not constitute a trade secret. However, under certain circumstances, generally known information can be organised in a way that qualifies it for protection as a trade secret – eg, a large list of customers with information that is in principle publicly available. It also means that the group of people with access to the information has to be limited, definable and closed in the sense that the people with access to it cannot be unreservedly authorised to use or pass it on.
- The trade secret holder must have taken reasonable steps to keep the information secret – reasonable steps can be that the trade secret holder has established confidentiality agreements, rules of internal procedure and/or special access rights to the information.
- The disclosure of the information must likely lead to competitive injury to the holder, in order for the information to qualify as a trade secret – the trade secret information must thus have objective commercial value on account of the information being secret.

1.5 Reasonable Measures

"Reasonable steps" as a prerequisite for trade secret protection was introduced in 2018 with the Trade Secrets Act, implementing the Trade Secrets Directive. The previous Swedish legislation did not explicitly require reasonable precautions, and it was commonly considered sufficient that people with access to the information understood from its character that it was intended to be a trade secret. Swedish trade secret case law generally reflected this understanding (NJA 1998 s. 663).

According to the preparatory works to the Trade Secrets Act, reasonable steps demands that the trade secret holder has been active in protecting the information, but the activity does not have to be extensive and depends largely on the kind of information. Reasonable steps can be instructions on how trade secrets should be handled in the workplace (including confidentiality and non-disclosure agreements), or that trade secrets are only accessible to those with special competence in the organisation. However, it is not enough that employees or others should just understand from the character of the information that it should be kept confidential. The Swedish legislator has understood the requirement as one of substance rather than form.

There is not yet much case law on what concrete actions constitute reasonable steps in this regard. However, courts have so far considered confidentiality agreements with employees and franchisees to constitute reasonable steps (District Court judgment given on 26 of March 2020 in case T-2921-18). Confidentiality clauses in employment agreements have also been considered reasonable steps (Labour Court judgment given on 13 January 2021 in case B 42/20, AD 2021 nr 1).

Ultimately, it will be the CJEU that decides what is required by trade secret holders to protect the confidentiality of their information.

1.6 Disclosure to Employees

The disclosure of a trade secret from the trade secret holder to an employee does not affect the trade secret's protection, as long as the information still qualifies for protection according to Section 2. However, the employees who are given access to the information must not be permitted to freely disclose or use the information.

In order to guarantee that the disclosure of a trade secret to an employee does not negatively impact the protection of the trade secret, the trade secret holder should take active measures to make clear to the employee that the trade secret information is secret and may not be shared. This can be done through written or verbal instructions (with documented written instruction being preferable), and through confidentiality clauses in employment agreement.

A rule of thumb is that the secret should not be available to employees other than those who need it in order to conduct their work.

Similarly, the disclosure of a trade secret from the trade secret holder to a consultant or another third party does not affect the trade secret's protection, as long as the information still qualifies for protection according to Section 2. As a practical matter, however, the more and wider the information is shared, the higher the demands for secrecy become, and the stricter the confidentiality and non-disclosure agreements should be drafted in order to minimise risk to the integrity of the trade secret.

1.7 Independent Discovery

Independent discovery and reverse engineering are natural parts of product and service development in many industries and markets, and are recognised as such in the structure and provisions of the Trade Secrets Act.

Independent discovery and reverse engineering should, in principle, not affect the existence and possible protection of trade secrets. For example:

- Company A is the trade secret holder of certain information about a technical solution to detect fissures in bridges;
- Company B's independent discovery of similar or even theoretically identical information means that Company B may use this information in any way relevant under the Trade Secrets Act, including by using the information or disclosing it freely;
- Company A has developed and sells a sensor to detect fissures in bridges; the sensor functions according to a system that is a trade secret and known only by Company A;
- Company B is allowed to conduct reverse engineering on the sensor (unless Company B has agreed contractually not to do so); Company B may use the information accessed through reverse engineering freely.

In the example above, Company B's act of independent discovery, or reverse engineering, does not affect that information's possible protection as a trade secret for the trade secret holder Company A, as long as Company B keeps the

information secret. But if Company B decides to disclose the information freely, this means Company A's trade secret no longer qualifies for protection under Section 2 since the information is "generally known". The same information may therefore, in theory, be protected as a trade secret by several different trade secret holders, as a result of the companies' independent research and development or reverse engineering.

It may often be advisable to document independent discovery or reverse engineering work in order to be able to establish that this was indeed the way in which the information came to be known by Company B, rather than through misappropriation of trade secrets from Company A.

1.8 Computer Software and Technology

Neither computer software, source code nor technology broadly speaking enjoy any kind of unique protection in the Trade Secrets Act. However, the Swedish legislator is currently considering new revisions to the Act to specifically protect "technical trade secrets" that may correspond to technology (DS 2020:26 *Bättre skydd för tekniska företagshemligheter*). This new legislation only concerns criminal sanctions against trade secret misappropriation and has not yet been adopted into law.

1.9 Duration of Protection for Trade Secrets

Trade secret protection under the Trade Secrets Act has no time limit. The information retains its protection as a trade secret as long as the qualifications in Section 2 are fulfilled.

The effect of the disclosure of a trade secret depends on who discloses the trade secret and how it is disclosed.

If the trade secret holder discloses information without conditioning the disclosure on the trade secret not being disclosed further (ie, through a confidentiality or non-disclosure agreement), the information no longer qualifies for protection under Section 2 since the holder has not taken reasonable steps to keep the information secret. This applies regardless of whether the trade secret was disclosed to one person or more broadly, and regardless of whether the disclosure was accidental or intentional.

If someone other than the trade secret holder discloses the information, the information does not lose its protection unless and until it becomes "generally known" in the relevant circles according to Section 2. There is no specific grace period in this regard, and trade secret holders should act with all due haste when finding evidence of third party illegal disclosure in order to make sure further disclosure is stopped before the information becomes generally known.

Trade secret information may be shared between a trade secret holder and its employees, consultants or business partners and still retain its status as a trade secret, through a "controlled disclosure" if there are contractual agreements in place (confidentiality and non-disclosure agreements) that guarantee that the Section 2 qualifications for trade secret protection are still met.

1.10 Licensing

Trade secrets may be commercialised, for example through licensing agreements between the trade secret holder and a licensee. However, there are no such explicit provisions in the Trade Secrets Act, and the licensor and licensee must instead rely on general principles when entering into commercial relations concerning trade secrets.

For the specific purpose of protecting and commercialising trade secrets, the licensing agreement should contain rigorous confidentiality and non-disclosure clauses to make sure that the secret is not further disclosed (which could lead to the trade secret information becoming "generally known" in the relevant field), and should include detailed routines for how the licensee should keep the information secret in its business (in order for the trade secret holder/licensor to be able to show that reasonable steps have been taken to protect the information).

1.11 What Differentiates Trade Secrets from Other IP Rights

Trade secrets are not considered a traditional IP right in Sweden and there are many differences between trade secret protection and protection as an IP right (patent, copyright, trade mark, design, etc). The most relevant of these differences are as follows.

- An IP right constitutes an exclusive right to use, for example, a patented invention (in a certain country, during a certain time period). Trade secret protection on the other hand only protects against the misappropriation of trade secrets and does not, for example, protect against independent discovery and reverse engineering.
- IP rights have time limits (although some rights can be extended indefinitely). A trade secret has no time limit as long as the qualifications in Section 2 of the Trade Secrets Act are fulfilled.
- Many IP rights need to be registered with a national Patent and Trademark Office, or with an international body like the EUIPO. This is not the case for trade secrets, the protection of which is created without any formalities.
- The Trade Secrets Act does not offer trade secret holders many of the legal tools included in Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (Enforcement Directive), such as infringement investigations, which have been implemented in all national IP laws. This means that many of these tools cannot be used in litigation solely concerning trade secret misappropriation.
- Litigation concerning trade secrets is not under the exclusive jurisdiction of the Swedish specialist IP courts, the Patent and Market Court and the Patent and Market Court of Appeal.

1.12 Overlapping IP Rights

An act of misappropriation of trade secrets often simultaneously constitutes an act of IP infringement. As an example, an employee's disclosure of customer information (that constitutes a trade secret) may also constitute copyright infringement if the customer information constitutes a database work or sui generis database and a copy of the database is made in the act of disclosure, or if the disclosure constitutes a making available to the public under the Copyright in Literary and Artistic Works Act (SFS 1960:729).

It is possible to assert trade secret rights in combination with other intellectual property rights in litigation, according to Chapter 14 of the Code of Judicial Procedure. In fact, this is commonly done in Swedish litigation. If the trade secret misappropriation and IP rights infringement is connected, it would be considered highly unusual not to seek to have the cases handled jointly in this manner, and the court may under certain circumstances decide on joint handling even if a party disagrees.

In practice, the ability to combine several rights in the same proceedings may be curtailed by conflicting exclusive jurisdictions such as that of the Labour Court and the IP courts.

1.13 Other Legal Theories

It is possible to bring claims relating to trade secrets, broadly speaking, according to other legal theories than trade secret misappropriation under the Trade Secrets Act.

Fiduciary Duty of an Employee

Employees have a duty of loyalty towards their employer, so it is possible to bring an action against employees that disclose information in order to damage their employer. This is possible even if the information does not qualify as a trade secret. However, the duty of loyalty ends with the employment. An action on the basis of a breach of the fiduciary duty can therefore not be brought against a former employee that discloses information to damage the employer after the employment has ended. Instead, such action has to be brought on the basis of trade secret misappropriation.

Contract

It is also possible to act on the basis of legally binding agreements, such as confidentiality and non-disclosure agreements or exit agreements, if the other party has breached the agreement and that breach constitutes a misappropriation of trade secrets.

1.14 Criminal Liability

Two acts of trade secret misappropriation are criminalised under the Trade Secrets Act.

- According to Section 26, corporate espionage is the act whereby someone intentionally and unlawfully obtains access to a trade secret. This generally excludes employees, consultants and business partners who have lawful access to the information, but someone that accesses the information without permission is, in principle, subject to the sanction. Aggravated corporate espionage can result in imprisonment of up to six years, but such penalties are highly unusual.
- According to Section 27, unlawful dealing in a trade secret is the act whereby a person intentionally acquires a trade secret, with knowledge that the person providing it, or any person prior to him, has obtained access to it through corporate espionage. Aggravated unlawful dealing in a trade secret can result in imprisonment of up to four years, but again such penalties are highly unusual.

Two additional criminal sanctions for the misappropriation of trade secrets are currently contemplated for inclusion in the Trade Secrets Act in DS 2020:26 *Bättre skydd för tekniska företagshemligheter*: the unlawful use of trade secrets and the unlawful disclosure of trade secrets. In both cases, the new criminal sanctions target criminal activity by a person with legal access to the trade secret, thus supplementing the existing criminal provisions that only target criminal activity by a person without legal access to the trade secret.

Additionally, under certain circumstances trade secret misappropriation may fall under the general criminal provision breach of trust in Chapter 10 Section 5 of the Swedish Criminal Code. Breach of trust is the act whereby a person in a position of trust – usually a high ranking official – abuses their position of trust and thereby causes a loss for the principal. Applied specifically to trade secret misappropriation, the abuse has to be in direct relation to the position of trust and the trade secret has to be accessed as a result of the person's position. Aggravated breach of trust can result in imprisonment of up to six years, but such penalties are highly unusual.

There is no formal bar against a trade secret holder pursuing both civil and criminal claims simultaneously – for example, a criminal case against the person who committed corporate espionage by disclosing a trade secret to a third party competitor, and a civil case against

the third party competitor for the misappropriation of trade secrets through subsequent use of the disclosed trade secret. It is highly uncommon for parties themselves to prosecute a claim of criminal liability. Instead, suspected crimes are reported to the authorities. The crimes discussed above fall within the purview of the public prosecutors.

1.15 Extraterritoriality

The Swedish courts have jurisdiction to hear a claim of misappropriation abroad if the defendant is domiciled in Sweden. Under Art 7 of Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast), the courts may have jurisdiction even if the defendant is not domiciled in Sweden but that depends on the facts of the case. A claimant who wishes to bring a claim based on misappropriation abroad will generally not be required to do anything other than if the claim pertained to misappropriation in Sweden. Under the applicable conflicts of law rules, Swedish law may apply to misappropriation that takes place abroad – for example, if both the misappropriating party and the trade secrets holder have their habitual residence in Sweden.

There is also a measure of extraterritoriality in the misappropriation concept. Under Section 3 of the Trade Secrets Act, the import or export of goods, the design, characteristics, functioning, production process or marketing of which benefits significantly from a misappropriated trade secret, is an independent act of misappropriation.

2. MISAPPROPRIATION OF TRADE SECRETS

2.1 The Definition of Misappropriation

According to Section 3 of the Trade Secrets Act, misappropriation of a trade secret is when someone does the following without the consent of the trade secret holder:

- accesses, appropriates or otherwise acquires the trade secret;
- uses the trade secret; or
- discloses the trade secret.

The first type of misappropriation concerns different ways in which a person can obtain the trade secret information for their own use. “Accessing” and “otherwise acquiring” a trade secret are broad terms that cover various circumstances where trade secret information is intentionally obtained by someone who does not have lawful access to the information (corresponding to the criminal sanction corporate espionage). “Appropriating” a trade secret in this context means that a person who already has lawful access to the trade secret information (for example, by being an employee) appropriates that information by making it his own – for example, by copying trade secret information from a computer at work to a USB drive and transferring it to a personal computer at home (without having any work-related reason to do so).

The second type of misappropriation concerns someone other than the trade secret holder commercially using the trade secret in their own business. An employee using the information privately therefore falls outside the scope of use. Use of a trade secret also covers the circumstance where a person manufactures goods, the design, characteristics, functioning, production process or marketing of which significantly benefits from a misappropriated trade secret. The same applies when a person offers such goods

for sale, places them on the market, or imports, exports or stores them for these purposes.

The third type of misappropriation is when someone discloses a trade secret to a third party.

Under Section 4 of the Trade Secrets Act, misappropriation is only actionable if it is unjustified. This is a broad exception meant to allow the use and disclosure of trade secrets where this objectively appears justified. Examples of this include the use or disclosure of trade secrets in court proceedings where doing so is necessary to protect rights, providing documents or information where there is a legal obligation to do so, and whistle-blowing.

2.2 Employee Relationships

Employees have a fiduciary duty towards their employer, but it is advisable for employees to sign confidentiality undertakings with respect to the employer's information.

The misappropriation of trade secrets by an employee is, in principle, dealt with in the same way as a misappropriation by a third party under the Trade Secrets Act.

Both an employee and a third party may misappropriate in various ways according to Section 3, even if certain kinds of violations are more commonly carried out by employees (misappropriation through appropriation) while other kinds of violations are more commonly carried out by a third party (misappropriation through use).

There are, however, important differences when dealing with employees' misappropriation. As for the employee's liability, under Section 7, an employee who intentionally or negligently misappropriates a trade secret of which they learned in the course of their employment, under such circumstances that they knew or should have known that they were not permitted to disclose it, shall compensate the employer for the loss incurred as a result of the action. Importantly, the Swedish trade secret legislation has traditionally been understood to mean that an employee is allowed to use trade secret information in any way he or she chooses after leaving the employment. This follows from Section 7 second paragraph, which states that an employee is only liable for misappropriation through use or disclosure following the termination of employment if there are "exceptional reasons" for holding the former employee liable.

Exceptional reasons may, however, be a somewhat misleading term as such exceptional reasons are often found to be established in trade secret litigation – for example, if the employee planned and prepared their subsequent misappropriation during their employment.

Additionally, the provision for exceptional reasons in Section 7 second paragraph is not legally binding if the parties have agreed otherwise in contract – for example, by entering into a customary non-disclosure agreement that clearly prohibits the misappropriation of trade secrets in the time after the termination of the employment.

2.3 Joint Ventures

There is no specific obligation between joint venturers in respect of trade secrets under the Trade Secrets Act. The general rule on trade secrets shared in confidence applies, if the requirements set out in that rule are met.

However, joint ventures commonly lead to the creation of jointly held trade secrets, which sometimes present complicated legal questions since such joint control is not governed by the Trade Secrets Act and there is limited guidance in Swedish law. Parties should thus endeavour to agree from the outset on how any jointly held secrets should be treated.

A party that enters into a joint venture and agrees with the other party that there is confidentiality between the parties does not have to repeat this every time a trade secret is disclosed in the course of the venture. The joint venturer is bound by the initial confidentiality agreement but the requirement of reasonable steps should be borne in mind and care should be taken to ascertain that the other party understands what information is confidential.

2.4 Industrial Espionage

Section 26 covers corporate espionage (see **1.14 Criminal Liability**).

3. PREVENTING TRADE SECRET MISAPPROPRIATION

3.1 Best Practices for Safeguarding Trade Secrets

As set out above, a trade secret holder must take reasonable steps to protect the information in order for it to qualify for trade secret protection.

Basic best practices recognised in different industries and markets in Sweden to ascertain that reasonable steps are followed include the following:

- including confidentiality clauses in employment agreements, consultancy agreements and commercial agreements like joint ventures;
- educating and instructing employees, consultants and business partners on how trade secrets are to be handled in the workplace, with a special focus on digital storage and access; compartmentalising different levels of trade secret information in internal data systems and physical collections, and only granting employees, consultants and business partners access to trade secrets at the different levels if access is strictly needed; and
- keeping records on who has access to information, especially tracking data traffic.

3.2 Exit Interviews

Exit interviews for departing employees are common in certain industries, especially for high-level employees who are likely to have access to significant amounts of trade secrets.

Since written assurance of confidentiality cannot be required from the departing employee at the time of the exit (ie, such assurances cannot be forced on the departing employee in order to "allow" the employee to leave), the exit interview should be viewed as a reminder to the employee of his or her existing obligations towards the employer post-termination. It is therefore important that confidentiality clauses are included in the employment agreement from the start of employment, or as soon as possible. In the context of exit interviews, it is not prohibited to ask about the employee's new position.

4. SAFEGUARDING AGAINST ALLEGATIONS OF TRADE SECRET MISAPPROPRIATION

4.1 Pre-existing Skills and Expertise

The Trade Secrets Act recognises an important distinction between an employee's own general knowledge and skill and trade secrets belonging to the employer.

Section 2 second paragraph explicitly states that experiences and skills gained by an employee in the normal course of their employment cannot be a trade secret. In the literature, such personal experiences and skills are characterised by not being transferable through instructions, while a trade secret is a piece of information that

can easily be transferable to another employee through instruction. Generally, personal experiences and skills are also not specific to the workplace.

There is no doctrine of "inevitable disclosure" in Swedish trade secret jurisprudence. There is no indication that a court would ever assume that a former employee will misappropriate the former employee's trade secrets in his or her new employment, and such a claim would go against the foundational principles of Swedish trade secret and labour law.

Employers will instead have to rely on non-disclosure and non-compete clauses in high-level employees' employment agreements to protect their interests in this regard. Concerning non-compete clauses specifically, Swedish courts apply these restrictively and generally do not allow them to last longer than 18 months (and in many cases, 18 months would be considered wildly excessive).

4.2 New Employees

Swedish employers may use the following best practices to minimise the likelihood that they will be subject to a trade secret misappropriation claim from a new employee's former employer:

- check whether the employee is bound by any non-disclosure or non-compete agreement;
- if the company has entered into non-compete agreements with employees that are not enforceable (because the duration is too long or the scope is too broad), the employee and the new employer may consider bringing this up with the former employer in order to minimise the risk of subsequent litigation; and
- be flexible in structuring the new employee's work during the onboarding process, or longer, if any legal or public relations risks could be construed from the employee's previous engagement.

5. TRADE SECRET LITIGATION

5.1 Prerequisites to Filing a Lawsuit

According to the Trade Secrets Act or other Swedish law, there are no prerequisites or preliminary steps that a trade secret holder must take before taking civil action based on the misappropriation of trade secrets and filing a lawsuit.

If the trade secret holder is represented by a member of the Swedish Bar Association (*advokat*), the applicable ethics rules dictate contacts between the lawyer and defendant before a suit is filed, in order to let the defendant give its position on the matter (commonly through cease and desist letters). However, the ethics rules do not demand such contacts in matters where a preliminary injunction is sought ex parte, for example, since contacting the defendant in such situations would rob the ex parte injunction of its intended effect.

5.2 Limitations Period

There are limitation periods under Section 24 of the Trade Secrets Act.

A claim for damages under the Trade Secrets Act may only pertain to loss that occurred during the five years immediately preceding the commencement of the action. The limitation is counted from when the actual loss occurred and not when the trade secret holder found out about the loss. Damages for losses suffered prior to the five years are barred.

A claim for an injunction or other measures under the Trade Secrets Act must be commenced within five years of the date on which the trade secret holder became aware, or should have become aware, of the misappropriation or imminent misappropriation of the trade secret on which the action is based. When the holder

should have become aware of the misappropriation is decided on the basis of how the trade secret was misappropriated and what control measures the holder could have taken to realise the misappropriation.

These two different limitations do not necessarily coincide. An injunction claim could, for example, be barred because the misappropriation happened more than five years ago, and the holder should have been aware of this, while it is still possible to claim damages for losses occurred within the five-year period if such losses occurred continuously over the years.

5.3 Initiating a Lawsuit

Following the cease and desist phase (if applicable), trade secret owners initiate a lawsuit simply by filing a summons application with the applicable court. As a practical matter, however, there are several issues that a trade secret holder should tend to before filing a lawsuit.

The trade secret holder or its legal representative should:

- pay the court fees;
- file a physical power of attorney with the summons application (if applicable); and
- file a physical bank guarantee for costs incurred due to a wrongly issued preliminary injunction (if applicable).

A Swedish court will generally not issue a summons or a preliminary injunction, nor make other procedural decisions, before the above documentation has been presented in physical form to the court.

5.4 Jurisdiction of the Courts

Different Swedish courts have jurisdiction in cases concerning the misappropriation of trade secrets under the Trade Secrets Act, depending on the parties involved and the subject matter of the lawsuit.

Courts of General Jurisdiction

The district court at the domicile of the defendant has general jurisdiction in cases of misappropriation of trade secrets where the defendant is not a current or former employee of the claimant.

The district court handles the case according to the normal Swedish procedural rules in the Code of Judicial Procedure. The district court's judgments are appealed to the competent Court of Appeal (leave to appeal is needed and commonly granted), with the Supreme Court being the final instance (leave to appeal is needed and is generally not granted).

Labour Court (as the Court of First Instance)

The Labour Court in Stockholm has exclusive jurisdiction in cases of misappropriation of trade secrets where the defendant is a current or former employee of the claimant, and the employer is bound by a collective labour agreement with a trade union that the employer entered into for itself. The Labour Court's judgment cannot be appealed.

District Court (Labour Dispute)

The district court at the domicile of the defendant has jurisdiction in cases of misappropriation of trade secrets where the defendant is a current or former employee of the claimant, and the employer is not bound by a collective labour agreement with a trade union that the employer entered into for itself.

The district court handles the case in accordance with the procedural rules in Swedish labour law. The district court's judgments are appealed to the Labour Court (leave to appeal is needed and commonly granted).

Patent and Market Court

Claims for the misappropriation of trade secrets are not subject to the exclusive jurisdiction of the Swedish specialist IP courts, the Patent and Market Court and the Patent and Market Court of Appeal in Stockholm. It is, however, not uncommon for cases concerning the misappropriation of trade secrets to also concern IP rights infringement (most commonly copyright or patent infringement), which are under the exclusive jurisdiction of the specialist courts.

IP rights infringement claims may be handled jointly with claims for the misappropriation of trade secrets before the specialist courts, as long as the defendant is not a current or former employee. In such cases, the Patent and Market Court's judgments are appealed to the Patent and Market Court of Appeal (leave to appeal is needed and commonly granted), with the Supreme Court being the final instance (leave to appeal is needed and is generally not granted).

5.5 Initial Pleading Standards

The pleading standards applicable to claims for the misappropriation of trade secrets in Sweden are generally the same standards applicable in other Swedish litigation, including IP litigation.

There are few formalities under Swedish procedural law that apply to a party's calling of evidence. Generally speaking, all kinds of evidence can be called by the parties, and freely evaluated by the court.

A trade secret owner may allege facts in a summons application based on information and belief (according to the authors' understanding of this common law legal term), without substantiating every fact with evidence, especially during the preliminary injunction phase. There are no formal limitations on what can be alleged but if evidence is not offered the court may ultimately reject the claim on the merits. There may be sanctions in very serious cases of unsubstantiated claims.

5.6 Seizure Mechanisms

In cases concerning the misappropriation of trade secrets, the court can order documents or objects containing misappropriated trade secrets to be handed over to the trade secret holder, according to Sections 17-20. The court can also order product recalls or have the products or documents destroyed, modified or subjected to any other measure aimed at preventing misappropriation. The court can only issue seizure orders based on Sections 17–20 in a final judgment.

During the preliminary injunction phase, the claimant must instead rely on the general seizure rules in the Code of Judicial Procedure. According to Chapter 15 Section 3, if a person shows probable cause to believe that he or she has a claim against another (in this case, a claim for the misappropriation of trade secrets), and if it is reasonable to suspect that the opposing party, by carrying on a certain activity, will hinder or render more difficult the exercise of the applicant's right, the court may order seizure measures suitable to secure the applicant's right. The general seizure rules are complicated to apply and may not be used as a substitute to an infringement investigation to simply secure evidence of the misappropriation of trade secrets (NJA 2017 s. 457).

5.7 Obtaining Information and Evidence

There is no discovery phase in Swedish litigation. Instead, there are two legal mechanisms available to obtain information and evidence to support a trade secret claim.

Document Production under Chapter 38 Section 2 of the Code of Judicial Procedure

Document production (edition) is used to obtain written evidence once a claim has been

brought. Anybody holding a written document that is assumed to be of importance as evidence can be ordered by the court to produce it. It is required that the party holds a specific document of importance for the case, so specific, identified documents may be sought but categories of documents can be sufficiently identified if properly delimited. Trade secret information is privileged in this respect, and a court will only order the production of trade secret documents if there are extraordinary reasons for the order. The courts are generally restrictive when it comes to breaking through the privilege.

Infringement Investigations According to Applicable IP Legislation

Infringement investigations, as prescribed in the Enforcement Directive, are not available under the Trade Secrets Act and are thus not (strictly speaking) available to support claims for the misappropriation of trade secrets. Infringement investigations are available in Swedish IP legislation, however. Since an act of misappropriation of trade secrets is often simultaneously an act of IP rights infringement, infringement investigations based on IP rights infringement nonetheless often have practical use also for claims for the misappropriation of trade secrets. An infringement investigation is granted by the court if the reasons for the measure outweigh the inconveniences and other harm it may cause the defendant.

Fact gathering outside the scope of these mechanisms is possible, but caution should be taken, since corporate espionage is criminalised (fact-finding missions should be limited to publicly available information about the defendant).

5.8 Maintaining Secrecy While Litigating

Documents received and produced by Swedish courts are generally publicly available to anyone that requests them. Similarly, hearings and trials before Swedish courts are open to the public. There are mechanisms available under the Trade Secrets Act as well as the Code of Judicial Procedure to ensure that trade secrets are kept secret in litigation and not disclosed to the public.

A party that discloses trade secret information in submissions to the court may request the court to mark the submission as secret, and not make the document publicly available, according to the Public Access to Information and Secrecy Act (2009:400). Similarly, a party that plans to disclose trade secret information in a public hearing or trial may request the court to have the hearing behind closed doors. The court usually grants such requests, and trade secrets disclosed in this manner are covered by secrecy.

There is, however, no possibility under the applicable Swedish legislation to keep the adverse party from having access to submissions that include trade secrets, or from being part of the hearing where trade secret information is discussed. In theory, access may be curtailed with respect to how the adverse party is given access. This power is fairly new, and the courts are expected to be very restrictive in its application.

A party or party representative who intentionally or negligently uses or discloses a trade secret learnt as a result of court proceedings is liable for losses resulting from the disclosure or use, according to Section 8 of the Trade Secrets Act. The same goes for anyone participating in a court proceeding behind closed doors and thereafter intentionally or negligently revealing trade secrets learnt during the proceedings.

5.9 Defending against Allegations of Misappropriation

There are several defences against allegations of trade secret misappropriation, with the most common being lack of protection (ie, the infor-

mation in question does not qualify as a trade secret), the absence of misappropriation, consent, that misappropriation was justified and, with respect to damages, that the necessary subjective element is not met, as well as various objections to the quantum of damages.

The burden of proof that the trade secret has been misappropriated rests with the claimant. In cases where claims for the misappropriation of trade secrets fail, it often comes down to a question of evidence and whether the claimant has been able to substantiate the alleged facts.

5.10 Dispositive Motions

According to Chapter 44 Section 2 of the Code of Judicial Procedure, courts can issue a default judgment (*tredskodom*) fully granting the claimant's claims if the defendant does not file a response to the summons application or does not attend court-ordered hearings.

Courts can only grant such default judgment motions if the case is amenable to out-of-court settlement. If any of the claims made by the claimant are of a nature that the parties cannot fully dispose of through contract, a dispositive motion cannot be issued. The administrative fine with which injunctive relief is combined is an exercise of public authority and is not amenable to settlement. If injunctive relief is sought, it will accordingly not be possible to grant a default judgment.

The courts have no power to grant the claim summarily if the defendant participates in the proceedings.

5.11 Cost of Litigation

Trade secret litigation generally involves significant amounts of evidence and legal argumentation, and may also include expert evidence. Trade secret litigation rarely costs less than EUR100,000 per instance, and often more.

According to Chapter 18 Sections 1 and 8 of the Code of Judicial Procedure, the losing party shall compensate the winning party's reasonable litigation costs, fully covering the costs of preparation for trial and presentation of the action, including fees for representation and counsel. In practice, this means the winning party is often awarded about 75–100% of its actual costs, which is considered high from an international perspective.

Members of the Swedish Bar Association (*advokat*) may not represent clients through a contingency fee arrangement, according to the applicable ethics rules.

Though a fairly new phenomenon on the Swedish legal market, litigation financing is available and is growing in relevance.

6. TRIAL

6.1 Bench or Jury Trial

The Swedish legal system does not use jury trials, except in cases concerning freedom of the press.

6.2 Trial Process

Litigation in Sweden generally follows the below procedure in cases concerning the misappropriation of trade secrets:

- summons application;
- defence;
- if applicable, preliminary injunction decided without a hearing. (If an ex parte injunction is sought, that is decided before the defendant is served the summons application.) A preliminary injunction may be appealed, commonly leading to a period of non-action at the first instance court while the injunction is being litigated;

- additional submissions;
- case management hearing – the court shall work actively for a settlement but if one cannot be reached the hearing is used to plan for the main hearing;
- if applicable, procedural decisions on the production of evidence, orders for information, etc;
- final submissions from the parties, with final lists of evidence; and
- final hearing.

Cases concerning the misappropriation of trade secrets may, in theory, be decided on the papers without a hearing but that requires that no witnesses are adduced and that neither party requests a hearing.

The proceedings are adversarial and not inquisitorial. In Sweden, witnesses give live testimony. The party calling the witness carries out a direct examination and the other party may cross-examine. The court may ask questions to the witnesses but normally only does so to confirm its understanding of answers given on direct or cross.

The hearing consists of three phases: opening statements where the facts and written evidence are presented; the verbal evidence phase in which testimony is given; and lastly the closing arguments.

Typical trade secret proceedings last about 12-18 months, or longer if the case involves significant amounts of evidence, at each instance.

6.3 Use of Expert Witnesses

Expert witnesses are allowed and commonly used in trade secret proceedings. Expert witnesses are generally called by a party and tasked to prepare an expert witness report, which the other party can comment on and call their own expert witness to counter, before the hearing. At the hearing, expert witnesses generally present their testimony like regular witnesses, but are invited to more freely present their findings (instead of only answering questions from counsel) before being cross-examined by the other party. There are no rules curtailing in what respects expert evidence can be adduced.

It is difficult to estimate the cost of expert witness testimony in trade secret cases, since the parties are free to call virtually whoever they wish, but the costs are generally tens of thousands of euros, rather than hundreds of thousands.

7. REMEDIES

7.1 Preliminary Injunctive Relief

Courts can issue preliminary injunctions if the following requirements in Section 14 of the Trade Secrets Act are fulfilled:

- the claimant proves that there is probable cause that a trade secret has been misappropriated (or misappropriation is imminent);
- the claimant proves that there is reasonable cause to believe that the other party, through continued misappropriation, will further diminish the value of the trade secret; and
- the claimant posts a bond, usually in the form of a bank guarantee (the general wording of which follows from case law and must not be limited in several significant ways) covering the defendant's potential damages (including loss of profit). There has recently been a development in Swedish case law, where courts routinely demand higher bonds in the range of several hundred thousand euros.

Preliminary injunctions remain in place until the case is finally decided, unless the court decides otherwise. Where the alleged misappropriation constitutes use of a trade secret, however, under certain circumstances the court may dismiss a

motion for an injunction preventing use of the trade secret, if the defendant posts a bond covering the compensation payable to the trade secret holder, and the defendant's continued use of the trade secret does not lead to disclosure of the trade secret.

7.2 Measures of Damages

There are several viable methods of calculating damages under the Trade Secrets Act. The damages granted shall cover the harm done to the claimant through the defendant's misappropriation; punitive damages or statutory fixed damages are not available. In all circumstances, the damages granted shall not be so low so as to make the misappropriation a financially better solution for the defendant than following the law.

When calculating damages in these cases, all relevant circumstances shall be taken into consideration. Claimants are granted wide latitude in fashioning their claim for damages according to different relevant models, such as:

- direct losses of the claimant, including customers or orders lost as a result of the defendant's misappropriation of trade secrets;
- savings enjoyed by the defendant from misappropriating the trade secrets; or
- the profits of the defendant from misappropriating the trade secrets.

When calculating damages, consideration shall also be given to the interest of the holder of the trade secret in preventing unjustified misappropriation of the trade secret, and to circumstances other than those of purely financial significance. A measure of non-financial damages is thus compensated.

Since damages are hard to prove in trade secret litigation in Sweden, there is a supplemental rule in Chapter 35 Section 5 of the Code of Judicial Procedure that allows the court to estimate the damage to a reasonable amount, if full proof of evidence is difficult or impossible to present. This supplemental rule is often leaned upon in litigation.

7.3 Permanent Injunction

Courts can permanently injunct a defendant from continuing the misappropriation of trade secrets under penalty of a fine, according to Section 12 of the Trade Secrets Act. The fine is set to an amount that is assumed to make the respondent follow the injunction, and is usually significant (if breached, however, the fine accrues not to the trade secret holder, but to the Swedish state).

Courts can also order products to be recalled from the market or have the products or documents destroyed, modified or subjected to any other measure aimed at preventing misappropriation, according to Section 17.

Courts cannot, however, issue an order that limits an employee's subsequent employment in order to protect the plaintiff's trade secrets; there is thus no doctrine of "inevitable disclosure" in Swedish trade secret jurisprudence.

Employers instead have to rely on non-disclosure and non-compete clauses in high-level employees' employment agreements to protect their interests in this regard. Concerning non-compete clauses specifically, Swedish courts apply these restrictively and generally do not allow them to last longer than 18 months (and in many cases, 18 months would be considered wildly excessive).

7.4 Attorneys' Fees

According to Chapter 18 Sections 1 and 8 of the Code of Judicial Procedure, the losing party shall compensate the winning party's reasonable litigation costs in civil litigation, fully covering the costs of preparation for litigation and participating in the proceedings, including counsel's fees

and the party's own work with the dispute. In practice, this means the winning party is often awarded about 75–100% of actual costs, which is considered high from an international perspective.

Awards of litigation costs are decided by the court directly in the judgment.

7.5 Costs

See **7.4 Attorneys' Fees**. Costs incurred for the proceedings are generally recoverable insofar as they are considered reasonable.

8. APPEAL

8.1 Appellate Procedure

As set out at **5.4 Jurisdiction of the Courts**, cases regarding the misappropriation of trade secrets may be decided by several different courts in Sweden, depending on the parties and especially whether the defendant is a current or previous employee of the claimant.

First instance judgments by district courts may be appealed to the competent Court of Appeals, or to the Labour Court. First instance judgments of the Patent and Market Court may be appealed to the Patent and Market Court of Appeal. In all these cases, the losing party can appeal within three weeks (leave to appeal is needed and commonly granted). Appellants often file a pro forma appeal within three weeks and are granted several additional weeks to file a full appeal.

As also set out at **5.4 Jurisdiction of the Courts**, in some rare cases of the misappropriation of trade secrets, the Labour Court is the first and only instance, whose judgment cannot be appealed.

Both parties can appeal, provided that they have lost to some extent.

Appeals entail a de novo examination of the case, but witnesses do not generally give live testimony in the appellate phase. The testimony is filmed in the court of first instance, and the second instance court will watch that recording.

Certain forms of orders may be appealed separately, but most orders may not.

From filing the appeal until a decision is made by the appellate court usually takes 12–18 months.

8.2 Factual or Legal Review

The Swedish appellate courts review factual and legal issues in cases concerning the misappropriation of trade secrets. It is a full de novo examination of the aspect of the judgment being appealed, which does not need to be the entire judgment.

As with first instance procedures, cases concerning the misappropriation of trade secrets may, in theory, be decided on the papers, but generally a new in-person hearing is conducted where the parties are allowed to argue their case and present their evidence (witness testimony is not conducted again; instead, recordings from the first instance hearing are played).

9. CRIMINAL OFFENCES

9.1 Prosecution Process, Penalties and Defences

To initiate criminal prosecution for trade secret misappropriation, a criminal complaint needs to be filed with the police or the Swedish Prosecution Authority. A prosecutor investigates and decides if charges are brought.

The potential penalties for the crimes are up to six years of imprisonment (see **1.14 Criminal Liability**). The defences available to the criminal defendant are the same as in civil cases.

10. ALTERNATIVE DISPUTE RESOLUTION

10.1 Dispute Resolution Mechanisms

It is generally possible to arbitrate trade secrets disputes, and it is not uncommon to do so. This assumes, however, that there is an arbitration specifically covering the trade secrets dispute. There has been an academic debate as to whether there are limits to arbitrability in this respect, but there are no cases to support this.

Arbitration will normally be quicker than court proceedings. According to statistics published by the Arbitration Institute of the Stockholm Chamber of Commerce (SCC), final awards were given within 12 months of the case being referred to the tribunal (which happens after all administration associated with appointing the tribunal and paying the advance has taken place) in 77% of arbitrations conducted under the SCC Rules in 2019. There is also the option of agreeing on expedited arbitration, in which case an award will normally be given within six months of the reference to the tribunal.

Cost-wise, an arbitration can be expected to be more expensive, particularly since the fees and expenses of the tribunal and, in the case of institutional arbitration, arbitration institute are borne by the parties. An advance is normally required, and the losing party will normally bear the costs.

The major advantage of arbitration over litigation is the speed with which the proceedings are conducted and the ability to choose arbitrators with expertise in the field of the dispute. A traditionally held view is that confidentiality is one of the benefits of arbitration, but there is no legal obligation to keep arbitration proceedings confidential unless the parties have specifically agreed on such an obligation (NJA 2000 p. 538). It is also noteworthy that Section 8 of the Trade Secrets Act, which restricts the use and disclosure of trade secrets received as a consequence of court proceedings, does not formally apply in arbitration.

Interim relief granted by a tribunal is not enforceable in Sweden, but the arbitration agreement does not bar a party from seeking interim relief from the courts. A tribunal cannot combine its award with administrative fines. An injunction awarded in arbitration can be combined with such fines by the enforcement authorities at the enforcement stage.

Contributed by: *Björn Rundblom Andersson, Hans Eriksson and Axel Seger,* ***Westerberg & Partners***

Westerberg & Partners is an IP and litigation boutique in Stockholm. The IP team consists of around 20 lawyers covering all areas within IP, including patents, trade secrets, copyright, trade marks and related areas such as media and entertainment law, and marketing law. The IP practice handles both contentious and non-contentious work, including portfolio management. Westerberg & Partners is a leading firm in the Swedish IP market in terms of the number of lawyers and the width and depth of the team members' experience.

AUTHORS

Björn Rundblom Andersson is a partner at Westerberg & Partners. His practice is focused on contentious patent and trade secret matters. He has extensive experience of representing clients before Swedish courts and in arbitration, and he frequently acts in matters with a cross-border element. Björn has authored articles and contributed to books in the fields of intellectual property and dispute resolution.

Hans Eriksson is a partner at Westerberg & Partners, where he advises and litigates on behalf of clients in a wide range of industries in the fields of copyright, trade secrets, trade marks, design, unfair marketing practices and media. He is a board member of AIPPI Sweden and a member of SFU and SFIR. Hans writes and lectures regularly on IP and related issues.

Axel Seger is an associate at Westerberg & Partners, where his practice is focused on intellectual property law and marketing law. He holds a law degree from Uppsala University and has studied law at the University of Minnesota Law School. Axel is a member of AIPPI and SFIR.

Westerberg & Partners

Regeringsgatan 48
Stockholm
Sweden

Tel: +46 8 5784 03 00
Fax: +46 8 5784 03 99
Email: info@westerberg.com
Web: www.westerberg.com

Trends and Developments

Contributed by:
Björn Rundblom Andersson, Hans Eriksson and Axel Seger
Westerberg & Partners see p.24

Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (the Trade Secrets Directive) was implemented in Swedish law in 2018 by the enactment of the Trade Secrets Act 2018, which replaced the Trade Secrets Act 1990.

The implementation of the Trade Secrets Directive introduced several important changes that are likely to shape Swedish trade secret jurisprudence for years to come. These and other current trends and developments are described below.

Reasonable Steps to Keep Information Secret

Under the Trade Secrets Act 1990, only information that the holder kept secret could be protected as trade secrets. This was considered to require a degree of activity from the holder to maintain the confidential nature of the information but there were no specific formalities that needed to be observed (eg, Labour Court, judgment given on 1 April 2020 in case B 73/19, AD 2020 No 18). It has been established practice of the Swedish courts to construe the confidentiality requirement rather generously for trade secrets holders. Tacit or implied instruction to keep information confidential has been considered sufficient and so has tacit conditions of confidentiality when trade secret information has been disclosed in commercial relationships.

The Trade Secrets Act 2018 implemented the Trade Secrets Directive's explicit requirement of "reasonable steps" to keep the information secret, under Article 2 (1) (c). The Swedish legislator understood the requirement of reasonable steps to be a more demanding standard than that of the Trade Secrets Act 1990. The principal effect, as the Swedish legislator understood it, is that it will no longer be sufficient that a recipient, in light of the nature of the information, should understand that the trade secret holder intends for the information to be kept secret by the recipient.

However, a prominent authority on Swedish trade secrets law (Professor Emeritus, Reinhold Fahlbeck) does not agree with the legislator and has even suggested that the reasonable steps requirement is less demanding than the previous standard. As of yet there is no Swedish court practice on the subject and ultimately it will be for the CJEU to provide clarity as to what the reasonable steps standard requires of holders of trade secret information. As the issue is central to any litigation concerning the misappropriation of trade secrets, the issue is likely to reach the CJEU in record time.

Until the CJEU has provided clarity, it is advisable for trade secret holders to never share information outside the company without a written non-disclosure agreement and to have confidentiality undertakings in place for employees who come into contact with trade secret information, as well as written policies or instructions on how to treat such information.

Expanded Misappropriation Concept

Under the Trade Secrets Act 1990, there was no criminal or civil liability for a party with lawful access to trade secrets who acquired the

information for himself or herself – for example, a disgruntled employee who plans to start a new competing business. In line with the Trade Secrets Directive, the Trade Secrets Act 2018 expanded the misappropriation concept to include such unlawful acquisition of trade secrets. This is an important addition as misappropriation through disclosure or use may often be more difficult to prove than the taking of the information, which can often be proven through evidence from the company's computer systems. This important development also makes misappropriation actionable before actual use or disclosure has taken place, and thus enables trade secret holders to take action before more serious damage is done to the trade secret.

The first ruling on this issue was delivered by the Labour Court on 13 January 2021 (case no B 42/20, AD 2021 No 1), in which the court held that it was not proven that a former employee had made copies of the trade secrets with the intention to make them his. The court followed the legislator's intention that a distinction be made between copies an employee makes to facilitate his or her loyal work for the employer, and copies made with the intention of taking ownership of the trade secret. The burden to prove that the necessary intent was at hand appears to rest with the trade secret holder, but it should arguably suffice that the intent can be inferred from the circumstances surrounding the making of the copies.

Expanded Criminalisation Proposed

In December 2020, a government committee proposed criminalising the use or disclosure of trade secret information of a "technical nature" to which the misappropriating party had lawful access. This has been a controversial issue in Swedish trade secrets law since 2003, when a much-discussed judgment confirmed that an employee who had lawful access to the information in question could not be held criminally liable for corporate espionage (Svea Court of Appeal judgment given on 20 October 2003 in case no B 5221-03). Legislation has previously been proposed on two separate occasions by government committees, but no bill was submitted to the Swedish parliament on either occasion.

The 2020 proposal distinguishes itself from previous proposals in that the criminalisation is limited to trade secret information of a technical nature, and is thus more limited in scope than earlier proposals. It remains to be seen whether the government will proceed and put a bill before parliament.

Preliminary Relief

The Trade Secrets Act gives the court power to award preliminary injunction. The general rules on interim relief in the Swedish Code of Judicial Procedure apply in parallel, which means that the courts also have the power, for example, to order the interim seizure of documents or computer storage media containing trade secret information. It has not been uncommon to seek a preliminary injunction in parallel with the interim seizure of computer storage media and/or printed documents. The latter interim relief is in that event given to secure the merits of a claim, by giving the claimant possession of the computer storage media or the documents, or for their destruction.

In a 2020 decision, the Labour Court declined to grant such an interim seizure of computer storage media with reference to a balance of convenience test (judgment given on 14 April 2020 in case B 29/20, AD 2020 No 21). In that case, the claimant sought to be given possession of computer storage media that included the claimant's misappropriated trade secrets. The Labour Court reasoned that the computer storage media included both the claimant's trade secrets and significant amounts of other

data that the defendant needed in his business. The Labour Court further reasoned that, since the trade secrets were digital and remained in the possession of the claimant, the claimant had less reason to need to take possession of the computer storage media. Under all circumstances, the claimant was protected from further misappropriation of the information during the course of the proceedings by virtue of the preliminary injunction issued against the defendant. Following this development, it can be expected that it will be harder to be granted both preliminary injunction and interim seizure in the future.

Obtaining Evidence

Just like its predecessor, the Trade Secrets Act 2018 does not provide any remedies for securing evidence about infringement, similar to the infringement investigation orders and information orders available under Swedish IP legislation. In practice, Swedish trade secret litigants commonly tried to accomplish the same result by seeking interim relief in the form of the seizure of property that was reasonably considered to hold misappropriated information, and then subsequently requesting to be allowed to review the materials so seized. This practice was based on the general provision on interim relief in Chapter 15 of the Code of Judicial Procedure. However, in a 2017 decision, the Supreme Court ruled that the interim relief available under the Code only could be granted in order to secure a remedy on the merits and not to secure procedural claims (NJA 2017 s. 457).

The ruling effectively closed the door on this practice and, as the law currently stands, a trade secrets holder's only means of obtaining evidence by way of court order is to seek document production. This is a significant limitation of the ability to protect trade secrets as compared to IP rights, but this limitation is mitigated by the fact that trade secrets disputes often involve overlapping copyrights, databases or patents, for which the remedies in question are available and commonly used.

Vicarious Liability for the Misappropriation of Trade Secrets

Under Swedish damages law, companies generally bear vicarious liability for damages caused by their employees. The other side of that vicarious liability is that employees cannot be held liable for damages caused in their employment, unless there are exceptional reasons for doing so. In recent years, the Labour Court has applied this concept for trade secret misappropriation and ruled in a 2020 judgment (given on 26 February 2020 in case B 34/19, AD 2020 No 11) that a former employee could not be held liable for using trade secrets belonging to his first employer for the benefit of his new employer, unless there are exceptional reasons. In that case, several former employees of the claimant were named defendants but only one was held liable. The court held that the fact that he intentionally disclosed trade secrets to his new employer was sufficient to constitute exceptional reasons.

Contributed by: *Björn Rundblom Andersson, Hans Eriksson and Axel Seger,* ***Westerberg & Partners***

Westerberg & Partners is an IP and litigation boutique in Stockholm. The IP team consists of around 20 lawyers covering all areas within IP, including patents, trade secrets, copyright, trade marks and related areas such as media and entertainment law, and marketing law. The IP practice handles both contentious and non-contentious work, including portfolio management. Westerberg & Partners is a leading firm in the Swedish IP market in terms of the number of lawyers and the width and depth of the team members' experience.

AUTHORS

Björn Rundblom Andersson is a partner at Westerberg & Partners. His practice is focused on contentious patent and trade secret matters. He has extensive experience of representing clients before Swedish courts and in arbitration, and he frequently acts in matters with a cross-border element. Björn has authored articles and contributed to books in the fields of intellectual property and dispute resolution.

Hans Eriksson is a partner at Westerberg & Partners, where he advises and litigates on behalf of clients in a wide range of industries in the fields of copyright, trade secrets, trade marks, design, unfair marketing practices and media. He is a board member of AIPPI Sweden and a member of SFU and SFIR. Hans writes and lectures regularly on IP and related issues.

Axel Seger is an associate at Westerberg & Partners, where his practice is focused on intellectual property law and marketing law. He holds a law degree from Uppsala University and has studied law at the University of Minnesota Law School. Axel is a member of AIPPI and SFIR.

Westerberg & Partners

Regeringsgatan 48
Stockholm
Sweden

Tel: +46 8 5784 03 00
Fax: +46 8 5784 03 99
Email: info@westerberg.com
Web: www.westerberg.com

TAIWAN

Law and Practice

Contributed by:
Fred C.T. Yen and Amy N.Y. Ho
Tai E International Patent & Law Office see p.220

CONTENTS

1. LEGAL FRAMEWORK

1.1 Sources of Legal Protection for Trade Secrets

In Taiwan, the Trade Secret Act (TSA) was enacted in 1994, and since then has been amended twice, respectively in 2013 and 2020. The current TSA mainly governs the following items:

- the required elements of a trade secret;
- ownership of a trade secret;
- the licensing of a trade secret;
- misappropriation of a trade secret;
- the civil remedy and criminal penalty for the misappropriation of a trade secret;
- the issuance of a protective order during criminal investigation.

In addition, other laws relating to the protection of trade secrets may apply concurrently, including the Civil Code, Code of Civil Procedure, Criminal Code, Code of Criminal Procedure and Intellectual Property Case Adjudication Act (IPCAA). The Civil Code and Criminal Code generally provide for the tort law, obligations of contract and criminal penalties applied to disclosure of commercial or industrial secrets of others without a justifiable reason. The IPCAA specifically governs the adjudication of intellectual property disputes. The TSA and IPCAA prevail over the Civil Code, the Code of Civil Procedure, the Criminal Code and the Code of Criminal Procedure in trade secret litigations when there are issues of concurrency. There is no difference in the protection of trade secrets at national and local levels in Taiwan.

1.2 What Is Protectable as a Trade Secret

In Taiwan the information that can be protected under the TSA is defined as "any method, technique, process, formula, programme, design, or other information that may be used in the course of production, sale or operation" and must meet the following requirements:

- secrecy;
- economic value; and
- reasonable measures to maintain secrecy (Article 2 of the TSA).

1.3 Examples of Trade Secrets

A trade secret can be technical or business information, as long as it meets the definition provided by Article 2 of the TSA. Some examples of technical information are manufacturing processes, formulations or compositions of chemicals, computer software, design drawings, manufacturing parameters and testing reports or data. Examples of business information include a company's customer list, distribution locations, product prices, purchase costs, transaction reserve prices, personnel management, cost analysis, and other business-related information.

1.4 Elements of Trade Secret Protection

The three required elements of trade secret protection are explained as follows.

- "Secrecy" requires that a "trade secret is not known to the persons generally involved in the information of this type." This required element differs from the absolute novelty requirement for patents. The determination of secrecy is based on the industry standards. If people in the relevant field are aware of the information, the secrecy requirement of such information would not be satisfied.
- "Economic value" requires that a trade secret be of actual or potential economic value, including technical information at the research stage. For example, unsuccessful experimental data would be considered to be of economic value since it could save time or costs for competitors.
- "Reasonable measures" require that a trade secret-owner should have taken reasonable

measures to maintain secrecy in the first place. If a third party could easily acquire the information from the trade secret-owner, that information would not be considered as a trade secret.

1.5 Reasonable Measures

It is required for a trade secret-owner to show that reasonable measures have been taken to protect the secrecy of the information. The reasonable measures include that the trade secret-owner intends to protect the information, and actively maintains its confidentiality, such that other people could know that the information currently is and should be kept a secret. According to the courts, examples of reasonable measures are "marking on the document" remarks such as "Confidential" or "Restricted Access," locking the information of trade secrets or setting a password.

1.6 Disclosure to Employees

Disclosure of a trade secret to employees under neither confidentiality clauses in the employment agreement nor internal governing rules may not meet the secrecy requirement. Disclosure of confidential information to employees should be based on the standard of "who needs to know." If an employee can acquire the confidential information from the employer without restriction, the court may consider that the owner did not take reasonable measures to maintain the secrecy.

1.7 Independent Discovery

According to the legislative grounds of Article 10 of the TSA, if a third party knows the confidential information in an object through independent discovery or reverse engineering, such behaviours would be considered lawful methods under the TSA.

1.8 Computer Software and Technology

There is no specific law particularly governing the protection of trade secrets of computer software and technology. Computer software and technology are considered as trade secrets if the three statutory requirements (secrecy, economic value and reasonable measures) of a trade secret are satisfied.

1.9 Duration of Protection for Trade Secrets

The term of protection for a trade secret is not limited as long as the secrecy is kept. Accidental disclosure may be considered as not taking reasonable measures. When disclosure of trade secrets to employees, agents or subcontractors is inevitable in the operation of business, the controlled disclosure of trade secrets under the confidentiality clauses in a contract or non-disclosure agreement (NDA) is crucial to maintain the secrecy.

1.10 Licensing

A trade secret-owner is entitled to grant a licence to a third party for use of the trade secret (Article 7 of the TSA). Licensing a trade secret to a third party does not affect the existence of the trade secret as long as the secrecy is maintained. Thus, confidentiality clauses in licensing agreements or NDAs are crucial for licensing.

1.11 What Differentiates Trade Secrets from Other IP Rights

In Taiwan, trade secret protection differs from other IP rights in terms of the following aspects.

- Term of protection – the duration of protection for trade secrets is not limited if the secrecy is kept. Other IP rights, including patents, economic copyrights, integrated circuit layouts and plant varieties, are only in force for a specific length of time;
- Registration – except for trade secrets and copyrights, registration is required to acquire a patent, trade mark, integrated circuit layout or plant variety. Trade-secret protection has

an immediate effect without any registration process;
- Disclosure – disclosure to the public is necessary for a patent, trade mark, integrated circuit layout or plant variety right before or upon registration, so that any third party will be able to know the relevant information. A trade secret does not imply any disclosure to the public.

1.12 Overlapping IP Rights

If a trade secret is kept confidential in an oral or written form, the oral or written expression may also be eligible for copyright protection. In local practice, copyright claims were frequently filed in a litigation substantially for trade secret disputes before the TSA was enacted in 1994.

Besides, a company may use comprehensive IP strategies to protect products or methods of high commercial value. If the information can be easily known to the public through reverse-engineering, such as the structure of an object, a patent right could meet the demands for protection. However, a better version of a patented object or an improved manufacturing process through continual development is usually subject to trade-secret protection. It is possible for a plaintiff to assert the trade-secret right in combination with other IP rights, such as copyrights or patents.

1.13 Other Legal Theories

The Civil Code provides the general obligations of employment. An employee should treat as confidential the information which he or she knows or possesses during the employment. If an employee discloses the confidential information without a justifiable reason, it is possible for the employer to bring a claim for breach of contract.

A third party who has induced an employee to breach his or her contract with the employer may be jointly liable for the damage arising therefrom under the tort provisions in the Civil Code. If the third party is an enterprise as defined in Article 2 of the Fair Trade Act (FTA), a trade-secret owner may also seek remedies or bring claims under the FTA.

1.14 Criminal Liability

The TSA provides civil remedies and criminal penalties for trade-secret misappropriation. It is allowable for a trade secret-owner to pursue both civil and criminal claims. A person should be liable to criminal penalties under the following circumstances:

- the person intends to gain benefits illegally for himself or herself or a third party, or inflicts a loss on the trade secret-owner; and
- the person's act falls into any of the following categories:
  (a) acquiring a trade secret using wrongful means, such as an act of theft, embezzlement, fraud, threat or unauthorised reproduction;
  (b) disclosure or use of the trade secret acquired by wrongful means;
  (c) committing an unauthorised reproduction, usage, or disclosure of a trade secret known or possessed;
  (d) failing to delete or destroy a trade secret at the request of the trade secret-owner; and
  (e) use of the trade secret acquired from a third party who obtained the trade secret illegally.

Offenders shall be liable on conviction to imprisonment and fines under the TSA. If an offender intends to use a trade secret illegally in Taiwan, the offender should be liable on conviction to imprisonment for a term not exceeding five years, and, if any, a fine between TWD1 million and TWD10 million. As to the illegal use of the trade secret outside Taiwan, the offender

should be liable on conviction to imprisonment of between one year and ten years, and, if any, a fine of between TWD3 million and TWD50 million.

The criminal penalties are applicable to both natural and juristic persons. In addition, the employer (a natural or juristic person) may also be imposed a fine if his or her employee, agent or staff commits a crime under the TSA, unless the employer (or the representative of the juristic person) has done his or her utmost to prevent a crime from being committed.

1.15 Extraterritoriality

If either the illegal acts or the results arising from such acts take place in Taiwan, bringing a claim in Taiwan based on misappropriation occurring in another country is possible.

2. MISAPPROPRIATION OF TRADE SECRETS

2.1 The Definition of Misappropriation

Article 10 of the TSA provides for the definition of misappropriation of a trade secret. The types of misappropriation include acquisition, use and divulging of a trade secret by unlawful means. The term "unlawful means" refers to theft, fraud, coercion, bribery, unauthorised reproduction, breach of an obligation to maintain secrecy, inducement of others to breach an obligation to maintain secrecy, or other similar acts. Parties in interest in a litigation bear the burden of proof with regard to the facts favourable to their allegations (Article 277 of the Code of Civil Procedure). If a trade secret-owner asserts unlawful acquisition of a trade secret, such as theft, it is necessary to show evidence to prove that the defendant acquired the trade secret through theft. If the trade secret-owner alleges unlawful use of the trade secret, showing that the defendant actually used the trade secret is required.

2.2 Employee Relationships

Whether misappropriation involves an employee of a trade secret-owner will not affect a trade-secret misappropriation claim. If an employee breaches his or her employment agreement due to trade-secret misappropriation, the employee shall be liable for the damage incurred as a result of that illegal act.

2.3 Joint Ventures

There is no specific legal provision directed to the obligations between joint ventures in Taiwan. A joint-venture agreement with confidentiality and compensation obligations, or a separate NDA, is essential to maintain the secrecy of a trade secret.

2.4 Industrial Espionage

In Taiwan, there is no specific act or law directed to industrial espionage. Acts of industrial espionage are subject to the criminal penalties and civil claims that the Criminal Code and the TSA provide.

3. PREVENTING TRADE SECRET MISAPPROPRIATION

3.1 Best Practices for Safeguarding Trade Secrets

In Taiwan, in 2019, the Intellectual Property Office published the "Handbook of Teaching the Practice for the Trade Secret Protection (version 2)". The Handbook is quite helpful and applicable to all industries. The Handbook suggests that a company should establish clear policies for the management of trade secrets and adopt the following strategies as the best practices for safeguarding trade secrets:

- preparation of an inventory of confidential information, and further classification and labelling of the confidential information;

- establishment of a working code for the protection of trade secrets;
- management of employment for new employees and resignation;
- information and security control management;
- computer system management;
- an alarm system for abnormal use of confidential information and audit procedures; and
- on-the-job training to strengthen the employees' attention to trade secrets.

Common examples are signing an NDA or confidentiality clause with persons who need to know a trade secret (such as employees, consultants, subcontractors), remarking "confidential" on documents, emails, any physical media, restricting access to confidential information, access control of production sites or the offices, preservation of R&D records, cyber security or fire-wall of computer and network systems, and conducting an exit interview with employees.

3.2 Exit Interviews

To the best of current knowledge, the exit process of a departing employee in Taiwan usually includes the following steps:

- checking the employee's access to the confidential information prior to resignation and inquiring into any abnormalities;
- reminding the employee of and reiterating the duty of confidentiality in the employment agreement;
- supervising the employee's return or destruction of materials containing confidential information; and
- signing a non-competition agreement under proper circumstances.

In Taiwan, it is also common to request that a departing employee submit a written assurance that the employee knows his or her confidential duty actually and fully.

It is inevitable that inquiries will be made about the employee's reasons for leaving and future employment in an exit interview. In most cases, a departing employee is reluctant to talk about his or her new position during the interview.

4. SAFEGUARDING AGAINST ALLEGATIONS OF TRADE SECRET MISAPPROPRIATION

4.1 Pre-existing Skills and Expertise

In Taiwan, the doctrine of "inevitable disclosure" was first recognised in a judgment in 2013. However, the issues as to the distinction between an employee's general knowledge/skills and protectable trade secrets are still points of argument in lawsuits. In the 2013 judgment, the court adopted a strict standard for applying the doctrine of "inevitable disclosure", because the doctrine may affect the constitutional right to work (Article 15 of the Constitution) of a former employee. If an employer intends to assert the doctrine of "inevitable disclosure" in Taiwan, powerful grounds are required to convince the court.

4.2 New Employees

Before hiring an individual, it is necessary for an employer to ascertain the following:

- whether there are non-compete or confidentiality clauses in the employment agreement between the individual and his or her former employer and, if any, what the contents of those clauses entail; and
- whether the individual has to abide by a revolving-door clause or law and, if any, the specific obligations under that clause or law.

If an enterprise is suspected of being involved in unlawful employee-poaching, the enterprise and its representative will be subject, apart from

civil claims, to the criminal penalties and claims under the Criminal Code, the FTA and the TSA. During the process of bringing an employee on board, an employer may enter into an agreement with an individual to be hired that the individual will not supply any commercial or industrial secrets of his or her former employer.

5. TRADE SECRET LITIGATION

5.1 Prerequisites to Filing a Lawsuit

There are no prerequisites before a civil lawsuit is filed in Taiwan. It is notable that, under the laws, some specific civil disputes are subject to mandatory mediation by the court before litigation. The Code of Civil Procedure (Article 403) provides that some types of disputes are generally subject to mediation by the court before an action is initiated, where "disputes arising from an employment contract between an employer and an employee"; "disputes arising from a partnership between the partners, or between the undisclosed partners and the nominal business operator" and "other disputes arising from proprietary rights where the price or value of the object in dispute is less than TWD500,000" may result from trade-secret issues. The Labour Incident Act (Article 16) further provides that all labour cases, including non-competition disputes, are generally subject to mandatory mediation by the court before initiating litigation.

5.2 Limitations Period

A right to claim damages for a trade secret will be extinguished under any of the following conditions (Article 12 of the TSA):

- a trade secret-owner fails to exercise its right within two years from the date when the trade secret-owner knew of an act of misappropriation and the identity of a party who should be liable for the damage;
- within ten years from an act of misappropriation.

5.3 Initiating a Lawsuit

A written complaint, evidence and litigation fee should be submitted to the court to initiate a lawsuit. According to Article 244 of the Code of Civil Procedure, a written complaint should specify the following matters:

- the parties and their statutory agents;
- the claim and the transaction or occurrence giving rise to that claim; and
- the demand for judgment for the reliefs to be sought.

Further, a notarised and certified power of attorney is required if a trade secret-owner is a foreigner or foreign enterprise.

5.4 Jurisdiction of the Courts

In order to enhance the quality of trials in intellectual property litigation, the specialised Intellectual Property Court (IP court) was established on 1 July, 2008. During the past 12 years, the IP court has been playing an important role in promoting the evolution of IP practices. Most IP right-owners prefer to bring their claims to the IP court. According to the Labour Incident Act, enforced from 1 January 2020, trade-secret disputes involving non-competition agreements with an employee may be tried in the district court where the employee resides, upon the request of the employee.

5.5 Initial Pleading Standards

The Code of Civil Procedure provides that a written complaint should explain the claim and the transaction or occurrence giving rise to that claim, mandating that a plaintiff must assert detailed facts that underlie his or her claim.

It is usually difficult for a trade secret-owner to supply sufficient evidence when initiating a

lawsuit. In local practice, a trade secret-owner could allege facts before he or she has concrete evidence of misappropriation. It is not necessary to have hard evidence before bringing a claim, according to local practice.

5.6 Seizure Mechanisms

In Taiwan, a trade secret-owner is allowed to file a civil motion for preservation of evidence for seizing accused products or other evidence ex parte before initiating a lawsuit (Article 369 of the Code of Civil Procedure). The judge who grants the motion will take charge and carry out the preservation of evidence procedure.

5.7 Obtaining Information and Evidence

In Taiwan, there is no discovery system to assist both parties to collect evidence during litigation. However, both the Code of Civil Procedure and the IPCAA provide several methods for an IP-owner to obtain evidence. The fact-gathering activities may take place depending on the time when a lawsuit is filed.

- Before filing the lawsuit – in local practice, a trade secret-owner may file a motion to preserve evidence such as samples, design drawings, accounting documents, or any information stored as electronic files. Whether a motion for preservation of evidence is allowable is at the judge's discretion. The judge has full power to determine how to conduct preservation of evidence proceedings. If necessary, the judge will allow an inspection on the defendant's site to preserve evidence, such as manufacturing processes. If evidence could be obtained by the trade secret-owner or through an investigation during the trial, the judge would not grant preservation of evidence.
- After filing the lawsuit – the common investigation of evidence relating to IP disputes includes the examination of a witness, a motion to produce documentary evidence and a petition of inspection. The witness referred to herein is a fact witness, not an expert witness. Once a motion to produce documentary evidence is granted, if an opposing party does not produce those documents without a justifiable reason, the court may, at its discretion, hold that the trade secret-owner's allegation based on documents ordered to be provided is true. As to an inspection, a party in interest may request the inspection of an object or manufacturing process using video recording or photography outside the court, such as on the defendant's or a third party's premises.

5.8 Maintaining Secrecy While Litigating

The Code of Civil Procedure and the IPAA provide several ways to maintain the secrecy of a trade secret at issue or any evidence involving a third party's trade secret. It is possible to conduct fact-gathering on a confidential basis. The ways to maintain secrecy include the following.

- Non-public hearing – civil hearings are usually held in public. If a party's defence or attack involves a trade secret or privacy of the party, the court will hold a closed trial and restrict third parties from accessing the hearing or dossiers.
- Protective order – a party in interest or a third party who submits confidential materials to the court may file a petition for a protective order. The persons subject to the protective order shall use the trade secret only for purposes of the litigation. It is not permissible to disclose those trade secrets to others not subject to the protective order. If in violation of the protective order, the persons subject to a protective order shall be liable to criminal penalties. In principle, the pleading, evidence materials or ancillary documents that record confidential information are handled in a manner to ensure proper concealment or confidentiality. Only the judge, clerk, or

technical examiner officer can legally access the foregoing confidential information. Other personnel in the court are not permitted to access those materials.

5.9 Defending against Allegations of Misappropriation

The following defences are common and may be taken in combination in trade secret litigations, as long as any of these defences are considered sufficient to refute a trade secret-owner/plaintiff's assertion:

- the trade secret asserted by a plaintiff is known to the public or easily acquired from the public;
- the trade secret asserted by a plaintiff can be acquired through reverse engineering;
- the trade secret-owner has not taken reasonable measures to maintain its secrecy;
- the plaintiff is not the owner of a trade secret at issue;
- the defendant does not use a trade secret asserted by a plaintiff. Examples include i) the information used by the defendant differs from the trade secret, and ii) the technology used by the defendant was invented by independent discovery; and
- use of the confidential information is within the scope of the permitted use.

5.10 Dispositive Motions

In Taiwan, there is no "Dispositive Motions" system.

Under the Code of Civil Procedure (Article 249), if a plaintiff's claim is manifestly without legal grounds, the court may, without oral argument, issue a judgment dismissing the action with prejudice.

5.11 Cost of Litigation

A trade secret-owner usually brings monetary and permanent injunction claims in trade-secret litigation. A litigation fee for the monetary claim is about 1.1% of the amount of a claim for the first instance, and about 1.65% for the second/third instance. It is not easy to calculate the claim value of a permanent injunction. The litigation fee regarding the permanent injunction is determined by the court in accordance with the nature of each case. The remaining expense of litigation may include fees for photocopies, video recording, or travel expenses of witnesses. Litigation financing is not available in Taiwan.

6. TRIAL

6.1 Bench or Jury Trial

In Taiwan, there is no jury trial system. All cases are examined and tried by professional judges.

6.2 Trial Process

All criminal cases should be tried in a competent district court for the first instance. The criminal cases could be appealed to the IP Court for the second instance. The plaintiff may choose to bring civil claims to either the IP Court or, under certain legal conditions, to a district court for the first instance. The IP Court shall handle the civil appeal process (the second instance), no matter which court the cases were filed with for the first instance. If a plaintiff first brings trade-secret civil claims to the IP Court, the IP Court will have judicial powers for the trials in the first and second instances. The Supreme Court is responsible for a civil or criminal trial in the third instance.

The judges in the first and second instances will examine both factual and legal issues of the case. Both parties may present their assertions in the pleadings and the oral hearings and request investigation of evidence during the trial of the first and second instances. The courts responsible for the trials of the first and the second instances must hold oral arguments. In the

third instance, the Supreme Court only considers legal issues and renders a final and binding judgment. No further appeal is permitted.

To speed up the examination of IP cases, the judge would set a trial plan for each case. Each party should follow the trial plan to raise their assertions, and request the investigation of evidence. If a party in interest delays presenting an attack or defence in a timely manner, the court may deny the means of attack or defence.

According to the IP court's report in 2019, the average trial pendency of trade secret litigation for the first and the second instance is around 300 days.

6.3 Use of Expert Witnesses

In Taiwan, the Code of Civil Procedure provides for expert testimony as an evidence-taking method. An expert witness shall be appointed by the court or agreed by both parties, according to Article 362 of the Code of Civil Procedure. The expert witness is responsible to the court instead of either of the parties in interest.

There were debates on whether the expert witness testimony for either of the parties in interest should be introduced into civil litigation in Taiwan. In local practice, a written testimony for either of the parties in interest is allowable to be submitted at trial. However, the court may not consider such an expert testimony at trial because neither the Code of Civil Procedure nor the IPCAA provides a legal basis for an expert witness as support for either of the parties in interest. Therefore, the services of expert witnesses have been engaged in very few IP cases in Taiwan. Besides, there is no specific process or rules for the parties in interest to prepare or use expert testimony. Whether an oral presentation at trial of an expert witness is allowable is at the judge's discretion. The cost of an expert witness testimony varies a great deal, depending on the agreements between the party in interest and the expert witness.

It has recently come to light that an expert witness testimony for either of the parties in interest has just been introduced into the Commercial Case Adjudication Act, to be effective from 1 July 2021, albeit seemingly regardless of trade-secret disputes.

7. REMEDIES

7.1 Preliminary Injunctive Relief

In Taiwan, preliminary injunctive relief is available according to Article 22 of the IPCAA. Whether the preliminary injunctive relief is allowable will be based on the following factors:

- the existence of the legal relation in dispute;
- the likelihood of success of the applicant in the principal case in the future;
- whether the granting or rejection of the application will cause irreparable harm to the claimant or opposing party; and
- evaluation of the balance on the degree of damage to both parties and the impact on public interest.

Generally, the effect of preliminary injunctive relief can last until a final and binding judgment, and the claimant shall pay a monetary bond for the preliminary injunction. The amount of the bond depends on various factors of the case, and is determined at the judge's discretion.

7.2 Measures of Damages

In Taiwan, calculating damages for a trade-secret infringement is difficult, since the loss of the trade secret-owner is not easy to prove. Thus, Article 13 of the TSA provides several methods for calculating damages:

- the injury actually suffered;

- the lost interests;
- the amount of profits normally expected from the use of the trade secret minus the amount of profits earned after the misappropriation;
- to request the profits earned through the act of misappropriation from the person who misappropriated. If the defendant is unable to prove the costs or the necessary expense, the total income gained from the act of misappropriation shall be deemed as the profits.

Among the foregoing, calculation of the total income gained from the act of misappropriation can notably reduce the burden of proof of a plaintiff as long as the plaintiff acquires the information relating to the sale amount and prices of the infringing products. If a party has proven the damage but not the exact amount, the court shall, taking into consideration all circumstances, determine the amount by its conviction according to Article 222 of Code of Civil Procedure.

If an act of misappropriation is found to be intentional, the court may, at the request of the trade secret-owner, award damages greater than the actual damage. The amount shall not exceed three times the amount of the proven damage.

7.3 Permanent Injunction

According to Article 11 of the TSA, it is allowable to claim the following in the litigation:

- a permanent injunction;
- the destruction or necessary disposition of the accused products; and/or
- the destruction or necessary disposition of the items used exclusively in the misappropriation.

A necessary disposition includes the recall of the accused products by the respondent itself or through enforcement by the court. Due to the right to work under the Constitution, the court will adopt a strict standard to determine whether an injunction is issued to an employee unless a non-compete clause of the employment exists. The statutory limitation period to institute a permanent injunction is 15 years, based on Article 125 of the Civil Code.

7.4 Attorneys' Fees

In Taiwan, whether a party in interest appoints an attorney as advocate in the first or second instances is arbitrary. Thus, attorney fees shall be borne respectively by the party who instructs for legal services. Since it is necessary to appoint an attorney as the advocate in the third instance, the court of the third instance shall determine in the judgment an award of the attorney's fee. Based on the current practice, the award is relatively low. If a plaintiff would like to seek an award of attorney's fee, the plaintiff may claim it in the pleadings. Whether the claim for the attorney's fee is permitted is at the judge's discretion.

7.5 Costs

The losing party will bear the litigation fee incurred during the litigation. The possible recovery of court costs will include:

- the litigation fees for filing the lawsuit and appeals; and
- fees for photocopies, video recording, transcripts, translation of litigation documents, daily fees, travel expenses of witnesses and experts, and other necessary fees and disbursements.

After the judgment becomes enforceable, the court of the first instance shall, upon a motion, fix the amount by a ruling (Article 91 of the Code of Civil Procedure). It is possible for the respondent to recover the litigation fee paid during the litigation.

8. APPEAL

8.1 Appellate Procedure

If the losing party is dissatisfied with the outcome of the first instance, the losing party must file an appeal with the original court of the first instance within 20 days after receiving the judgment. Also, the litigation fee for appeal should be paid. If the losing party is not satisfied with the outcome of the second instance, the losing party must file an appeal with the original court of the second instance within 20 days after receiving the judgment of the second instance. In addition, the litigation fee for the third instance and a power of attorney must be submitted. Then, the court of the second instance will transfer the appeal case to the Supreme Court. The appeal process does not differ, no matter which court the case was filed with.

Furthermore, where one of the grounds of attack or defence is presented separately for decision, the court may enter an interlocutory judgment (Article 383 of the Code of Civil Procedure). Filing an appeal for the interlocutory judgment is not permissible. In trade-secret litigation, the judge may render an interlocutory judgment regarding the infringement issues, and then examine the damage issue. If the defendant is dissatisfied with the interlocutory judgment, the defendant cannot file an appeal at this stage and must wait until the final judgment is rendered.

8.2 Factual or Legal Review

In Taiwan, the court of the second instance will consider both factual and legal issues. Therefore, the court of the second instance will review the case de novo. The parties in interest may present a new attack/defence or request investigation of evidence in the second instance to support their assertions further. If the new attack/defence or the investigation of evidence will delay the close of the oral argument, the judge may reject them. An appellant may choose which issue is waived or preserved prior to filing an appeal, and will be precluded to claim again a waived issue if the waived issue has been recorded on the record of hearing. Further, the court of the third instance (the Supreme Court) only considers legal issues. In general, the Supreme Court examines the appeal on paper. If necessary, the Supreme Court will hold an oral hearing.

9. CRIMINAL OFFENCES

9.1 Prosecution Process, Penalties and Defences

It is necessary to institute a criminal investigation upon filing a complaint unless the crime is related to the use of a trade secret outside Taiwan. The criminal penalties are different, depending on the territory where the trade secret is unlawfully used. After the criminal investigation is instituted, the public prosecutor will request the trade secret-owner to fill in a "case explanation form" to illustrate briefly the following information:

- the contents, ownership, features and estimated value of the trade secrets;
- measures and methods that have been adopted to protect the trade secret; and
- information on the offender and infringement approach.

The case explanation form can assist the public prosecutor in understanding the case in order to initiate a seizure action and conduct the investigation of trade-secret misappropriation. If needed, the trade secret-owner, including its employees, shall elaborate the information given in the case explanation form, with the public prosecutor in attendance. In principle, the defences against misappropriation of trade secrets are the same as those in a civil case.

10. ALTERNATIVE DISPUTE RESOLUTION

10.1 Dispute Resolution Mechanisms

Mediation and arbitration are common alternative dispute resolutions (ADR) for civil disputes. In Taiwan, there is no specific law relating to the resolution of IP disputes through an ADR mechanism.

Mediation in the court can save many of the costs. In Taiwan, the court will question parties in interest about their intentions to conduct mediation after the plaintiff files a suit. If a case is not complicated, both parties may reach a settlement through mediation.

If a case is complicated, the trade secret-owner usually prefers filing a criminal complaint and subsequently institute a civil action. The reasons to institute a criminal litigation may include acquiring favourable evidence, imposing pressure on an infringer, and maintaining secrecy of confidential information. In order to avoid a criminal penalty on conviction, it is common for a defendant to reach a settlement with a trade secret-owner before the oral argument of the criminal trial in the first instance is closed.

To the best available understanding, it is not common to resolve a trade-secret dispute through arbitration.

Tai E International Patent & Law Office has matured into a major international IP law firm in Taiwan over the past 60-plus years. Today, Tai E provides a high level of quality legal service to its clients from every corner of the world. With their support and trust, Tai E takes great pride in being referred to as one of the pioneering IP law firms in Taiwan. Tai E employs more than 280 professionals, including attorneys at law, patent attorneys, trade mark agents, technical specialists and legal consultants, in four Taiwan offices. With every effort made on both international and domestic IP prosecution and protection, Tai E is familiar with scenarios of the IP markets, from global giants to individual inventors as well as particular changes of local IP practice and trends of current international IP harmonisation, based upon its accumulated abundant professional experience in different IP jurisdictions.

AUTHORS

Fred C.T. Yen graduated with BSc, MSc and LLB degrees and has been engaged in intellectual property practice for nearly 30 years. Fred is a managing partner of TAI E International Patent and Law Office. He advises clients on intellectual property matters, including patent, trade secret, trade mark, copyright, anti-competition, pharmaceutical and biologics regulatory affairs, and plant variety right. Fred has been a practising patent attorney, primarily in the fields of pharmaceuticals and life science, as well as an arbitrator, mediator and trade mark agent, for many years.

Amy N.Y. Ho received her MSc (chemical engineering) and LLB degrees from the National Taiwan University. She is an attorney admitted to the Taiwan Bar and a certified patent attorney. In addition, she passed the 2013 Patent Bar of China and is also a mediator of the Chinese Arbitration Association, Taipei. Due to her technical background and legal expertise, Amy excels at explaining complex technical issues in a concise way before the Intellectual Property Court and has successfully helped clients to protect their IP rights in defence against improper allegations.

Tai E International Patent & Law Office

9Fl, No 112, Sec 2
Chang-An E. Rd.
Taipei 10491
Taiwan
R.O.C.

Tel: +886 2 2506 1023
Fax: +886 2 2506 8147
Email: ipdept@taie.com.tw
Web: www.taie.com.tw

台一國際智慧財產事務所
台一國際法律事務所
Tai E International Patent & Law Office

Trends and Developments

Contributed by:
Yulan Kuo, Jane Wang and Brian Hsieh
Formosa Transnational Attorneys At Law see p.225

Taiwan's Trade Secrets Act (the Act) has been the basis upon which the owners of trade secrets have relied for protection of their confidential information or other technologies that those owners seek to keep confidential from their competitors. Owners can seek legal protection from the Act as long as they can establish that their secrets meet the three requirements as set forth by the Act:

- secrecy – the secret is not generally known to persons in the same field;
- commercial value – the owner of the secrets enjoys a certain level of commercial benefit because the secret is not known by the public;
- reasonable protective measures – the owner has taken reasonable measures to ensure the secrecy.

When the Act was enacted in 1996, it only provided owners of secrets with civil remedies (monetary compensation and or injunctive relief) for any misappropriation of their secrets. At that time, owners of secrets had to rely on Taiwan's Criminal Code if they wanted to pursue criminal liabilities for those who stole their secrets.

In 2013, the Act was amended to impose criminal liabilities upon those who misappropriated trade secrets. In particular, the 2013 Amendment provides increased penalties for those who misappropriate trade secrets with the intention of using those secrets in a foreign country (including China). Moreover, under the 2013 Amendment, employers may face criminal liabilities if their employees misappropriate trade secrets during the course of the employees' performance of their duties to the employers; the employers may be exempt from the same criminal liabilities only if the employers can establish that the employers have taken all possible measures to prevent their employees from misappropriating others' trade secrets.

In 2020, the Act was further amended to enable prosecutors to issue protective orders for any materials that are subject to their investigations on a potential offence of the Act. The 2020 Amendment also explicitly acknowledged that a foreign secrets-owner shall enjoy legal protection from the Act in just the same way as a Taiwanese individual or entity; foreign companies may file criminal complaints with Taiwan's enforcement authorities once they discover that their trade secrets have been misappropriated in Taiwan.

A Trend: More Owners of Trade Secrets Are Willing to Take Action to Enforce Their Trade Secrets' Rights

Many high-profile cases, both civil and criminal, have been reported since the Act's 2013 Amendment. Prior to the 2013 Amendment, it was difficult for secrets' owners to enforce their rights to their trade secrets upon finding misappropriation. Rather, companies often utilised patents, trade marks, or copyrights to protect their intellectual properties; they would consider enforcing their rights to their trade secrets only if no alternatives were available to them. The 2013 Amendment substantially changed the situation. A trend of increasingly more trade secrets' owners being willing to enforce their rights in and to their trade secrets has been observed in Taiwan after the 2013 Amendment.

According to the statistics published in 2020 by the Taiwan Intellectual Property Court (IP Court), a judicial body hearing exclusively IP-related matters, the IP Court received four and three civil complaints filed by trade secrets' owners claiming misappropriation of trade secrets in 2011 and 2012, respectively. The number of new trade secrets complaints being filed with the IP Court in 2013 and 2014 then increased to seven. The number of new cases reached 11 in 2015 and 13 in 2016. These statistics do not include civil cases in relation to trade secrets being heard by other courts. This data also does not include the number of criminal cases. The increase of the IP Court's docket for these trade secrets cases illustrates that owners of intellectual property in various industries now have a greater recognition that trade secrets' rights are enforceable and afforded legal protection.

The Landmark Case

It is believed that several landmark cases where trade secrets' owners successfully obtained protections from courts made considerable contributions to this trend. One cannot disregard the Largan case, in particular, when discussing the development of trade secrets law in Taiwan. In December 2017, the IP Court awarded enhanced damages of approximately USD50.7 million to Largan Precision Co Ltd. (Largan) in a trade secrets' misappropriation case, in which Largan alleged that four of its former employees, as well as their next employer (the defendants, collectively), jointly misappropriated Largan's trade secrets in relation to Largan's confidential technologies for optical lenses. In February 2021, the appellate division of the IP Court sustained the IP Court's 2017 enhanced damages award, dismissing the defendant's appeals requesting that the aforementioned award be set aside.

The Largan case is a landmark case in Taiwan trade secrets law for many reasons. First, the amount of the enhanced damages award is the highest damages award granted by the IP Court. According to the IP Court's 2017 ruling, the granted amount was three times the established amount of damages; the IP Court granted that enhanced damages award of three times the established damages amount because the IP Court found that the defendants infringed Largan's trade secrets wilfully. This judgment sent the signal that the Act's enhanced damages provision, under which a court may award a secrets' owner enhanced damages up to three times the actual amount of damages suffered by the secrets' owner, will be applied when the court finds wilful infringement.

In addition, when determining the amount of actual damages, the IP Court accepted Largan's argument and took into consideration the costs and expenses that Largan had invested in developing and researching Largan's secret technologies involved in this case. This is because, as Largan argued, Largan has never considered selling or licensing its manufacturing technologies to any third parties, and it would be difficult for Largan to prove the actual value of the secret technologies by referring to any transactions. The IP Court's holding in this regard gives inventors an incentive to invest more resources on technologies that the inventors would like to keep confidential from any other competitors.

Moreover, it is noteworthy that in order to prove the actual costs and expenses that Largan invested in researching and developing the secret technologies, Largan produced an expert report by a forensic accountant. The IP Court looked into the report, as well as the testimonies given by experts (both from forensic accountants) appointed by the two parties. The IP Court based its opinion in this regard substantially on the testimonies of both expert witnesses. The Largan case is thus a good example of expert witnesses assisting the court (or a fact-finder) to understand better the issues with which the

court may otherwise be unfamiliar, due to the lack of expertise in a particular field.

Proper Management of/Restrictions on Talent Flow

Most trade secrets cases share a similar scenario: the flow of talent — where a former employer has accused its former employee (sometimes, along with the employee's current employer) of misappropriating the former employer's trade secrets. As previously noted, the Act imposes upon an employer criminal liabilities when its employee misappropriates someone else's trade secrets in the course of that employee's performance of his or her duties to the employer. In some court cases, criminal sanctions were imposed upon companies whose employees misappropriated their former employers' trade secrets because the companies failed to take proper management measures to prevent their employees from using confidential materials obtained by their employees from their employees' former employers.

This has caused the relevant industries to explore further how to manage the flow of talent better. In particular, when a company is considering hiring an excellent candidate, the company must consider whether it needs reject this candidate because the candidate recently completed his or her work at a competitor firm. Moreover, when hiring someone who has just left a job with a competitor, companies would have to determine whether it is sufficient to clear the trade secrets concern by merely asking the employee to sign a document representing that he or she will not use any confidential materials obtained from his or her former employers. If the answer to this question is no, the company still needs to oversee every movement that this employee takes when he or she performs his or her job duties for the company. A company's close scrutiny of an employee's everyday life will absolutely trigger a debate on whether an employee should still enjoy a certain level of reasonable expectation for privacy in his or her working environment. Companies thus are wondering whether there is any precise standard that they should follow in order to avoid unnecessary disputes. Also considered for evaluation is the issue of whether there exists a safe labour provision, similar to the notice-and-take-down clause in copyright law, which could properly address this concern.

The aforementioned issues discussed remain, however, unsettled, and will be the subject of future developments in case law in this regard. Companies doing business in Taiwan, nonetheless, should pay great attention to their internal policies in relation to the recruitment of employees and to information security.

Future Direction of Amendments of the Act

Opinions have been stated that Taiwan should amend the Act further, along with other statutes, to prevent core/sensitive technologies from being leaked to competitors in foreign countries. In particular, these opinions have been voiced due to the concern that certain technologies are key to Taiwan's continuing economic development and that society as a whole will be in imminent peril if those technologies become known to competitors in foreign countries (and or by hostile political powers).

Counter-arguments have been made, at the same time, that the current content of the Act is sufficient to address this concern and that national security should not be a concern addressed by the Act. The debate is still ongoing, and close attention to future developments is prudent.

Formosa Transnational Attorneys At Law is one of the largest law firms in Taiwan. Formosa Transnational plays a leading role in Taiwan's IP community. The firm's technology and law department consists of experienced litigators, transactional attorneys, and patent engineers, knowledgeable in various areas of law and technology and who have multilingual capabilities and multi-jurisdictional experiences. Specifically, the firm has Japanese-speaking attorneys and engineers and is capable of handling cases in either Japanese or English, or both. Since the establishment of Taiwan's specialised Intellectual Property Court in 2008, the team has been widely recognised as one of the most successful in patent litigation. The firm has a group of experienced trial lawyers and patent engineers working closely together in patent-related cases, which is the key to the successes of its patent clients. In addition to the IP dispute resolution practice, the firm handles a large volume of patent and trade mark matters, including filing and prosecution and all other aspects of trade mark and patent usage and protection.

AUTHORS

Yulan Kuo is a senior partner at Formosa Transnational. His practice focuses on patent litigation, intellectual property, biotechnology, and IT technology. Mr Kuo has been practising for 30 years. His team includes engineers holding PhD and Master's degrees. Mr Kuo served as counsel to the Judicial Yuan, the highest judicial branch of the Taiwan government, in the establishment of the IP Court. Mr Kuo is active in patent practice and has been highly recommended as a leading lawyer by the IP community. Mr Kuo is a member of the AIPPI, the APAA, the AIPLA, the INTA, and the ACS.

Jane Wang is a partner at Formosa Transnational. Her practice includes patent litigation, IP, data protection, licensing, antitrust, and emerging technologies. Ms Wang has extensive experience in cross-jurisdictional projects. She serves multinational conglomerates based in the US, Canada, the EU, the UK, Singapore, Korea, Japan, Hong Kong, China, Taiwan, and other countries. Ms Wang co-chaired the IP/IT practice group of a top-tier global law firm network with lawyers from 89 jurisdictions. In Taiwan, Ms Wang co-chaired the Intellectual Property and Innovative Technology Committee of the Taipei Bar Association. She is a member of the APAA, the INTA, the AIPPI, and LESI.

Brian Hsieh is a partner at Formosa Transnational. His practice includes IP, administrative law, data protection, competition, and media and entertainment law. Dr Hsieh is an experienced litigator. He has counselled on and handled a wide range of regulatory matters for many global companies in the industries of technologies, e-commerce, online platforms, etc. Dr Hsieh is an active member of the Taiwan Criminal Defence Attorneys Association, which is dedicated to reforming Taiwan's criminal procedure system and to training and developing the advocacy skills of younger lawyers. He is currently chair of the Taipei Bar Association's Academic Exchange Committee.

Formosa Transnational Attorneys At Law

13F, Lotus Building
136 Jen Ai Road Section 3
Taipei 106
Taiwan

Tel: 886 2 2755 7366
Fax: 886 2 2708 435
Email: yulan.kuo@taiwanlaw.com
Web: www.taiwanlaw.com

TURKEY

Law and Practice

Contributed by:
Orcun Cetinkaya, Bentley Yaffe and Yagmur Kaya
Cetinkaya see p.245

CONTENTS

1. LEGAL FRAMEWORK

1.1 Sources of Legal Protection for Trade Secrets

Under Turkish Law, there are no laws or regulations that specifically aim to govern trade secrets and their protection. That being said, some provisions in both civil and criminal statutes safeguard trade secrets.

According to prevailing opinion in Turkish legal literature, trade secrets are subject to constitutional protection primarily under Article 17/1 of the Constitution of the Turkish Republic, which states that "Everybody has a right to live and the right to protect and improve his/her corporeal and spiritual existences." Trade secrets are considered a part of corporeal existence.

The most specific and detailed regulations that protect trade secrets are the unfair competition provisions of Turkish Commercial Code No 6102 (TCC), Article 55 of which explicitly stipulates that "disclosing manufacturing and business secrets that belong to others unlawfully" constitutes unfair competition. Under Turkish Law, manufacturing and business secrets fall within the scope of trade secrets. The other unfair competition conduct related to trade secret protection is "utilising others' works without authorisation". Individuals or legal entities whose trade secrets are disclosed or whose work is utilised without authorisation may resort to legal remedies (both civil and criminal) stipulated in the TCC with regards to unfair competition.

Article 527 of the TCC also regulates the confidentiality requirement for those individuals or legal entities who review the corporate documents and books of joint stock companies in respect of their duties (such as attorneys, the officials of the notary public, experts and employees of intermediary firms). Such persons are obliged not to disclose business secrets they have obtained from corporate documents books, or companies can claim compensation for their material and immaterial damages.

Article 396 of the Turkish Code of Obligations No 6098 (TCO) sets out a specific provision under its section on employment contracts, which aims to protect employers' trade secrets that are disclosed to employees in the course of their work.

Under the Turkish Competition Regime, undertakings can request confidentiality with regards to their trade secrets while submitting any information or document to the Turkish Competition Authority. If the Turkish Competition Authority accepts these confidentiality requests, it will not disclose such information to the public.

Article 239 of the Turkish Criminal Code No 5237 (the Criminal Code) also regulates criminal liability regarding the misappropriation of trade secrets.

Finally, Turkey is a party to the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), Article 39 of which stipulates the protection of trade secrets.

1.2 What Is Protectable as a Trade Secret

The unfair competition provisions of the TCC (Articles 55 to 63) do not provide a definition of trade secrets. Under Turkish Law, the decisions of the Turkish Court of Cassation (ie, the highest court of appeal) shed light on the meaning of trade secrets.

In its decision with the merit No 2016/6958, decision No 2019/4349 and date 21 October 2019, the Turkish Court of Cassation generally defines a trade secret as "information that (i) provides economic advantages to its individual or legal entity owner against its competitors, (ii) is kept as a secret by its owner, and (iii) reason-

able measures are taken by its owner to keep it confidential." With regards to unfair competition, the Court of Cassation defines a trade secret more specifically as "a piece of information, model, formula or layout that is utilised by its owner during his/her business activities and provides economic advantages to its owner against competitors who do not have access to such information."

In the light of this definition, any information including formulas, models, strategies, technical features of manufacturing, supply sources, research and development activities and networks will be considered as trade secrets under the Turkish Law if it fulfils the following conditions.

- The information must have secrecy – must not be known by the public and could not easily be obtained through lawful means. More specifically, the courts will assess whether the information is known by other players active in the industry and, if it is known, the degree of competitors' knowledge.
- The owner must take necessary and reasonable measures to keep the information confidential. The owner must present that he/she put effort into maintaining the secrecy of the information in an active manner.
- The information must have economic value stemming from its secrecy nature, and this economic value must not just be in the eye of its owner but also in the eyes of the owner's competitors.

Under the Turkish Competition Regime, the Communiqué on The Regulation of The Right of Access to The File and Protection of Trade Secrets No 2010/3 (the Communique) provides an explicit definition of trade secrets. Accordingly, in addition to the above-mentioned criteria, the information must be likely to result in severe damage to the undertaking when it is disclosed to third parties, especially competitors. Moreover, information or documents related to the agreements or actions that violate competition law cannot be qualified as trade secrets.

1.3 Examples of Trade Secrets

Turkish courts have qualified the following kinds of information as trade secrets under the TCC:

- manufacturing secrets;
- technical information in relation to manufacturing;
- information on drug licences;
- lists that indicate the discounts made to customers;
- lists that indicate the payment methods of customers; and
- companies' commercial books.

Under the Turkish Competition Regime, the Communique defines trade secrets as information related to corporate governance structure, the financial situation of the company, amounts of cash and loans, research and development activities, operational strategy, raw material resources, technical aspects of manufacturing, pricing policies, marketing tactics, market shares, and wholesale and retail customer networks.

1.4 Elements of Trade Secret Protection

Unfair competition conducts with regards to trade secret protection are stipulated in Article 55 of the TCC as follows:

- disclosing others' business and manufacturing secrets to third parties in an unlawful manner;
- utilising others' business and manufacturing secrets after obtaining them unlawfully;
- utilising someone's work without authorisation; and

- inducing employees, attorneys or other assistants to reveal the business and manufacturing secrets of their employers and clients (ie, offering money to employees in exchange for the trade secrets of his/her employers).

Unfair competition conducts are not limited by the major forms listed in the TCC. In principle, actions and business practices that are incompatible with commercial honesty constitute unfair competition.

In this respect, acquiring trade secrets without consent, even if they are not utilised or disclosed, should also be considered unfair competition conduct. Article 39 of TRIPS requires the member states to take necessary steps to prevent the unauthorised acquisition of trade secrets contrary to honest commercial practices. In order to comply with the provisions of TRIPS, the unfair competition provisions must be interpreted in this manner.

In such cases, individuals or legal entity trade owners can apply particular legal remedies, including compensation claims, requesting the determination of the unfairness of the conduct, and requesting prevention of the unfair competition.

The only condition to apply for these legal remedies is that their clients, professional reputation, commercial activities or other economic interests must be damaged due to these conducts of unfair competition.

Under the Turkish Competition Regime, to benefit from the trade secret protection before the Turkish Competition Authority while submitting any corporate information or document, the information or document must not be the only evidence of the particular competition law violation. Otherwise, the Turkish Competition Board can disclose such information or document in accordance with the principle of proportionality by striking a balance between public interest and the owner's interest.

1.5 Reasonable Measures

The unfair competition provisions of the TCC do not require the trade secret owner to take reasonable measures to maintain the secrecy of the information. That said, the Turkish Court of Cassation considers whether the owner has taken reasonable measures to keep the information confidential in order to qualify such information as a trade secret.

In its decision with the case No 2016/6958, decision No 2019/4349 as mentioned in **1.2 What Is Protectable as a Trade Secret**, the Turkish Court of Cassation does not explicitly address which measures are reasonable. The assessment thereof will be made on a case-by-case basis in light of the commercial customs in accordance with Article 1(2) of the TCC, which refers to commercial customs for the matters not explicitly regulated in the provisions. Although the reasonable measures will differ according to sector, in general, the following measures should be taken:

- marking the document as confidential;
- distinguishing the trade secrets from another kind of information and limiting access to documents that contain trade secrets;
- disclosing the trade secrets only to employees who need such information to fulfil their duty; and
- while disclosing the information in a contractual relationship, setting out a non-disclosure clause in the contract, or signing a separate non-disclosure agreement.

By way of illustration, in its decision No 2014/445 and dated 24 February 2020, Bakirkoy 1st Commercial Court of First Instance did not qualify a customer portfolio as a trade secret since

this customer portfolio had been open to many employees regardless of whether or not they needed it for their duties.

1.6 Disclosure to Employees

Employers can disclose their trade secrets to employees for the purposes of work. To the extent the trade secrets are disclosed to the employee in the course of their work, such disclosure will not impede the protection of these trade secrets. Under Article 396 of the TCO, employees are obliged not to disclose or utilise for their interests the employers' business and manufacturing secrets.

Although the TCO obligates employees to keep employers' manufacturing and business secrets confidential, in practice many employers prefer to set forth a non-disclosure clause in employment contracts or to sign a separate non-disclosure agreement. Stipulating a penalty clause for non-compliance provides a more intense safeguard to mitigate the risk of disclosure by employees.

1.7 Independent Discovery

Independent discovery will impede the trade secret protection of the information since it invalidates the condition of not being known by the public. In a similar manner, reverse engineering (ie, analysing the design and technical aspects of the product in order to identify manufacturing and operational secrets) invalidates the secrecy nature of the trade secret. If the technical aspects of a product that constitutes a trade secret are discovered through reverse engineering, these technical aspects will no longer be subject to trade secret protection.

Under the unfair competition provision of the TCC, obtaining trade secrets by reverse engineering does not constitute an unlawful means of obtaining, and reverse engineering does not result in unfair competition. Generally speaking, the ground of the unfair competition concept stands upon the good faith principle. Purchasing a product and then obtaining its secrets with reverse engineering does not violate this principle. However, the courts could diverge from these general principles, depending on the circumstances of each case.

1.8 Computer Software and Technology

Under Turkish Law, there are no regulations in relation to trade secret protection that are unique and separately applicable to computer software and/or technology.

1.9 Duration of Protection for Trade Secrets

Trade secrets are subject to protection as long as they maintain their secrecy and fulfil the conditions for qualifying as a trade secret (see **1.2 What Is Protectable as a Trade Secret**). Disclosing trade secrets to third parties either in a contractual relationship under a non-disclosure clause or in the context of a contract based on a fiduciary relationship will not adversely affect the secrecy nature of the trade secrets and hence the protection.

However, if the owner discloses the trade secrets to third parties without mentioning their secrecy nature and requesting confidentiality, such disclosure will impair the trade secret protection. Publishing the information to the public also removes trade secret protection.

Therefore, trade secret owners must mention the nature of the information (ie, that it is a trade secret) and, if possible, must conclude non-disclosure agreements in writing before giving access to third parties for trade secrets.

The effect of accidental disclosure will differ upon the circumstances of the event. In contrast with intentional disclosure, in the case of accidental disclosure, the owner's intention to keep

the information confidential remains. Therefore, such disclosures will not directly lead to the dissolution of the trade secret qualification. In such cases, the conclusion will depend on whether the information has lost its secrecy (see **1.2 What Is Protectable as a Trade Secret**).

1.10 Licensing

Under Turkish law, rights with respect to licensing will depend on the nature of the trade secret and whether such trade secret is also protected separately under a patent or utility model. In addition to licence agreements relating to such patents and utility models, general licence agreements can also be concluded with regard to copyrights that are based on the rights-holders' right to authorise adaptation, reproduction, distribution, representation and the broadcast of such information. In order to permit the use of trade secrets, parties can draw up a licensing agreement or a know-how transfer agreement. It is advisable for this contract to contain a confidentiality/non-disclosure clause with a penalty clause that obliges the counterparty to pay a fixed penalty fee in the case of breach of non-disclosure. Such a penalty clause serves to mitigate the risk of a disclosure by the counterparty.

1.11 What Differentiates Trade Secrets from Other IP Rights

The main difference between trade secrets and intellectual property such as patents, trade marks and copyright is the scope of the protection. Intellectual property rights can be claimed against any person who infringes them, regardless of the fault or negligence of the infringer.

Furthermore, intellectual property owners have exclusivity (the period and scope of which will depend on the type of intellectual property right) over the intellectual property, meaning that right owners can assert claims against any persons who copy or in any other way infringe upon the intellectual property. However, the trade secret owners cannot assert any and all claims against persons who developed the trade secrets by themselves without any use of or reference to the trade secrets.

Another point of difference is that the protection of trade secrets is closely related to the efforts utilised to keep such information confidential. However, intellectual property rights are protected regardless of confidentiality – with intellectual property rights such as patents and trade marks becoming protected upon registration and works subject to copyright being protected upon creation.

1.12 Overlapping IP Rights

It is possible to assert trade secret rights in combination with other types of intellectual property rights. The most common example is trade secret claims to be asserted along with patent claims or copyright claims.

However, other registered intellectual property rights such as trade marks are less likely to be asserted alongside trade secret claims since these rights require public registration and disclosure, while the main aspect of a trade secret is confidentiality.

1.13 Other Legal Theories

Article 55 of the TCC regulates the conduct of "tortious interference with contract by inducing employees, attorneys, or other assistants to obtain or disclose manufacturing and trade secrets of their employers and clients" as unfair competition. If the employers or clients have suffered due to such conduct, they can bring claims for tortious interference with the contract under the unfair competition provisions of the TCC.

1.14 Criminal Liability

Under Turkish Law, two different provisions set forth criminal liability in the misappropriation of

trade secrets: Article 62 of the TCC and Article 239 of the Criminal Code.

Article 62 of the TCC regulates criminal liability for unfair competition conduct. Under this provision, imprisonment or a judicial fine of up to two years will be imposed on individuals or the representatives of legal entities who:

- intentionally disclose the business and manufacturing secrets of others in an unlawful manner;
- intentionally utilise the other's works without authorisation; or
- induce employees, attorneys or other workers to reveal their employers' and clients' manufacturing or trade secrets.

In respect of this crime, the complainants could only be:

- individuals or legal entities whose customers, credits, professional reputations, commercial activities or other economic interests have suffered or are at risk due to the unfair competition conduct;
- customers whose economic interests have suffered or are at risk;
- chambers of commerce and industry, chambers of artisans, stock exchanges, and other professional and economic associations that aim to protect their members' economic interests pursuant to their statutes; or
- non-governmental organisations that protect customers' economic interests pursuant to their statutes.

However, if these conducts constitute another crime under laws that require more severe penalties, the punishment under this provision will not be imposed.

Article 239 of the Criminal Code regulates criminal liability for individuals who obtain information or documents that constitute trade secrets, banking secrets and customer secrets because of their title, duty, profession or art. Accordingly, individuals who disclose such information or documents or provide them to unauthorised persons shall be punished with imprisonment of one to three years and a punitive fine of up to 5,000 years (the punitive fine for one day can range from TRY20 to TRY100).

If such information and documents are disclosed or provided to unauthorised persons by individuals who have obtained such information or documents unlawfully, these individuals will be sentenced with the same penalty.

If such information and documents are disclosed to a foreigner who is not resident in Turkey, the sentence will be increased by one third, and the complaint will not be mandatory for initiating the criminal lawsuit.

Individuals who violate their confidentiality obligation stipulated in Article 527 of the TCC and disclose the trade secrets that they obtained during their duty for reviewing the corporate books of joint stock companies will be punished pursuant to this provision (Article 562/5(7) of the TCC).

The trade secret owner can pursue both civil and criminal claims.

1.15 Extraterritoriality

In cases where the misappropriation happens in another country, the jurisdiction of the Turkish courts will be determined according to the rules that regulate the competence between first instance courts (Article 40 of the International Private and Civil Procedure Law No 5718).

Accordingly, a claim in relation to misappropriation that happens in another country can be

brought before the Turkish courts in the following instances:

- if the misappropriation claims involve a defendant who is resident in Turkey (Article 6 of Turkish Code of Civil Procedure No 6100 (TCCP));
- if the damage due to unfair competition conduct occurs or is at risk of occurring in Turkey (Article 16 of the TCCP);
- if the place where the contract will be performed is in Turkey in cases where the misappropriation is based on a contract (Article 10 of the TCCP); and
- if the workplace of the employee is in Turkey in cases where the misappropriation is based on an employment contract (Article 44 of the International Private and Civil Procedure Law No 5718).

2. MISAPPROPRIATION OF TRADE SECRETS

2.1 The Definition of Misappropriation

Under the unfair competition law provisions of the TCC, the unlawful disclosure of trade secrets to third parties constitutes unfair competition conduct. The following cases are classed as unlawful disclosure:

- disclosing information that was obtained without the permission of its owner and in secret (ie, by stealing or hacking);
- disclosing information that was obtained in the context of a contract that has confidentiality/non-disclosure obligations; and
- disclosing information as a breach of contract that is based on confidence/fiduciary duty.

In such cases, the owner must prove that:

- the piece of information qualifies as a trade secret;
- the defendant has obtained this trade secret by unlawful means; and
- the defendant has disclosed this trade secret unlawfully.

In cases where the disclosure is based on a breach of a contract, the owner must show that the disclosed trade secret was given to the defendant within the context of the contract. If the trade secrets are not exposed but utilised, the trade secret owner must prove that utilisation.

If the plaintiff asserts the claim in relation to the utilisation of work without authorisation, he/she must prove that the defendant has utilised the work and that this utilisation was without consent.

2.2 Employee Relationships

Under Turkish law, employees are obliged not to disclose their employers' business and manufacturing secrets to third parties and not to utilise these secrets for their own interests as long as the employment contract is in effect. This obligation survives after the termination of the contract if keeping the particular information confidential is mandatory to safeguard the employer's legitimate interest (Article 396 of the TCO).

Employers can assert claims under both the unfair competition provisions of the TCC and Article 396 of the TCO against employees who disclose or utilise their trade secrets. If the employer pursues claims under Article 396 of the TCO, he/she has to prove his/her legitimate interests with regards to that information. The elements of trade secret protection under the unfair competition will not differ.

2.3 Joint Ventures

Under Turkish law, joint ventures are regarded as "simple partnerships" and are subject to the provisions of simple partnership agreements

stipulated in Articles 620 to 645 of the TCO. None of these provisions explicitly regulates an obligation between partners with regards to the protection of trade secrets.

That being said, in Turkish legal literature, the prevailing opinion is that the partnership agreements are based on a fiduciary relationship, and that partners owe each other duties of fiduciary and loyalty. Accordingly, these duties could be seen in Article 626 of the TCO, which regulates the non-competition principle, while Article 628 of the TCO sets forth the partners' duty of care. According to Article 626 of the TCO, the partners shall not undertake transactions for their interests or other third parties' interests that might damage or hinder the aim of the partnership.

In this regard, it is argued that each joint venturer has to take the necessary measures to protect and not disclose the trade secrets belonging to the joint venture or other joint venturers. It is recommendable to conclude a non-disclosure agreement between joint venturers.

2.4 Industrial Espionage

As mentioned in **1.15 Extraterritoriality**, Article 239 of the Criminal Code regulates criminal liability for disclosure of trade, banking and customer secrets. Under this provision, individuals who disclose information or documents that constitute trade secrets, banking secrets or customer secrets, or who provide them to unauthorised persons, shall be punished with imprisonment of one to three years and a punitive fine of up to 5,000 years (the punitive fine for one day ranges from TRY20 to TRY100). If such information and documents are disclosed to a foreigner who is not resident in Turkey, the sentence will be increased by one third, and the complaint will not be mandatory for initiating the criminal lawsuit (see **1.14 Criminal Liability**).

3. PREVENTING TRADE SECRET MISAPPROPRIATION

3.1 Best Practices for Safeguarding Trade Secrets

In general, the best practices to maintain the protection of trade secrets are as follows:

- concluding non-disclosure agreements with third parties such as customers, distributors, sellers and sub-contractors;
- concluding non-disclosure and non-competition agreements with employers;
- organising documents in a way that separates the documents that contain trade secrets from those that do not, labelling the documents that contain trade secrets as confidential;
- classifying the information as publicly known, accessible for any employee, sensitive, and accessible with permission or strictly confidential, and instructing employees on the nature of each type of information in writing;
- limiting both psychical and electronic access to documents with trade secrets, enabling access only for employers who need that information for their work;
- after obtaining the consent of the employee, monitoring the electronic devices of the employees and supervising whether they use the electronic data lawfully;
- taking security measures for the protection of information technology systems, such as firewalls, password protection, virus scanners, etc; and
- conducting risk assessments to detect potential means of disclosure.

3.2 Exit Interviews

Employers generally remind departing employees that they have to return any documents or other materials belonging to the employer. Human resources will also inform the employee

of the non-competition clause if such a clause exists in the employment contract. During exit interviews, employees do not have to answer any questions or make any explanation with regards to their new position.

4. SAFEGUARDING AGAINST ALLEGATIONS OF TRADE SECRET MISAPPROPRIATION

4.1 Pre-existing Skills and Expertise

Although Turkish law does not differentiate the pre-existing skills and expertise of employees from trade secrets, the courts have established a distinction between the two.

It is a natural consequence that employees will acquire professional knowledge and skills while working in a company, so such knowledge and skills cannot be regarded as trade secrets.

By way of an illustration, in its decision No 2014/445 and dated 24 February 2020, the Bakirkoy 1st Commercial Court of First Instance decided that it is natural for an employee working in the marketing department to know the customers of that company and to use this information in their subsequent employment. However, the way in which this information is utilised by the employee in question may give rise to unfair competition claims, depending on the competition clauses in the employment agreement. In addition, the distinction between pre-existing skills and trade secrets would defer, depending on the sector and the employee's position.

Under Turkish law, the inevitable disclosure doctrine (under which the former employer can interfere in the subsequent employment of the employee if the disclosure of trade secrets is inevitable) is not recognised. Under no circumstances can starting to work in a competitor company result in a violation of unfair competition provisions or the confidentiality duty of the employee, which survives after the termination.

The TCO allows employers to obtain an undertaking from the employee with regards to non-competition for a period of up to two years following the termination of the contract. However, even this clause does not enable the employer to prevent subsequent employment in a competitor. If the employee begins to work with a competitor and violates the non-competition clause, the former employer can only claim compensation for his/her damages that occurred due to such violation.

4.2 New Employees

To mitigate risks arising from unintentional use of a former employer's trade secrets, an employer can obtain an undertaking from new employees to not disclosure their former employer's trade secrets. In the case of accidental disclosure, the new employee must be obliged to inform the new employer about the trade secret nature of the information. This written undertaking will show the good faith and honesty of the subsequent employer if any dispute arises.

5. TRADE SECRET LITIGATION

5.1 Prerequisites to Filing a Lawsuit

In general, Turkish law does not provide any prerequisite before initiating a lawsuit except the mandatory mediation for money claims in relation to commercial law (Article 5 of the TCC). As unfair competition is regulated in the TCC, mediation is also compulsory for money claims arising from unfair competition. Money claims arising from employment contracts are also subject to mandatory mediation (Article 3 of the Labour Courts Law No 7063). In other words, in the case of disclosure by an employee, the

relevant employer must first apply to the mediation process.

After invoking the mediation process, the plaintiff must submit the mediation minutes stating that the parties could not settle as a result of the mediation process to the court while initiating the lawsuit. If this step is not taken, the court will reject the case without examining its merits due to a lack of cause of action.

It is worth noting that trade secret cases with the nature of a declaratory action or with a request for the prevention of unfair competition without any money claims will not be subject to compulsory mediation.

Even though it is not obligatory, it is common in Turkey for the claimant to send a cease-and-desist letter in case of trade secret violation to ex-employees and/or the competitors that hired them prior to the mediation stage.

5.2 Limitations Period

The statute of limitations in trade secret claims varies according to the relationship between the parties and the type of the claim.

If the trade secret claim constitutes unfair competition under the TCC, the limitation period is one year from the day the plaintiff learns that they are entitled to file a lawsuit, and three years from the initiation of this right in any case. However, if the act of unfair competition is also an act that requires a penalty that is subject to a longer limitation period under the Criminal Code, this period is also valid for civil cases.

If there is a contract between the parties with a confidentiality clause and the actions of the defendant constitute a breach of such contract, the limitation period is ten years in principle, according to the TCO.

5.3 Initiating a Lawsuit

The plaintiff must file a lawsuit petition before the competent court to initiate a trade secret claim, as in the general practice of Turkish civil law. The plaintiff explains the subject of the dispute along with the relevant facts and evidence. The plaintiff must identify the counterparty by including relevant information of the counterparty in the lawsuit petition.

The court fees and expenses must also be deposited with the court ahead of starting the proceedings.

As explained in **5.1 Prerequisites to Filing a Lawsuit**, the claimant must apply to the mediator first if the claim involves a money claim.

5.4 Jurisdiction of the Courts

The jurisdiction of the court authorised to review a trade secret claim varies depending on the relationship between the parties and the legal status of the claim. The jurisdiction of the court is different if the claim has arisen from a breach of contract or unfair competition.

Under Turkish law, acts that constitute unfair competition are classified as tort. As no special jurisdiction is provided in the TCC for unfair competition claims, the jurisdiction rules that apply to tort claims also apply to unfair competition claims. In this regard, unfair competition claims can be initiated before the competent court in the area where:

- the defendant is residing;
- the unfair competition has been committed;
- the damage has occurred or is likely to occur; or
- the plaintiff is residing (Article 16 of the TCCP).

Trade secret claims that are based on a breach of a contract can be initiated before the compe-

tent court in in the area where the defendant is residing in the execution place of the contract (Article 10 of the TCCP).

Under Article 18 of the TCCP, parties to a contract can conclude a jurisdiction agreement or draw up a clause in relation to jurisdiction in the relevant contract. Unless otherwise provided in the contract, this jurisdiction will be exclusive, and parties must bring a claim before the courts stipulated in the particular contract.

5.5 Initial Pleading Standards

Trade secret claims are subject to the general pleading standards of the TCCP, according to Article 194 of which the claimant must substantiate its claims up to a reasonable extent for the case to be heard before a civil court. In other words, the plaintiff cannot only allege facts "on information and belief". However, the claimant may not be in possession of all evidence that will potentially support its case whilst filing the lawsuit, which is not an obstacle for the claimant to initiate its case as the claimant can ask the court to collect this evidence from either the defendant(s) or third parties.

When it comes to money claims connected to trade secret violation, claimants are expected to declare the entire amount of their damages to the extent they can at the beginning of the lawsuit, as per Article 119 of the TCCP. If the amount of this damage is to be determined according to the evidence to be collected by the court, including expert witness evidence, the claimant can be allowed to initiate the case without specifying the amount of its damages.

5.6 Seizure Mechanisms

The claimant may request civil courts to conclude preliminary injunctive relief regarding the prohibition of the supply of the accused products (ie, the products manufactured through misappropriation of the trade secrets), which might include the seizure of products until the decision of the first instance court. However, the court may seek a high threshold of evidence with regards to the rightfulness of the complaint. The court may conclude to order such injunctive relief ex parte if the protection of the claimant's rights requires the relief in an immediate manner.

In order to obtain preliminary injunctive relief, the claimant must provide a security, which is generally requested by the court as 15% of the value of the protection provided (ie, the quantum of the case or goods to be seized). However, as per Article 392 of the TCCP, the court may decide not to request a security if the request is based on the official document or any other similar strong evidence, or as the conditions require.

5.7 Obtaining Information and Evidence

With regards to civil law cases, the party preparation principle is recognised under Turkish law. Therefore, as a rule, parties are expected to submit their evidence or provide its whereabouts to the court. The same principle applies to civil cases arising from trade secret violations.

The inquisitorial system is used in criminal cases and therefore, in any criminal investigation initiated due to a trade secret violation, the prosecutors' office or the criminal court would need to search for evidence in order to hand down a decision.

Prior to filing lawsuits, however, the claimants can request determination of the evidence as per Article 400 of the TCCP in cases where there is a likelihood that the evidence in question could disappear. It is common in practice for claimants to request on-site inspections and expert reports within the context of determining the evidence to process prior to filing their substantive claims.

Additionally, the Turkish Industrial Property Law stipulates that the right owner can request the

court to order the counterparty to submit and disclose the documents regarding the infringement. This mechanism can also be used by the owner if the trade secret theft or misappropriation also constitutes unlawful use of an industrial property right.

5.8 Maintaining Secrecy While Litigating

In principle, hearings of civil, administrative and criminal proceedings are open to the public in Turkey but it is not permissible to take photos, videos or voice recordings.

To avoid a public hearing, parties can request a confidentiality order from the court, or the court may decide to hold the hearing in private ex officio if public morality, public safety or the relevant person's superior interest so requires.

When it comes to the confidentiality of the court documents, only the parties and their representatives can access the court papers and obtain copies of them.

An exception to the above is that seasoned lawyers can review all court files if there is no confidentiality order but they cannot obtain copies of the court papers without power of attorney from one of the parties in the proceedings.

5.9 Defending against Allegations of Misappropriation

The defences available in trade secret litigation vary from case to case depending on the nature of the dispute and the claims asserted. In this regard, there is no general best practice for trade secret litigation, but some points are worth noting.

Defendants generally challenge the nature of information as a trade secret or as pre-existing skills or knowledge of the employee with regards to previous employee disclosure. Defendants could also argue that the disclosure of the trade secret or use of the work was not unlawful. Also, defendants focus on the causation between the violation of trade secrets and damages occurring in money claims. In money claims, the defendants try to force the claimants to ascertain the amount of their claims to make them deposit higher application fees and use this high quantum as a basis for higher representation fee claim pro rata to the amount of the case to be denied by the court.

5.10 Dispositive Motions

Turkish law does not provide for dispositive motions before the trial.

5.11 Cost of Litigation

In Turkey, the majority of the costs and fees are collected in advance from the plaintiff while filing the case. Those include application fees, decision and judgment fees, expert and witness fees, and notification fees. There might be occasions, however, where courts order the defendants to pay the fees of expert witnesses, particularly when it is only the defendant who relies on the expert evidence, or the fees for additional expert reports if the initial reports were rejected only by the defendant(s). Another fee to consider is the pro rata decision and judgment fee for money claims, which is 6.831% of the case amount. For cases with no money claims, the decision and judgment fees are negligible fixed amounts. Other costs of litigation can also be calculated on a pro rata basis or as a fixed fee, depending on the type of the claim.

Finally, the claimants should bear the representation fee in mind, which the losing party must pay to the lawyers of the winning side and is calculated with reducing rates pro rata to the claimed amount as per an official tariff. This is separate from the professional fee determined between the lawyer and the client.

Turkish law does not allow contingency fees. The attorney fees cannot be lower than the amount stipulated under the minimum attorney fees tariff. However, lawyers are allowed to receive premiums based on their success rate.

There are no restrictions regarding litigation funding under Turkish law.

6. TRIAL

6.1 Bench or Jury Trial

Jury trials are not available under Turkish law.

6.2 Trial Process

A large percentage of trials are conducted in writing under Turkish law as a principle, including trials regarding trade secret claims. Although oral arguments are also part of the trial, the written submissions are the core element of the trial process.

The court holds hearings and summons the parties several times during the trial. Generally, interlocutory decisions are granted in these hearings, such as summoning the witnesses, requesting documents or appointing experts.

The court may hear witnesses during these hearings upon the request of the parties. During the witness statements, the parties can request the court to ask questions of the witnesses.

The timetable for trade secret claims differs according to the nature and complexity of the dispute. Because proving the arguments in a trade secret claim can be challenging without the support of expert opinions in most cases, several expert opinions may be necessary during the trial, which may cause the trial process to take longer than other kinds of lawsuits. In this regard, the first instance phase of a trade secret claim can take approximately one to two years.

6.3 Use of Expert Witnesses

Expert opinions are one of the most important pieces of evidence in civil proceedings under Turkish law. The court appoints an expert or a panel of experts to explain the technical details of a dispute in most lawsuits.

The experts can be appointed by the court ex officio or upon the request of the parties. Since trade secret claims mostly require special or technical knowledge, expert opinions are highly important in a lawsuit regarding trade secrets.

As per Turkish law, the experts can be appointed by the court or an expert opinion can be obtained by the parties from an independent expert. However, the courts give more weight to the opinions of court-appointed experts than those obtained by the parties from an independent expert.

Court-appointed experts are prohibited from giving an opinion regarding legal matters, but experts introduced by the parties are permitted to do so.

Experts submit their opinion as a written report to the court instead of attending the hearings, in principle.

7. REMEDIES

7.1 Preliminary Injunctive Relief

According to Article 389 of the TCCP, the court may order any type of preliminary injunctive relief available under the conditions, which covers changes in existing circumstances that will result in severe difficulty or impossibility to exercise the right, or if a delay would cause an inconvenience or serious damage.

A party must file a petition to court to request injunctive relief, specifying the reason and the type of the injunctive relief required. It is possible

to request injunctive relief from the court before or during the trial.

Preliminary injunction orders are a temporary legal measure and expire with the finalisation of the decision of the court given in the merits of the case, unless the court converts the order to a permanent decision in its verdict.

As a rule, the court orders injunctive relief if the requesting party provides security. This security is provided in order to cover the potential loss of the counterparty or of third parties that may occur because of an unjustified request for injunctive relief. However, as per Article 392 of the TCCP, the court may decide not to request security if the request for such is based on the official document or any other similar strong evidence, or as the conditions require. Generally, the security requested by the court is 15% of the value of the protection provided – ie, quantum of the case, goods seized or likely profit of certain duration of manufacturing if it is ceased due to the injunction.

7.2 Measures of Damages

As described in **1. Legal Framework**, there are several laws protecting trade secrets in Turkey. Actions contrary to those laws may be subject to pecuniary and non-pecuniary damage claims, as per the general rules of the TCO.

In addition, pursuant to Article 56 of the TCC, a compensation lawsuit can be filed in order to request pecuniary damages for loss caused due to the faults of the perpetrator that constitutes unfair competition.

The legal requirement for a successful claim for pecuniary damages is the existence of unfair competition, loss due to unfair competition, culpability and a causal bond.

In addition, a person whose personal rights have been unlawfully violated due to unfair competition can claim non-pecuniary damages in accordance with Article 58 of the TCO. Unlike pecuniary damages claims, non-pecuniary damages can be claimed regardless of the severity of the culpability.

Punitive damages are not available in Turkey, except for those regulated under the Turkish Competition Regime.

7.3 Permanent Injunction

There is no permanent injunctive relief mechanism in Turkey.

However, along with the pecuniary and non-pecuniary compensation awards, Turkish courts can decide on orders at the end of the proceedings that might have permanent effects on the defendants. According to Article 56 of the TCC, the claimant party may request the following from the court:

- determination of the unfairness of the act;
- the prevention of unfair competition; and
- the removal of the financial situation arising from the unfair competition, the correction of any false or misleading statements that led to the unfair competition and, if it is necessary to prevent infringement, the destruction of the means and goods that led to the unfair competition.

Among those, the prevention of unfair competition gives sufficient ground for permanent measures to limit the way in which the defendants act. Similarly, the court can order the demolition of goods that are produced as a result of the violation. These requests can be made if trade secret violations are raised within the framework of an unfair competition claim.

It is not possible to limit employees' subsequent employment in cases of the disclosure of trade secrets. In practice, claimants try to draw certain boundaries regarding the way in which the employee will share information based on his/her previous experience, but courts do not leave any room for interpretation.

Even if there is a non-competition agreement between the previous employer and the employee, the former can only request compensation for the losses and damages that have occurred, without being able to limit the employee's future employment in anyway whatsoever.

7.4 Attorneys' Fees

As per Turkish law, professional fees cannot be requested from the other/losing party. However, as mentioned in **5.11 Cost of Litigation**, the courts order official attorneys' fees to be paid by the losing party; such fees are calculated pro rata with reducing rates to the claimed amount according to an official tariff. The fees are revised every year by the circulars.

7.5 Costs

The court fees and costs are collected in advance in the civil courts, and deposited by the plaintiff before filing the case as a rule. The litigation costs include expenses such as decision and judgment charges, expert and witness fees, notification fees and documentation fees.

Since the plaintiff is required to pay the costs in advance before initiating the lawsuit, the defendant is required to reimburse the plaintiff party for the court costs and expenses if the plaintiff wins the case. The losing party is also obliged to pay the attorney fees at the end of the proceedings, as described in **7.4 Attorneys' Fees**.

The costs are calculated by the court in accordance with the Act of Fees.

8. APPEAL

8.1 Appellate Procedure

In Turkish legislation, the hierarchy of the court system is as follows:

- first instance court;
- regional courts of appeal; and
- Court of Cassation.

Both claimants and respondents can appeal the first instance court's final decision to regional courts of appeal, and the final decisions of regional courts of appeal to the Court of Cassation, under some conditions indicated in laws.

As a rule, parties can appeal only the decisions of first instance courts that exceed the amount of TRY5,880 for 2021 (this amount is amended annually) to be examined by the regional courts. Only the following decisions of courts of appeal can be appealed to the Court of Cassation:

- decisions in which the amounts do not exceed TRY78,630;
- disputes within the jurisdiction of the courts of peace, excluding disputes regarding real property rights;
- decisions of a regional court of appeal on the first instance court's decision regarding the place of jurisdiction, or the competence or authorisation of the court;
- decisions regarding ex parte proceedings;
- decisions on the correction of the Civil Registry;
- records of persons, excluding the cases that bear consequences regarding paternity; and
- decisions on temporary legal protections.

Both the final decisions of regional courts of appeal and decisions of the Court of Cassation may be appealed within two weeks of the notification being served. The appeal process is the same for all civil cases.

On the other hand, the rejection of a decision on the acceptance of a preliminary injunction request can only be appealed together with the final decision.

8.2 Factual or Legal Review

Under the first step of the Turkish Appeal Regime (ie, bringing the decision of the first instance courts to the regional courts of appeal), the regional court of appeal reviews both the factual and legal issues of the case. In other words, the regional court of appeal examines:

- whether the particular court has considered all evidence provided by the parties;
- whether the court has analysed the facts of the cases properly; and
- whether the court has applied and interpreted the law in an appropriate manner.

In this regard, the regional court of appeal may re-hear witnesses, carry out on-site inspections, and collect the evidence that was referred by the parties but not collected by the first instance court. In addition, as a rule, the regional courts of appeal hold hearings for the sake of the right of defence. However, the parties cannot assert any claims or evidence at the regional court of appeal that they did not assert in the first instance trial. At the end of the appeal review, the regional court of appeal may uphold the decision of the first instance court, and conclude a new decision.

Conversely, appealing to the Court of Cassation is a legal remedy that aims to examine the decisions of the regional courts of appeal and ascertain whether the law and legislation were applied to the case properly; the Court of Cassation is not obliged to check facts or evidence. Unlike the regional courts of appeal, in principle the Court of Cassation examines the case file without holding a hearing. That being said, in cases where the decision of the regional court exceeds TRY117,960 and one of the parties requests the hold of hearing on their appeal petition, the Court of Cassation must hold a hearing. At the end of the appeal, if the Court of Cassation upholds the decision of the regional court of appeal, the case will be returned to the first instance court or the regional courts of appeal.

Under Turkish law, it is possible to waive the right to appeal. However, since the decision of the court of first instance or the regional courts of appeal will be deemed accepted with all its consequences in the case of a waiver, the waiving party cannot reserve any terms and conditions in its waiving petition.

9. CRIMINAL OFFENCES

9.1 Prosecution Process, Penalties and Defences

As described in **1.14 Criminal Liability**, there are two different provisions under Turkish Law that regulate criminal liability in the misappropriation of trade secrets: Article 62 of the TCC and Article 239 of the TCC. Criminal prosecution can be initiated with the complaint of the complainant for both crimes.

With reference to Article 55 of the TCC and according to the provisions in Article 62 of the TCC regarding trade secrets, imprisonment or a judicial fine for up to two years can be imposed on individuals or the representatives of legal entities who:

- disclose others' business and manufacturing secrets unlawfully (ie, in secret and without permission or by other unlawful means) and intentionally; and
- entice employees, attorneys or other workers to reveal their employers' and clients' manufacturing or trade secrets.

On the other hand, Article 239 of the TCC regulates criminal liability for individuals who obtain information or documents that constitute trade secrets, banking secrets or customer secrets in the course of their title, duty, profession or art. Individuals who disclose such information or documents, or who provide them to unauthorised persons, shall be punished with imprisonment of one to three years and a punitive fine up to 5,000 years.

The process starts with the filing of a criminal complaint before a prosecutor's office. The complainant must apply to the law enforcement authorities or the chief public prosecutor's office within six months of the occurrence of the trade secret theft (Article 73 of the Criminal Code). As soon as the prosecutor finds out about a situation that gives the impression that a crime has been committed, he/she conducts an investigation to decide whether to file a public lawsuit; if the prosecutor reaches a sufficient suspicion that the crime was committed at the end of the investigation, he/she prepares an indictment and submits it to the court, and thus the criminal trial begins.

According to Article 62 of the TCC, those who deliberately commit one of the unfair competition acts outlined in Article 55 are punished. Therefore, unlike civil proceedings, the defendant cannot be punished in cases where he/she did not disclose the trade secrets on purpose. In this scope, a perpetrator may make a defence that he/she did not disclose the trade secret or did not know that the information was a trade secret, or that they disclosed it unintentionally. However, such defence cannot be made in civil proceedings, in which the defendant can only claim that he/she did not disclose trade secrets or did so lawfully. In other words, the absence of intention cannot be the defendant's defence in civil proceedings.

The complainants can request search and seizure orders from the public prosecutor or the criminal judge, and can attend the raids to be conducted for the seizure of evidence with the law enforcement officers.

10. ALTERNATIVE DISPUTE RESOLUTION

10.1 Dispute Resolution Mechanisms

Mediation and arbitration are the most commonly used ADR processes in Turkey. However, due to the nature of trade secrets violation, civil and commercial litigation as well as criminal litigation are more likely in Turkey.

Mediation is compulsory for money claims involving trade secret civil litigation. In other words, the use of mediation for trade secrets litigation is common.

When it comes to arbitration, obviously parties must agree on this process following a request raised by the claimant in the cease-and-desist letter or during the mediation process. Given the nature of such disputes, it is less likely for the defendants to consent to an ADR process that will potentially accelerate the proceedings. The defendants in these types of cases might understandably be more lenient towards litigation with two tiers of high court review.

Cetinkaya is a full-service law firm based in Istanbul that represents international institutions, national governments, multinational companies, Turkish conglomerates and high net worth individuals. Cetinkaya regularly acts in high-value and precedent-setting cases, successfully representing clients in disputes across a range of industries in Istanbul and Turkey. Alongside numerous commercial litigation cases, Cetinkaya excels in domestic and international arbitration. The firm regularly acts as counsel in trade secrets cases, advising on trade secret misappropriation, breach of privacy rights and obtaining preliminary injunctions, representing clients successfully in civil and criminal cases.

AUTHORS

Orcun Cetinkaya is a partner and head of dispute resolution at Cetinkaya, specialising in crisis management, commercial litigation, financial crime and arbitration. He represents clients in high-profile civil litigation, trade secret misappropriation and related claims, as well as regulatory breaches and allegations of fraud in Turkey. His arbitration practice often involves cases in connection with Turkish foreign investments in the region. He also represents international clients in relation to the enforcement of arbitral awards in Turkey.

Bentley Yaffe is a partner and the head of intellectual property at Cetinkaya, specialising in data protection, compliance, media and entertainment, technology and intellectual property law. He has extensive experience in advising on data protection and privacy matters, and in acting as counsel in trade secrets cases. In addition to designing and implementing data protection compliance processes, he provides project-based support for the design of privacy features. Bentley also manages clients' intellectual property portfolios, providing contentious and non-contentious support in the areas of trade mark, copyright and patent law.

Yagmur Kaya is an associate at Cetinkaya and provides legal support to local and international clients in relation to corporate and commercial law, competition law and compliance. She assists in preparing and revising various types of commercial agreements. Yagmur regularly advises clients on trade secret law and also has in-depth knowledge of international trade law, particularly the anti-discrimination principles of the WTO, customs law, subsidies and countervailing duties.

CETINKAYA

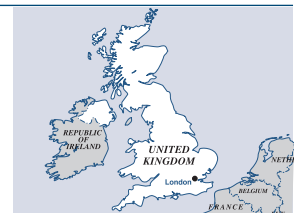
Akat Mah Cebeci Cad No 24 Besiktas
34335 Istanbul
Turkey

Tel: +90 212 351 3140
Fax: +90 212 352 3140
Email: info@cetinkaya.com
Web: www.cetinkaya.com

UK

Law and Practice

Contributed by:
Nicola Dagg, Steven Baldwin, Daniel Lim and Gabriella Bornstein
Kirkland & Ellis see p.263



CONTENTS

1. LEGAL FRAMEWORK

1.1 Sources of Legal Protection for Trade Secrets

In the UK, trade secrets are protected by:

- common law/equity that protects confidential information;
- the implementation of the EU Trade Secrets Directive ((EU) 2016/943) (the "Directive") through statute, the Trade Secrets (Enforcement, etc) Regulations 2018 (SI 2018/597) (the "Regulation"); and
- contractual measures, typically in employment contracts or non-disclosure agreements.

These sources are interlinked. For example, contractual arrangements can support or be raised in addition to claims under the Regulation or under common law/equity.

The Directive/Regulation does not displace the protection afforded by common law/equity.

The authors note that due to the UK's exit from the European Union and following the expiry of the transition period on 31 December 2020, CJEU case law continues to apply to lower courts in the UK. However, future CJEU decisions, including in relation to the Directive, will not apply. As noted above, given the Directive/Regulation did not significantly change the position under common law/equity, this is unlikely to cause significant disruption to the law.

1.2 What Is Protectable as a Trade Secret

Trade secrets protect information with a high degree of confidentiality that is of commercial value by virtue of it being secret in the sense of not being generally known to the public. There is no limit on the type of information that can be classified as a trade secret.

Under common law, the court has given examples such as "secret processes of manufacture such as chemical formulae, designs or special methods of construction" and "other information which is of a sufficiently high degree of confidentiality as to amount to a trade secret". This is contrasted with confidential information that is not a trade secret, to which there is a lower degree of obligation and that an employee is free to use and disclose once out of the employ of their employer.

Under common law, the relevant factors to be considered in determining whether information held by employees falls into the former or latter class of confidential information (or is not confidential at all) include:

- the nature of the employment;
- the nature of the information;
- whether the employer impressed the confidentiality of the information on the employee; and
- whether the information can be isolated from other information that the employee is free to use.

(See, eg, Faccenda Chicken Ltd v Fowler (1987) Ch 117.)

Under the Directive as implemented by the Regulation, a trade secret is defined as information that:

- is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among, or readily accessible to, persons within the circles that normally deal with the kind of information in question;
- has commercial value because it is secret; and

- has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

In the recent Court of Appeal decision of Shenzhen Senior Technology Material Co Ltd v Celgard, LLC [2020] EWCA Civ 1293, LJ Arnold underlined that the doctrine of misuse of confidential information is (i) all about control of information and (ii) a species of unfair competition. There is no property in information, and the Trade Secrets Directive does not create a (proprietary) species of intellectual property right.

1.3 Examples of Trade Secrets

2020 saw the first UK cases under the Directive/Regulation. Those cases related to:

- technical information regarding battery separators (see Celgard, LLC v Shenzhen Senior Technology Material Co Ltd [2020] EWHC 2072 (Ch), upheld on appeal [2020] EWCA Civ 1293), where the court considered there to be a serious issue to be tried and that the balance of convenience favoured the granting of an injunction against the defendant; and
- customer lists (see Trailfinders Limited v Travel Counsellors Limited & Ors [2020] EWHC 591 (IPEC)), where the court found the defendants to have breached their obligations of confidence owed to the claimant.

Some examples of types of information found to constitute a trade secret under common law are:

- products and methods (see Balston Ltd v Headline Filters [1990] FSR 385);
- formulations (eg, formulation of inks, see Johnson & Bloy (Holdings) Ltd v Wolstenholm Rink plc [1989] FSR 135);
- supplier or client lists (see PSM International Ltd v Whitehouse [1992] FSR 489);
- sales and distribution methods (see PSM International Ltd v Whitehouse [1992] FSR 489);
- marketing and advertising strategies (see PSM International Ltd v Whitehouse [1992] FSR 489); and
- some databases (Vestergaard Frandsen A/S and others v Bestnet Europe and others [2009] EWHC 657 (Ch) cf Roger Bullivant Ltd v Ellis [1987] ICR 464).

However, there is no limit on the type of information that can qualify for protection.

1.4 Elements of Trade Secret Protection

Under Common Law/Equity

The seminal test for an action in breach of confidence is set out in Coco v AN Clark (Engineers) Ltd [1968] FSR 215.

The following apply.

- The information must have the necessary quality of confidence. The information must therefore be sufficiently secret and valuable. It must have "the necessary quality of confidence about it, namely it must not be something which is public property or public knowledge" (Saltman Engineering Co Ltd v Campbell Engineering Co Ltd [1948] 65 RPC 203 [1948] 65 RPC 203, at 215).
- The information must have been imparted in circumstances importing an obligation of confidence. Such circumstances could arise, eg, through being imposed by contract, because of the particular circumstances in which the information was imparted, due to a special relationship between the parties (eg, doctor-patient, lawyer-client).
- Threatened or actual unauthorised use. This can include use outside the scope of authorisation; eg, where the confidential information has been disclosed for a specific purpose and it is used for an ulterior purpose.

Under the Directive/Regulation

The following questions apply.

Is the information a "trade secret"?

Under Article 2(1), "trade secret" means information that meets all of the following requirements:

- it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among, or readily accessible to, persons within the circles that normally deal with the kind of information in question;
- it has commercial value because it is secret; and
- it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

Was there unlawful acquisition, use or disclosure?

The claimant must prove one or more of the following, in circumstances constituting a breach of confidence in confidential information:

- unlawful acquisition;
- use; or
- disclosure.

1.5 Reasonable Measures

Under the statutory regime imposed by the Directive/Regulation, for information to qualify as a trade secret, it must have been subject to "reasonable steps under the circumstances" to keep it secret (Regulation 2(1)). As yet, the cases decided since the statutory regime in the UK came into force have not considered the interpretation or practical consequences of this new requirement in any detail.

It is expected that what constitutes "reasonable steps" in any given case will depend on, among other things, the type of information, its value, how that information is required to be used in the day-to-day operation of an undertaking's business, and the ordinary practices in the industry sector in which the undertaking operates.

Under the common law/equitable regime for breach of confidence, "reasonable steps" is not a requirement for protection of information as a trade secret. However, the information in question must have "the necessary quality of confidence" (which means it needs to be "sufficiently secret") as well as have been "imparted in circumstances importing an obligation of confidence". In practice, and subject to how the case law in the statutory regime develops, it seems likely that establishing that certain "reasonable steps" have been taken will assist in demonstrating the "necessary quality of confidence" test has been satisfied.

Some good practice options include:

- ensuring that dissemination of the trade secret to employees is on a need-to-know basis only;
- implementing strict security measures around employees who have access to the trade secret;
- providing employees who have access to the trade secret with appropriate training to raise awareness of the key issue of confidentiality;
- implementing protective measures over the storage of confidential information, including any trade secrets where relevant, such as keeping hard copies physically secure and using passwords or encryptions if stored electronically;
- marking confidential documents as confidential; and
- protecting electronic files with passwords and considering the use of firewalls, automatic intrusion detection systems and authentication measures.

Following the exit of the UK from the European Union, it remains to be seen whether decisions from European courts, including the CJEU, in relation to the meaning of "reasonable steps" under the Directive/Regulation will influence UK judges.

1.6 Disclosure to Employees

Disclosure to employees does not impact the availability of protection for a trade secret per se. However, the manner (eg, breadth) with or without accompanying confidentiality controls and the extent of the disclosure are relevant in so far as these factors will relate to the assessment of whether reasonable steps were taken to keep the information secret.

For example, if trade secrets are stored on the company's shared drive with no restrictions on which employees can access the information, this may undermine statutory protection as it could be perceived as a failure to take reasonable steps and make it appear for common law purposes as if the information did not have the necessary quality of confidence.

1.7 Independent Discovery

Trade secret protection does not protect against another party's independent discovery of the substance of the secret information or genuine reverse engineering. An element of misappropriation is required; ie, unlawful acquisition, use or disclosure that constitutes a breach of confidence in confidential information.

1.8 Computer Software and Technology

There are no computer/software-specific protections for trade secrets in the UK.

1.9 Duration of Protection for Trade Secrets

There is no limit on the duration of protection of a trade secret. It will retain its protection as long as it is kept sufficiently secret and, for statutory protection, reasonable steps to protect its secrecy have been, and continue to be, taken.

However, information can lose its trade secret status by becoming out of date and/or ceasing to have commercial value.

The controlled disclosure of trade secret information in a confidential setting – eg, in accordance with a non-disclosure agreement (NDA), or appropriate confidentiality terms in an employee agreement – will not affect the existence or duration of the trade secret per se, but in general the more people to whom a secret is disclosed, the higher the risk that the information becomes generally known, with an accompanying risk of loss of trade secret protection. As noted above, limiting disclosure of trade secrets to a need-to-know basis is a potential reasonable step that can be taken to protect the secrecy of information.

In general, owners of trade secrets should ensure all disclosure is accompanied by well-defined trade secrets policies, appropriate NDAs or other confidentiality terms, and clear parameters and protections surrounding use and onward disclosure.

1.10 Licensing

The owner of a trade secret has a right to commercialise the trade secret, including via licence.

The trade secret owner needs to take reasonable steps to maintain the secrecy of the information. For example, licences should include carefully crafted confidentiality provisions specific to the relevant trade secret. Furthermore, practical measures should be set up to ensure protection of the trade secret within both the licensor and licensee companies, including who has electronic and physical access to the information.

If there are a large number of non-exclusive licences, it is possible that even with the protection of confidentiality clauses, the information will no longer be sufficiently secret to qualify as a trade secret.

1.11 What Differentiates Trade Secrets from Other IP Rights

Trade secrets are more flexible and potentially broader in scope/subject matter than other IP rights. They can cover very commercially valuable information that it is not possible to protect (either at all, or effectively) by patents (eg, algorithms) or copyright (eg, the recipe for Coca-Cola). They are also not time limited, unlike patents, designs or copyright. The most significant difference is that there is no public disclosure at all, unlike for patents or trade marks of designs.

Trade secrets can also be enforced through equity and contractual bases.

1.12 Overlapping IP Rights

It is possible for trade secrets to co-exist with other rights; eg, trade secrets in pre-clinical data that accompanies an unpublished patent application for a new chemical entity.

Alternatively, it is possible to have a trade secret in relation to an algorithm that co-exists with copyright rights.

However, a trade secret requires maintaining information as confidential that is antithetical to most (but not all) other IP rights that require disclosure as a condition of the right.

1.13 Other Legal Theories

Trade secrets misappropriation can also potentially be litigated through the tort of inducing or procuring a breach of contract, the tort of unlawful interference, breaches of fiduciary duty (eg, where the misappropriation is by an employee) or breach of contract (where there is an NDA in place).

Tortious claims may be useful should a party wish to bring an action against an ex-employee's new employer who is a competitor. The tort requires actual knowledge and intention to cause economic loss.

1.14 Criminal Liability

There are no criminal offences specific to trade secrets misappropriation.

However, there may be criminal laws that can cover misappropriation. For example, "fraud by abuse of position" under Section 4 of the Fraud Act 2006 or offences under the Computer Misuse Act 1990.

Civil trade secrets claims under common law/equity and the Directive/Regulation can be pursued in parallel.

1.15 Extraterritoriality

It is possible to bring a claim based on misappropriation that happens in another country. The key question is whether the UK is an appropriate forum in which to hear the dispute, considering the totality of the dispute between the parties (forum conveniens). The courts look for factors connecting the dispute to the jurisdiction; eg, damage suffered.

The recent case of Celgard, LLC v Shenzhen Senior Technology Material Co Ltd [2020] EWHC 2072 (Ch) confirmed the ability to bring a trade secrets claim in the UK based on an extraterritorial misappropriation. This point was upheld on appeal ([2020] EWCA Civ 1293). In Celgard, Celgard is based in the USA, the relevant former employee signed an NDA governed by the law of South Carolina, USA, and any misappropriation of trade secrets was likely to have taken place in the USA. The incorporation of those trade

secrets into products by the defendants would have taken place in China. However, the UK was where Celgard would lose a key customer and therefore the location where the damage became irreversible.

A key point in relation to jurisdiction, which was discussed in the Court of Appeal, was the effectiveness of Article 4(5) of the Directive, which prohibits unlawful use of a trade secret in the context of goods "where the person carrying out such activities knew, or ought, under the circumstances, to have known that the trade secret was used unlawfully within the meaning of paragraph 3". Paragraph 3 includes reference to a person "having acquired the trade secret unlawfully", which leaves open the question of which law should apply to the question of whether the acquisition was "unlawful". This was not resolved in the Court of Appeal and Arnold LJ acknowledged that this was a very difficult question that may, in due course, have to be answered by the CJEU (at least for the remaining member states of the EU).

2. MISAPPROPRIATION OF TRADE SECRETS

2.1 The Definition of Misappropriation

Under Regulation 3(1), the claimant must prove one or more of unlawful acquisition, use or disclosure, in circumstances constituting a breach of confidence in confidential information. As the claimant only needs to prove one of unlawful acquisition, unlawful use or unlawful disclosure, it is possible in a claim for misappropriation that the information was gained lawfully but then used or disclosed unlawfully. For example, the trade secret may have been shared during a joint venture and then misappropriated by the joint venture partner by use of the trade secret outside the scope of the joint venture.

Under common law/equity the element of "misappropriation" is captured by the third limb of the common law test; ie, unauthorised use (or threatened use) outside the scope of consent will be a breach.

2.2 Employee Relationships

Trade secrets misappropriation under the Regulation/Directive does not differ for an employee. The same requirements of secrecy, commercial value and reasonable steps apply.

Under common law/equity, employees are under a general fiduciary duty to keep their employer's information confidential. This duty is qualified in the case of ex-employees. For an ex-employee, only trade secrets rather than "mere" confidential information can be protected. This is the main factor that distinguishes trade secrets from confidential information under UK law.

The relevant factors to be considered in determining whether information held by employees falls into the "mere confidential information" class or the "trade secrets class" are set out in **1.2 What Is Protectable as a Trade Secret**.

This distinction is particularly critical where there is an absence of express restrictions.

However, employees also usually have express terms in their employment agreements restricting use and disclosure of confidential information and trade secrets, including post-employment.

2.3 Joint Ventures

Any joint venture is likely to have express confidentiality provisions included in the agreement forming the joint venture.

Furthermore, it is possible that a fiduciary relationship will in fact be found with respect to (eg, the directors of) the joint venture, such that the

parties will owe each other fiduciary obligations, including the duty of confidence.

In Ross River Limited v Waveley Commercial Limited (2012) EWHC 81 (Ch), the High Court set out two propositions for identifying the existence of a fiduciary relationship:

- a fiduciary is someone who has undertaken to act for, or on behalf of, another in a particular matter in circumstances that give rise to a relationship of trust and confidence; and
- this concept captures a situation where one person is in a relationship with another that gives rise to a legitimate expectation, which equity will recognise, that the fiduciary will not utilise their position in a way that is adverse to the interests of the principal.

Therefore, it is likely to depend on the nature of the joint venture and the way in which rights and duties are divided and information disclosed as to whether the relationship between the parties engaged in a joint venture will be considered a fiduciary one.

2.4 Industrial Espionage

Industrial espionage is a lay rather than legal term in the UK. The type of additional claims available will depend on the type of industrial espionage and the type of actor (ie, state/foreign private individual/domestic citizen). For example, criminal claims may be possible in relation to "fraud by abuse of provision" under Section 4 of the Fraud Act 2006 or offences under the Computer Misuse Act 1990. Civil trade secrets claims under common law/equity and the Directive/Regulation are also likely to be available.

3. PREVENTING TRADE SECRET MISAPPROPRIATION

3.1 Best Practices for Safeguarding Trade Secrets

There are no specifically sanctioned "best practice" guidelines in the UK regarding safeguarding trade secrets. The following are merely some suggestions.

Implementation of best practices may include the following.

Physical steps:

- building access controls;
- ID security check; and
- security guard monitoring.

Digital protection:

- dedicated VPNs;
- printing logs;
- USB drive restriction;
- remote access restriction; and
- password protection.

Policies/agreements:

- detailed pre-employment screening;
- regular training; and
- division of information.

3.2 Exit Interviews

Exit interviews are quite common in the UK. Depending on the circumstances of the person's position and departure, a confirmatory confidentiality agreement may be signed. Employers will usually ask where the employee is going, but the employee is under no obligation to provide that information.

4. SAFEGUARDING AGAINST ALLEGATIONS OF TRADE SECRET MISAPPROPRIATION

4.1 Pre-existing Skills and Expertise

The UK recognises the distinction between the general knowledge and skills of an employee and protectable trade secrets.

In general, types of employee "knowledge" can be classified into the following categories:

- trade secrets, which are protectable (regardless of contractual provisions) both during and after employment;
- confidential information, which is protectable during the term of employment;
- information that amounts to the skill and knowledge of the employee, which belongs to the employee; and
- public information, which cannot be protected.

The Directive expressly provides that it will not restrict employees' use of "information that does not constitute a trade secret as defined", or of "experience and skills honestly acquired in the normal course of their employment".

UK law recognises a distinction between making use of information and skills acquired from years of working in a job or industry and particular information that is specifically committed to memory (see Printers and Finishers Ltd v Holloway (1965) 1 WLR 1 and Faccenda Chicken Ltd v Fowler (1987) Ch 117).

There is no specific doctrine of "inevitable disclosure" in the UK. However, a similar concept is incorporated into breach of fiduciary duties. For example, in Prince Jefri Bolkiah v KPMG (1998) UKHL 52, the court held that once it was shown that the firm (KPMG) was in possession of confidential information due to employee knowledge, the evidential burden shifted to the firm to show that there was no risk that the information would come into the possession of those acting against the original holder of the confidential information.

4.2 New Employees

When hiring an employee from a competitor, best practices include:

- requiring the new employee to sign an affidavit or employment agreement confirming they did not take their previous company's information and will not use it in their present employment; and
- maintaining records of independent creation of new concepts/ideas/customer lists.

5. TRADE SECRET LITIGATION

5.1 Prerequisites to Filing a Lawsuit

There are no trade secrets-specific pre-action procedural steps that must be satisfied before a trade secrets action can be commenced in the UK.

Under Civil Procedure Rule (CPR) 7, proceedings commence when the court issues (ie, seals and dates) a claim form at the request of the claimant. A claim form is a brief document, setting out key information about the claim and the relief sought.

Once issued by the court, the claim form must be served within four months (or six months where it is to be served outside the jurisdiction).

A more detailed account of the factual elements of the claim as alleged is set out in the particulars of the claim, which must be contained in, or served together with, the claim form, or served

on the defendant within 14 days of service of the claim form (but no later than the latest day for serving the claim form).

5.2 Limitations Period

Under the Directive/Regulations, the limitation period is six years (Regulation 5). The limitation period begins from the later of:

- the day on which the unlawful acquisition, use or disclosure that is the subject of the claim ceases; or
- the day of knowledge of the trade secret holder (ie, when the owner becomes aware of the breach).

A breach of confidence/trade secrets under equity does not have a limitation period – see Limitation Act, Section 36(1).

In most cases, action will be taken immediately on discovery of the breach so the relevance of the limitation period is minimal.

5.3 Initiating a Lawsuit

See **5.1 Prerequisites to Filing a Lawsuit**.

5.4 Jurisdiction of the Courts

There is no specialised trade secrets jurisdiction. Claims under GBP100,000 are likely to be brought in the County Court and claims over GBP100,000 or claims that the claimant views as complex or of particular importance are likely to be brought in the High Court. In the High Court they are likely to be heard in the Business and Property Courts. Which specific list (eg, commercial, IP, Chancery) will depend on the broader context of the trade secrets dispute; ie, whether it will take place in the context of a contractual dispute.

5.5 Initial Pleading Standards

The pleadings must contain all material facts to make out the claim. The claimant is not required to present its evidence of those facts at the pleading stage. However, the claimant/its solicitors are required to sign a statement of truth in relation to their honest belief in the truth of the matters pleaded. Cases based on inference are also permitted, but are more liable to be struck out depending on the strength of the inference.

Although there are no special requirements for trade secrets, an area of difficulty for claimants can be pleading what constitutes the trade secret itself with the necessary specificity (see Saltman Engineering Co Ltd v Campbell Engineering Co Ltd (1948) 65 RPC 203) to avoid the claim being struck out.

5.6 Seizure Mechanisms

In exceptional circumstances, a party may be awarded a search order upon application to the court, allowing their representatives to enter the defendant's premises and search for, remove and detain any documents, information or material pertinent to the case.

In the English courts, search orders are considered an extremely invasive measure, and will only be awarded (under the court's power derived from Section 7(1) of the Civil Procedure Act 1997) for the purpose of preserving evidence in the most extreme cases. The claimant must show both that it has a strong case and that there are good reasons for believing that the defendant is likely to destroy evidence.

Seizures are also available as an interim measure under Regulation 11(3). This provision is yet to be tested in the UK courts.

5.7 Obtaining Information and Evidence

Parties can seek assistance from the court to obtain evidence through the process of disclosure (either pre-action or after proceedings have started). The level of disclosure available is a matter of juridical discretion.

The UK business and property courts are currently involved in a disclosure pilot scheme running until the end of 2021. It is expected to continue in a similar form afterwards. The guidelines are contained in Practice Direction 51U.

Parties may follow one of disclosure models A to E, depending on the level of disclosure required for the case. At one end of the spectrum, model A only requires disclosure of any known adverse documents; and at the other, model E requires "wide search-based disclosure", and is ordered only in exceptional circumstances.

Disclosure of documents may also be ordered under CPR 31.16 before proceedings are commenced, where such documents are desirable in order to dispose fairly of anticipated proceedings, assist resolution of the dispute without proceedings, or to save costs. For instance, in The Big Bus Company Ltd v Ticketogo Limited (2015) EWHC 1094 (Pat), the court granted pre-action disclosure of Ticketogo's licences with third parties (for lawyers' eyes only) on the basis that it might dispose of the action.

In extreme circumstances, a party may be awarded a search order upon application to the court, allowing their representatives to enter the defendant's premises and search for, remove and detain any documents, information or material pertinent to the case. This is discussed in **5.6 Seizure Mechanisms**.

5.8 Maintaining Secrecy While Litigating

In its inherent jurisdiction, the court is able to close hearings and declare certain evidence confidential and the parties and court can limit information to "confidentiality clubs".

Furthermore, the Directive/Regulation specifically requires that trade secrets remain confidential during and after legal proceedings. Regulation 10(1) prevents those who take part in trade secret proceedings (including parties, lawyers, experts and court officials) from using or disclosing the trade secret or information alleged to be a trade secret. This subsists until the court finds that the information was not a trade secret or where it enters the public domain (Regulation 10(3)). The court may also restrict access to a document or hearing, or redact its judgment under Regulation 10(5). These steps can be taken on the application of a party or its own initiative (Regulation 10(4)). Parts of the judgment can be redacted in accordance with Regulation 18.

5.9 Defending against Allegations of Misappropriation

Best practices for a defendant in a trade secret litigation is to show that the alleged trade secret does not meet the required standards of a trade secret. For example, to attack each of the elements to show that the alleged trade secret was not secret, not commercially valuable or that reasonable steps were not implemented to keep it confidential or that the information was generally known within the industry in question. If applicable, the defendant can also attempt to show that the use or disclosure was within the scope of permitted use; for example, the alleged use may be within the scope of the interpretation of the joint venture contract.

There are limited defences available on public interest and whistle-blower protection grounds, but these are unlikely to be available to most defendants in trade secrets litigation.

5.10 Dispositive Motions

The UK courts have case management powers over their cases. While there are no specific dispositive motions in relation to trade secrets proceedings, UK courts routinely split the question of liability (first) and relief/quantum (second) into separate hearings.

Furthermore, parties can apply for a separate question where the answer may dispose of the action in its entirety. For example, the defendant can apply for a strike out of the claimant's pleading and the claimant can apply for a summary judgment.

Ultimately, this is within the judge's discretion.

5.11 Cost of Litigation

The costs of a proceeding are widely variable depending on the technology involved and the experts and/or experiments required. Litigation funding is available in the UK.

6. TRIAL

6.1 Bench or Jury Trial

Trade secret proceedings are heard and decided by a single judge in the first instance.

6.2 Trial Process

The claimant files its claim form and particulars of the claim that pleads the cause of action and states the requested relief. The defendant is then required to file an acknowledgement of service and a defence (and the claimant may reply). Usually, one to two months after the close of pleadings, there will be a case management conference (CMC), at which the court will direct how the matter will progress to trial, including in relation to disclosure, factual and expert evidence, the exchange of skeleton arguments and a trial date.

Fact witnesses give their evidence in chief by way of witness statement and are cross-examined during the hearing if required. Expert evidence is given by way of written report and expert witnesses may also be cross-examined if required during the hearing. The parties provide written skeleton arguments ahead of the hearing, and further opening and closing submissions are made orally during the hearing (closing submissions are also exchanged in writing). The judge almost always reserves judgment and then provides a written judgment, usually within three months.

6.3 Use of Expert Witnesses

The UK allows for expert evidence. There are strict requirements to ensure the independence of the expert testimony, which are set out in CPR part 35. The expert's ultimate duty is to assist the court. Experts must prepare their own reports and cannot be actively prepared for cross-examination by the lawyers.

Experts must agree to be bound by the CPR 35 requirements.

The cost of experts varies depending on the field, type of expert, time commitment required and general complexity of the case.

7. REMEDIES

7.1 Preliminary Injunctive Relief

Interim injunctions are available by application to the court and are a discretionary equitable remedy. Injunction applications are usually heard on an inter partes basis (notice is given to the defendant) and can be heard urgently if required. In order for an interim injunction to be granted, under Section 37 of the Senior Courts Act 1981, the court must be satisfied that it is "just and convenient". This is generally established by following the test developed in American Cyanamid Co (No 1) v Ethicon Ltd (1975) UKHL 1.

Requirements for Preliminary Injunctive Relief

Firstly, there must be a serious question to be tried on the merits. This is generally regarded as a low threshold to satisfy. What needs to be shown is that the patentee's cause of action has substance (ie, some prospect of success).

Secondly, the court considers the "balance of convenience". Some key considerations relevant to whether the balance of convenience favours the granting of an interim injunction are the following.

- Would damages be a sufficient remedy?
- Is there irreparable harm?

Delay in applying for an interim injunction will reduce the likelihood of obtaining one.

If an interim injunction is granted, the court may require that the injunction applicant gives an undertaking in damages; ie, agrees to pay damages to the respondent for losses caused by granting of the injunction if later it is held that the injunction was wrongly granted (eg, if the court finds that the information in question was not a trade secret).

Ex Parte Injunctions

Ex parte injunctions (ie, without notice to the other side) are available in very exceptional cases, such as where the matter is so urgent that there may not be time to notify the defendant, or where there is real concern that the defendant may seek to dispose of evidence.

In an ex parte hearing, the applicant must provide full and frank disclosure to the court and disclose all matters that are material to the court (including legal principles that are not in its favour). If an ex parte injunction is granted, the court will usually make provision for a return date hearing, at which the respondent may contest the injunction.

Available Interim Measures

Regulation 11 of the Regulation outlines available interim measures, which include:

- the cessation of, or (as the case may be) the prohibition of, the use or disclosure of the trade secret on a provisional basis;
- the prohibition of the production, offering, placing on the market or use of infringing goods, or the importation, exportation or storage of infringing goods for those purposes; and
- the seizure or delivering up of the suspected infringing goods, including imported goods, so as to prevent the goods entering into, or circulating on, the market.

These provisions have not been tested in the UK courts but would probably be interpreted in a way that is consistent with the requirements of those remedies at common law.

7.2 Measures of Damages

Under common law, the claimant may elect between damages and an account of profits.

If the claimant elects an award of damages, it will need to show on the balance of probability the harm suffered by it. This may be by way of lost sales, lost contracts, lost royalties or any other compensatory measure. Punitive or exemplary damages are extremely rare.

If the claimant elects an account of profits, the substantial body of the evidence is likely to be derived from the defendant's disclosure.

Regulation 3 of the Regulation provides that common law remedies remain available to claimants. The Claimant can apply for relief both under common law remedies and the remedies under the Regulation.

Regulation 17(1) of the Regulation sets out the mechanism for assessing damages. The damages should be "appropriate to the actual prejudice suffered as a result of the unlawful acquisition,

use or disclosure of the trade secret"; ie, compensatory damages.

The court may take into account "appropriate factors", including:

- negative economic consequences, including any lost profits that the trade secret holder has suffered, and any unfair profits made by the infringer (Regulation 17(3)(i)); and
- non-economic factors, including moral prejudice (Regulation 17(3)(ii)).

The court may also award damages on the basis of a hypothetical licence (Regulation 17(4)). This is similar to under Article 13 of the IP Enforcement Directive (Directive 2004/48/EC).

7.3 Permanent Injunction

Permanent injunctions are available as a common law and statutory remedy for trade secrets misappropriation.

Regulation 3 of the Regulation provides that common law remedies remain available to claimants. The claimant can apply for relief both under common law remedies and the remedies under the Regulation.

Regulation 14 provides for the following non-financial corrective measures, which include permanent injunctions and delivering up of "infringing" goods:

- the cessation of, or (as the case may be) the prohibition of, the use or disclosure of the trade secret;
- the prohibition of the production, offering, placing on the market or use of infringing goods, or the importation, exportation or storage of infringing goods for those purposes;
- the adoption of corrective measures with regard to the infringing goods, including, where appropriate:
  - (a) recall of the infringing goods from the market;
  - (b) depriving the infringing goods of their infringing quality;
  - (c) destruction of the infringing goods or their withdrawal from the market, provided that the withdrawal does not undermine the protection of the trade secret in question;
- the destruction of all or part of any document, object, material, substance or electronic file containing or embodying the trade secret, or, where appropriate, delivering up to the applicant all or part of that document, object, material, substance or electronic file.

In making a Regulation 14 order, the court must take into account the specific circumstances of the case, including, where appropriate (Regulation 15):

- the value or other specific features of the trade secret;
- the measures taken to protect the trade secret;
- the conduct of the infringer in acquiring, using or disclosing the trade secret;
- the impact of the unlawful use or disclosure of the trade secret;
- the legitimate interests of the parties and the impact that the granting or rejection of the measures could have on the parties;
- the legitimate interests of third parties;
- the public interest; and
- the safeguard of fundamental rights.

If the court places a time limit on its Regulation 14 order, that limit must be sufficient to eliminate the commercial or economic advantage obtained by the misappropriation (Regulation 15(2)). There are no limits on the length of a permanent injunction, however, the defendant can apply to the court for the revocation of a Regulation 14 measure on the basis that the information

no longer constitutes a trade secret (Regulation 15(3)).

In relation to former employees, an employer may also be able to enforce a restraint of trade against an employee moving to a competitor. This will depend on the contractual background as well as the reasonableness of those restrictions, and the ability of the employee to continue to earn a living if so restrained.

7.4 Attorneys' Fees

See **7.5 Costs**.

7.5 Costs

The general rule is that the unsuccessful party pays the successful party's costs. The court has the power to make whatever costs orders it finds most appropriate (CPR 44). Costs awards can be reduced or limited due to poor conduct, failing to comply with pre-action protocols or other factors.

In making an order as to costs, the court must consider the overriding objective that cases be dealt with "justly and at proportionate cost". When considering whether costs incurred are proportionate, the court will consider:

- the amount in dispute;
- the value of any non-monetary relief sought;
- the complexity of the case;
- any additional costs relating to poor conduct on behalf of the unsuccessful party; and
- any other relevant factors in the circumstances.

The general rule is that costs will be assessed on the standard basis, which allows for the recovery of proportionate costs. This may mean that some costs are not recoverable and others are reduced. Parties should expect that if costs are calculated on the standard basis, the successful party will recover 60–75% of its costs. In assessing the proportion of its costs that a successful party may be able to recover, the court will typically consider the number of issues on which that party succeeded, as well as the time spent at trial on the issues raised by each of the parties.

8. APPEAL

8.1 Appellate Procedure

Applications for appeals need to be made within 21 days of the decision of the lower court. Appeals for trade secret cases require the permission of the court.

The application can be made to the lower court (High Court or County Court), or if they have already refused leave to appeal, the prospective appellant (claimant or defendant) may appeal to the Court of Appeal (CPR 52.3(2)).

Permission will only be given where the court believes that the appeal would have a real prospect of success, or there is some other compelling reason to allow the appeal to go ahead (CPR 52.6(1)). It usually takes 12–18 months for the Court of Appeal hearing to be heard.

A further appeal from the Court of Appeal to the Supreme Court is possible for matters of "general public importance". Permission is not usually granted. If it is, it usually takes a further one to two years for the Supreme Court hearing to be heard.

It is possible, although extremely difficult, to successfully appeal an interim decision (see Wright v Pyke and another (2012) EWCA Civ 931, Hadmor Productions v Hamilton (1983) 1 AC 191, stressing the limited function of the appellate court).

8.2 Factual or Legal Review

Appeals are limited to a review of the first-instance decision on points of law and do not usually involve reconsidering the evidence heard and findings of fact made at first instance. Parties have to apply to adduce fresh evidence and it is rarely allowed.

If an issue has not been raised at first instance, it is difficult to rely on it on appeal. Parties file written outlines both at the initial grounds of appeal stage and in submissions prior to the hearing. The parties' advocates will then have an opportunity for oral submissions.

9. CRIMINAL OFFENCES

9.1 Prosecution Process, Penalties and Defences

There are no criminal offences specific to trade secrets misappropriation.

However, there may be criminal laws that can cover misappropriation; for example, "fraud by abuse of position" under Section 4 of the Fraud Act 2006 or offences under the Computer Misuse Act 1990. Directors and other officers can also be prosecuted (together with the corporation) under the Fraud Act (Section 12). There are no specific defences to these sections.

Given "trade secret misappropriation" is not a specific offence, there are therefore not specific mechanisms available for trade secret owners to co-ordinate with law enforcement offences. Depending on the circumstances of the misappropriation, it is likely to be dealt with by cybercrime units.

10. ALTERNATIVE DISPUTE RESOLUTION

10.1 Dispute Resolution Mechanisms

There is no formal ADR mechanism, it is party led. The pre-action conduct can be taken into account by the court. The court's guidance is generally that litigation should be a last resort and that parties should consider whether negotiation or some other form of ADR might enable them to settle their dispute without commencing proceedings. Parties are expected to exchange sufficient information to understand the other's position and to attempt to settle the issues between themselves without recourse to litigation.

Parties are encouraged to consider ADR at the outset; however, they are also encouraged to consider ADR and settlement generally throughout the litigation timetable.

The Practice Direction on Pre-Action Conduct and Protocols explicitly refers to mediation, arbitration, early neutral evaluation and Ombudsmen schemes as ADR options available for resolution of disputes.

Kirkland & Ellis is an international law firm with approximately 2,900 attorneys across the United States, Europe and Asia. Kirkland's trade secrets litigation practice includes approximately 75 attorneys with years of experience representing both plaintiffs and defendants in trade secrets matters in diverse industries. They draw upon the formidable depth of Kirkland's intellectual property, commercial litigation and other practices to provide an approach tailored to the intricacies of each individual case. Kirkland's trade secrets attorneys have litigated the broad spectrum of trade secret disputes, ranging from outright theft to violation of various agreements, including employment, R&D, joint development, and technology transfer and know-how agreements. They have won significant victories for clients – including nearly USD1.4 billion in damages in 2020 alone – in these matters in UK courts, US federal and state courts, and in arbitrations, and have worked collaboratively with law enforcement agencies to protect clients' intellectual property. The practice's success is grounded in extensive jury and bench trial experience, and a sophisticated appellate practice to protect the clients' successes at the trial level.

AUTHORS

Nicola Dagg is a partner and leader of Kirkland's IP litigation practice in London. She draws upon a wealth of experience built up over more than 24 years at the forefront of IP litigation, particularly in relation to trade secrets and patents. Her broad and varied practice includes pharmaceutical and biologics patent litigation; strategic life sciences patent and product life cycle advice; co-ordinating global IP enforcement/defence cases; hi-tech, digital and telecommunications litigation; and SEP and FRAND disputes. Nicola, who also has an MA in natural sciences, is renowned for her strategic and creative approach to solving difficult and commercially critical IP issues and regularly represents her clients in ground-breaking cases in the Court of Appeal and UK Supreme Court.

Daniel Lim is a partner in Kirkland's IP litigation team in London. Daniel has a broad practice that covers a wide range of fields, but is particularly noted for his experience in high-stakes trade secrets and life sciences patent litigation, particularly in the pharmaceutical industry. Daniel is regularly called upon to assist clients in devising, co-ordinating and executing strategies for complex multi-jurisdictional disputes at a pan-European and global scale. His previous case experience covers a broad range of technical fields, including oncology, molecular diagnostics and biostatistics, often involving issues at the cutting edge of the law, notably in relation to second medical-use patents. Daniel frequently comments on life sciences and IP topics and is regarded as a thought leader in the IP community, including in his role as vice-chair of AIPPI's standing committee on biotechnology.

Steven Baldwin is a partner in Kirkland's IP litigation team in London with significant experience representing clients in trade secrets, patent, life sciences regulatory, copyright and trade mark matters. His practice focuses primarily on former employee trade secrets cases and complex cross-border life sciences and telecommunications patent disputes. Steven's trade secrets experience includes disputes in the life sciences and financial industries worth vast sums of money, including a case in which he successfully obtained the extradition of a trade secrets thief who had fled the UK, which resulted in their subsequent incarceration in the UK following criminal charges. Steven is routinely instructed on "bet the farm" cases and is renowned for his clear and focused strategic approach to litigation and finding novel solutions to the complex problems facing his clients. Steven's case experience covers a broad range of technical fields, including mobile telecommunications technologies, algorithmic trading, organic chemistry, antibody biologics, biological product development and screening platforms, formulation science, next generation cancer treatments, and e-cigarette/vaping technologies.

Gabriella Bornstein is an IP litigation associate in the London office of Kirkland & Ellis. She has brought to trial matters involving pharmaceutical and software patents, trade marks and copyright. She also has specific experience with the interplay between trade secrets and patent disputes. She has particular expertise with respect to trade secrets for algorithms and AI-led advancements. Gabriella is dual qualified in science and law, giving her particular insight into the challenges facing her IP clients.

Kirkland & Ellis International LLP

30 St Mary Axe
London
EC3A 8AF
United Kingdom

Tel: +44 20 7469 2000
Fax: +44 20 7469 2001
Email: Nicola.dagg@kirkland.com
Web: www.kirkland.com

KIRKLAND & ELLIS

USA

Law and Practice

Contributed by:
Claudia Ray, Joseph Loy, Patrick Arnett and Kyle Friedland
Kirkland & Ellis LLP see p.284

CONTENTS

1. LEGAL FRAMEWORK

1.1 Sources of Legal Protection for Trade Secrets

In the USA, trade secrets are protected by the following:

- federal trade secret statute, the Defend Trade Secrets Act (DTSA);
- individual state laws modelled after the Uniform Trade Secrets Act (UTSA), which was promulgated in 1979 as a model act that each state could use as a template for enacting its own trade secret legislation; and
- common law protection in New York, which is the only state that has not yet adopted a version of the UTSA.

An individual or corporate entity may bring claims under the DTSA and a state's trade secret law simultaneously because the DTSA does not pre-empt state trade secret laws. The UTSA, however, contains a pre-emption clause that displaces common law trade secret causes of action.

The interpretation of federal trade secret law is within the jurisdiction of the federal courts, with the Supreme Court of the United States acting as the final court of appeal for such interpretation. The interpretation of each state's statutory law is within the jurisdiction of the specific state within which the respective law was enacted. Federal and state case law serves to guide litigants' understanding of the metes and bounds of any particular trade secret law.

1.2 What Is Protectable as a Trade Secret

In general, a trade secret consists of commercially valuable information that is valuable because of its secrecy. A trade secret also has to satisfy a minimum standard of novelty to avoid being unprotected common knowledge.

Under the DTSA, a trade secret includes "all forms and types of financial, business, scientific, technical, economic, or engineering information" (18 USC Section 1839(3)).

Under the UTSA, a trade secret is information in the form of a "formula, pattern, compilation, program, device, method, technique, or process" (UTSA Section 1(4)).

Under the common law, a trade secret is "any formula, pattern, device or compilation of information which is used in one's business, and which gives [the business] an opportunity to obtain an advantage over competitors who do not know or use it" (Restatement of Torts Section 757, Comment b).

1.3 Examples of Trade Secrets

Examples of a trade secret under the DTSA and state trade secret laws modelled after the UTSA include:

- marketing and advertising research (Whyte v Schlage Lock Co, 101 Cal App 4th 1443, 1455-56 (2002));
- process and manufacturing technologies (see above reference);
- formulas and methods (see above reference);
- cost- and pricing-related information (Walker Mfg, Inc v Hoffmann, Inc, 261 F Supp. 2d 1054, 1080 (N.D. Iowa 2003));
- business plans and information, sales strategies and financial information (Avery Dennison Corp v Kitsonas, 118 F Supp 2d 848, 854 (SD Ohio 2000));
- source code (Wellogix, Inc v Accenture, LLP, 716 F 3d 867, 875 (5th Cir 2013));
- internal design and software architecture documents; and
- customer lists (Fireworks Spectacular, Inc v Premier Pyrotechnics, Inc, 86 F Supp 2d 1102, 1106 (D Kan 2000)).

Examples of a trade secret under the common law, which is still the applicable law in New York and continues to be persuasive precedent in UTSA states, include "any formula, pattern, device or compilation of information which is used in one's business", such as pricing-related information, customer lists or source code (Restatement of Torts Section 757, Comment b; Laro Maint Corp v Culkin, 700 NYS 2d 490, 492 (1999); E Bus Sys, Inc v Specialty Bus Sols, LLC, 739 NYS 2d 177, 179 (2002); MSCI Inc. v Jacob, 992 NYS 2d 224, 225 (2014)).

1.4 Elements of Trade Secret Protection

DTSA

Under the DTSA and state trade secret laws, a claimant must prove the following three elements to prevail on a claim of trade secret misappropriation:

- that the claimant owns a trade secret;
- that the trade secret was misappropriated by the defendant; and
- that the claimant was damaged by the defendant's misappropriation.

Under the DTSA and the various state trade secret laws modelled after the UTSA, a claimant has to prove the existence of a trade secret by showing the following:

- that the owner has taken reasonable measures to maintain the secrecy of the trade secret; and
- that the trade secret derives actual or potential economic value from not being generally known or readily ascertainable through proper means to another who can obtain economic value from the information's use or disclosure.

Additionally, some state trade secret laws explicitly state that the owner must have taken reasonable measures under the circumstances to maintain the secrecy of the trade secret – for example, see Alta Devices, Inc, 343 F Supp 3d at 877.

New York

In New York, there are six factors that are generally considered when determining whether a trade secret exists:

- the extent to which the information is known outside of an individual business;
- the extent to which it is known by employees and others involved in their business;
- the extent of measures taken to guard the secrecy of the information;
- the value of the information to the holder and to their competitors;
- the amount of effort or money expended in divulging the information; and
- the ease or difficulty with which the information could be properly acquired or duplicated by others.

Some courts in UTSA states continue to consider these six factors in determining the existence of a trade secret, despite having adopted the UTSA.

In order to prove trade secret misappropriation in New York, a claimant must prove that they own a trade secret and that the defendant used the trade secret by breaching an agreement, confidential relationship or duty, or through discovery by improper means.

Although ownership is a common element to most state and federal claims, recent trends suggest a claimant may be able to bring a claim for misappropriation under some state trade secret laws where the claimant only demonstrates lawful possession of the trade secret – for example, see Adv Fluid Sys, Inc v Huber, 958 F.3d 168, 177-178 (3d Cir. 2020).

1.5 Reasonable Measures

Trade secret owners must generally show that they took reasonable measures to protect their trade secrets. Examples of reasonable measures include:

- warning employees and third parties about the confidential nature of the information through, for example, confidentiality agreements, confidentiality designations on documents, employee training or trade secret policies in an employee handbook;
- password protections and electronic firewalls;
- physically locking confidential information;
- restricting access to physical and electronic areas where trade secrets are stored; and
- minimising the number of people that learn the trade secret.

1.6 Disclosure to Employees

An employee has an implied duty not to disclose an employer's trade secret. Disclosing a trade secret to an employee who cannot perform their job without knowledge of the trade secret does not destroy the trade secret. If, however, the trade secret is further disclosed to employees who do not need to know it to perform their jobs, and precautions are not taken to protect the confidentiality of the trade secret, then there may be a risk that trade secret protection will be lost.

1.7 Independent Discovery

Trade secret protection cannot be used against a party who independently discovered or reverse engineered the alleged trade secret. In other words, trade secret misappropriation is not a "strict liability" offence, unlike patent infringement. Misappropriation would not lie against an independent developer in part because there was no acquisition from the trade secret owner (nor from another party with an obligation to the trade secret owner).

Similarly, reverse engineering the alleged trade secret from a commercially available product would not be an "improper means" of acquiring the information under trade secret laws (although such activity could violate agreements including those imposed by "shrink-wrap" or "click-wrap" licences). Both independent development and reverse engineering suggest that the alleged trade secret is not difficult to properly acquire or duplicate, a factor often considered in evaluating whether trade secret protection is merited. Independent development and reverse engineering can therefore be valuable defences to a defendant faced with allegations of trade secret misappropriation.

Two parties could conceivably develop the same trade secret independently and without knowledge of the other's development, and both parties would have independent causes of action against third parties for misappropriation. For the same reasons discussed above, however, neither party would be able to successfully recover against the other for trade secret misappropriation.

1.8 Computer Software and Technology

Certain aspects of computer software and technology, such as proprietary source code and internal software design and architecture materials, may be protectable trade secrets under the DTSA and various state trade secret laws if the ordinary standards for trade secret protection are met. There are no specific protections that are unique to computer software and/or technology.

Aspects of software that are apparent to an end user, such as the software's general functionality or user interface, are unlikely to receive trade secret protection unless the end user licence or other agreement imposes an obligation to keep this kind of information secret.

The Computer Fraud and Abuse Act (CFAA) also establishes civil and criminal penalties for knowingly or intentionally either accessing a protected computer (without authorisation) or exceeding the authorised level of access.

1.9 Duration of Protection for Trade Secrets

Trade secrets may remain protected indefinitely, so long as the trade secret owner maintains the secrecy of the trade secret. Accidental or intentional public disclosure may terminate trade secret protection, but such considerations are generally fact-based inquiries.

Controlled disclosure of a trade secret – eg, for licensing or limited disclosure to third-party vendors and employees for business purposes – generally does not nullify trade secret protection. Owners of trade secrets should accompany any controlled disclosure of their trade secret with non-disclosure agreements, company policies or alternative safeguards that maintain the confidentiality of the trade secrets.

1.10 Licensing

A trade secret owner has a right to license the trade secret to a licensee through a contract or licensing agreement. The licensee may pay the trade secret owner royalties in exchange for using the trade secret.

The trade secret owner must still take reasonable steps to maintain the secrecy of the trade secret in order to retain trade secret protection. For example, the licensing agreement may contain a confidentiality restriction or a non-disclosure provision.

The licensing agreement may require the licensee to pay the trade secret owner royalties even if the licensed information is no longer sufficiently secret to qualify as a trade secret, unless the agreement specifically states otherwise. See Warner-Lambert Pharm Co v John J Reynolds, Inc, 178 F Supp 655 (SDNY 1959), aff'd, 280 F 2d 197 (2d Cir 1960).

1.11 What Differentiates Trade Secrets from Other IP Rights

One primary difference between patent and trade secret protection is public disclosure. Unlike a trade secret, which does not have to be registered and cannot be publicly disclosed, patents can only be obtained by applying to the US Patent and Trademark Office. During that process, the patent application and granted patent will be disclosed publicly.

Once the individual's patent application has been granted, the patent provides a 20-year monopoly right from the filing date of the earliest priority application, after which the patented invention enters the public domain and may be used by anyone.

Because of this mandatory disclosure, protecting information as a trade secret may be preferred to protecting it via patent. One disadvantage, however, is that although they can theoretically be protected indefinitely, trade secrets, unlike patents, can be independently discovered or reverse engineered, after which there may be no further protection.

1.12 Overlapping IP Rights

In the USA, patent, trade mark, copyright and trade secret are separate and independent forms of legal protection for intellectual property. Plaintiffs can, and do, frequently assert claims under more than one of these legal protections, simultaneously, based on the same or related conduct.

An individual cannot seek both patent and trade secret protection for the same information. They may, however, obtain overlapping rights in a single product, such as protecting the design of

the product with a patent, while protecting the composition of the product as a trade secret.

Copyright and trade secret laws may overlap in the computer software field since computer software may receive protection from both.

1.13 Other Legal Theories

In addition to federal or state trade secret claims, plaintiffs should consider whether other common law or statutory claims may apply to the conduct at issue, including, for example, breach of contract, tortious interference with contractual relations, unfair competition, breach of fiduciary duty, aiding and abetting a breach of fiduciary duty, or unjust enrichment.

1.14 Criminal Liability

Responsibility for enforcing criminal laws directed to trade secret theft and related activity rests with prosecutors at both the federal and state levels. While trade secret owners cannot pursue criminal claims as of right, they should consider whether to refer suspected or known trade secret theft to the Department of Justice or a state agency for investigation. The Economic Espionage Act (EEA) imposes criminal liability, including substantial fines and imprisonment, for intentional or knowing theft of trade secrets. As with many federal criminal statutes, attempts to commit trade secret misappropriation as well as conspiring with others in furtherance of stealing trade secrets are themselves criminal activities, even if the theft is not ultimately successful. Fines for organisations that commit an offence under the EEA can reach up to three times the value of the stolen trade secrets to the organisation, including avoided R&D expenses.

Defendants may avail themselves of defences unique to trade secret law. For example, the DTSA includes a "whistle-blower immunity" provision that shields a person from criminal liability under trade secret laws for disclosing a trade secret in confidence to a government official or an attorney solely for the purpose of reporting or investigating a suspected violation of law.

Separately, the CFAA establishes criminal penalties for knowingly or intentionally either accessing a protected computer (without authorisation) or exceeding an authorised level of access. Penalties include fines and imprisonment, the severity of which may be enhanced if the offence is committed for commercial advantage or financial gain.

1.15 Extraterritoriality

The DTSA appears to carry over the EEA's applicability to conduct outside the United States under certain circumstances. The simplest hook for extraterritorial application is if the misappropriator is a person who is a citizen or lawful permanent resident of the United States or an organisation that is organised under the laws of the United States or one of the States.

The DTSA may also have extraterritorial reach even if the misappropriator does not meet either criteria, as long as an act in furtherance of the offence was committed in the United States. Few courts have opined on the contours of extraterritorial application of the DTSA, however, and so the ability of domestic trade secret owners to redress theft by foreign companies and those in their employ will depend greatly on the facts of each particular case.

2. MISAPPROPRIATION OF TRADE SECRETS

2.1 The Definition of Misappropriation

The DTSA and UTSA both define misappropriation as the "acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means or disclosure or use of a trade

secret of another without express or implied consent" (18 USC Section 1839(5); Uniform Trade Secrets Act Section 1(2)).

Improper means include "theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means", but do not include lawful means of acquisition such as reverse engineering or independent discovery (18 USC Section 1839(6); Uniform Trade Secrets Act Section 1(1)).

2.2 Employee Relationships

There is an implied confidential relationship between employers and employees, such that the employee is obligated not to disclose the employer's confidential information.

Disclosing a trade secret to employees does not typically constitute public disclosure resulting in the termination of the trade secret, given that employees have a fiduciary duty to maintain the secrecy of the trade secret. Even if there is no express contractual term in an employment agreement prohibiting the employee from disclosing the trade secret, the employee still has an implied duty to maintain the secrecy of the trade secret.

If, however, the trade secret is disclosed to employees who do not need knowledge of it in order to perform their jobs, and precautions are not taken to prevent those employees from disclosing the trade secret, then the trade secret protection may be terminated. Thus, it is a beneficial precaution to require an employee, in express contractual terms, not to disclose the employer's trade secrets.

2.3 Joint Ventures

Entities that participate in a joint venture owe each other a fiduciary duty not to disclose their trade secret during the joint venture. Nevertheless, it is best practice to create a contract between the owners of the joint venture that requires them to maintain the secrecy of the trade secret both during the joint venture and after its dissolution. Alternatively, a joint venture might involve a company licensing its trade secret to a third-party company. Again, in this scenario, it is best practice for the company with the trade secret to require the third party to sign a contract stating that the third party will not disclose the company's trade secret, rather than relying on any implied duty of confidentiality.

2.4 Industrial Espionage

When a company possesses valuable confidential information, industrial espionage is a likely threat. Companies should take as many security measures as practically feasible to restrict access to trade secrets and confidential information. Even internally, the trade secrets should only be available to a limited number of need-to-know employees, and those employees should frequently be reminded of the confidential nature of the trade secret and be required to sign non-disclosure agreements.

If an individual commits an act of industrial espionage, they may be subject to criminal prosecution under the EEA (18 USC Sections 1831-1839), which provides a cause of action against domestic and foreign misappropriation of trade secrets.

The Federal Bureau of Investigation's Economic Espionage Unit can investigate instances of trade secret theft. There are dedicated units in the US Attorney's Offices that have the ability to prosecute trade secret espionage.

3. PREVENTING TRADE SECRET MISAPPROPRIATION

3.1 Best Practices for Safeguarding Trade Secrets

Common approaches for safeguarding trade secrets include physical, technological and personnel-related means, as follows.

- Physical steps:
  (a) building access controls;
  (b) ID security check;
  (c) security guard monitoring;
  (d) visitor logs;
  (e) supervised tours; and
  (f) labelling confidential information.
- Technological protection:
  (a) dedicated VPN networks;
  (b) password protection; and
  (c) mobile device management software.
- Personnel:
  (a) pre-employment screening including determining whether new hires are subject to any non-compete agreements;
  (b) training;
  (c) employee handbook that describes the policies on confidentiality and trade secrets; and
  (d) non-disclosure agreements for each new hire, visitor and third-party vendor/consultant.

3.2 Exit Interviews

It can be useful for an employer to conduct exit interviews of departing employees. Such interviews often incorporate some or all of the following:

- reminding the employee not to disclose any trade secret information;
- reminding the employee to return all company property, including badges, access cards and electronic devices such as laptops or cell phones;
- asking the employee about the nature of his or her new position, such as any responsibilities, the name of the new employer, and the new employer's address (but the employee may not have to answer);
- asking the employee if they have returned or destroyed electronic and physical copies of company materials;
- asking the employee to sign an affidavit of compliance or a written statement that they will not disclose confidential information or company trade secrets and that they have searched for, located and returned or destroyed all company property; and
- asking the employee if they have any questions regarding the confidentiality of any trade secrets.

4. SAFEGUARDING AGAINST ALLEGATIONS OF TRADE SECRET MISAPPROPRIATION

4.1 Pre-existing Skills and Expertise

An employee's general knowledge and skills, including those already possessed or learned from a prior job, do not per se count as trade secrets that the employee is prohibited from using at a subsequent position. When an individual accepts new employment with a competing entity, however, the employee needs to ensure that he or she only relies on such general knowledge and skill, and does not disclose any trade secrets or confidential information to the new employer.

In some situations, it may be difficult to separate the trade secrets from an employee's general skills, experience and knowledge. To account for those instances, the common law developed an "inevitable disclosure" doctrine, which rec-

ognises that there may be scenarios where the duties of the employee's new position inevitably require the disclosure of the trade secret from the employee's former employment. In such a situation, the previous employer may seek an injunction to prevent the employee from working with a subsequent employer at all (or in a directly competitive role) for a specified time (eg, one year).

However, even if such a risk of inevitable disclosure exists, many courts will deny injunctive relief on this basis alone, absent actual proof of misappropriation, preferring a policy of free employee mobility at the early stage of any litigation. These same courts nevertheless often entertain a cause of action for trade secret misappropriation – and even grant permanent injunctions – on a fully developed factual record proving elements of the claim.

4.2 New Employees

When hiring a new employee, there are a number of steps that an employer can take to minimise the risk of a trade secret claim, including the following:

- performing an analysis of the risk of litigation before hiring the employee;
- ensuring that the employee is not placed in a position where they will inevitably rely on and use a former employer's trade secrets;
- requiring the new employee to sign a non-disclosure agreement and explaining the trade secret confidentiality policy;
- reminding the employee not to disclose any trade secrets or confidential information from prior positions;
- training the employee on trade secret policies;
- requiring a new employee to sign a contract preventing them from disclosing trade secrets and/or confidential information from a previous employer; and
- assessing whether the new employee is subject to a non-compete agreement.

5. TRADE SECRET LITIGATION

5.1 Prerequisites to Filing a Lawsuit

There are no procedural prerequisites or requirements for filing a trade secret misappropriation lawsuit, although a lawsuit may be preceded by a cease-and-desist letter or a period of prior communication between the parties. Whether in anticipation of litigation or not, a trade secret owner may find it useful to send notices to former employees that go on to work for the trade secret owner's competitors, reminding the former employee of their confidentiality obligations.

The trade secret owner may likewise benefit from sending a notice to the former employee's new employer, to put the new employer on notice that the former employee had access to the trade secret owner's confidential information and remains under an obligation to maintain its secrecy.

A complaint alleging trade secret misappropriation under the DTSA, like any pleading in federal court, requires the submitting attorney to conduct a reasonable inquiry before filing, and courts may impose sanctions if the pleading is found to have been presented for an improper purpose, such as harassing the defendant, or if the factual contentions are unlikely to have evidentiary support after a reasonable opportunity for further investigation or discovery; see FRCP 11(b). Most state courts impose similar obligations.

5.2 Limitations Period

According to both the DTSA and the UTSA, a misappropriation claim must be brought within three years after the misappropriation was dis-

covered or should reasonably have been discovered. The particular facts that can put a trade secret owner on notice of a trade secret misappropriation claim vary but, generally, a trade secret owner should diligently investigate any objectively reasonable suspicions that its trade secrets have been disclosed improperly or used without consent. Another factor to consider when bringing DTSA claims is the timeline of the misappropriation and use of the trade secrets at issue.

Although there is uncertainty in this area, some courts have found that pre-enactment misappropriation may still be redressed by the DTSA if there are instances of use of the trade secrets occurring after enactment. For example, the DTSA is likely still available if the theft of a trade secret occurred prior to 11 May 2016 but the use or disclosure of the misappropriated trade secret occurred after the effective date of the DTSA. If all of the activity constituting the trade secret misappropriation occurred prior to 11 May 2016, however, the trade secret plaintiff may be limited to bringing claims under the UTSA.

5.3 Initiating a Lawsuit

An owner of a trade secret may file a complaint under either the DTSA or state trade secret laws (most of which conform to the UTSA) in federal or state court. The DTSA's jurisdictional element requires the asserted trade secret to be related to a product or service that is used or intended for use in interstate or foreign commerce.

The DTSA and most forms of the UTSA permit three theories of misappropriation: unconsented use, acquisition, or disclosure of a trade secret by a party who used improper means to acquire the trade secret or who knows or has reason to know that the trade secret was acquired by improper means. New York law more narrowly requires that the defendant uses the trade secret in order for a claim to be established.

Another option is to bring a claim of trade secret misappropriation in the US International Trade Commission (ITC) if products embodying a misappropriated trade secret are imported into the United States. While the ITC cannot award damages for trade secret misappropriation, it does have the authority to exclude imported goods that are produced through the exploitation of misappropriated trade secrets as an "unfair method of competition" or "unfair acts" in violation of the Tariff Act (19 USC Section 1337).

ITC investigations often proceed much faster than district court litigation, and trade secret owners should consider whether the benefit of securing a speedy remedy is offset by the constrained timeline in which to develop the evidence needed to support a finding of misappropriation.

5.4 Jurisdiction of the Courts

A trade secret claim may be initiated in federal court under the DTSA if the court is capable of exercising personal jurisdiction over the defendant in the chosen forum, and if the venue is proper. State law claims may be appended to a DTSA claim, or brought on their own in federal court if there is complete diversity of citizenship between parties (ie, no plaintiff shares the citizenship of any defendant and vice versa) and the plaintiff alleges an amount in controversy of more than USD75,000. State law claims may also be brought in the state in which the claims arose.

The choice of forum (either the state court or federal courts within the forum state) available to a plaintiff will depend on factors such as where the defendant lives, is incorporated or has significant business operations, and where the alleged acts of misappropriation occurred. A trade secret owner faced with acts of misappropriation by a foreign corporation may need either to sue a local subsidiary of the foreign corpora-

tion or to be prepared to show that the foreign corporation has sufficient minimum contacts with the chosen forum state, such as transacting business within the state or competing with the trade secret owner in that state.

Prospective trade secret claimants should also analyse any relevant contracts in order to be aware of any agreements related to specific jurisdictional requirements or admissions or the applicability of any arbitration clauses.

5.5 Initial Pleading Standards

In federal courts, the pleading standards for trade secret misappropriation claims are governed by the traditional notice pleading requirements of the Federal Rules of Civil Procedure: the plaintiff need only set forth sufficient facts to state a claim for relief that is plausible on its face. There is no heightened particularity standard as is required for fraud or mistake claims.

Thus, a trade secret plaintiff will likely be able to survive a motion to dismiss in federal court as long as it alleges sufficient facts to plausibly demonstrate that the information misappropriated constitutes a protectable trade secret, the information derives value from being secret, and the owner took reasonable measures to keep it secret.

Some state court civil procedure codes – most notably, California's – impose a heightened particularity standard that requires the plaintiff to identify the asserted trade secret with reasonable particularity before proceeding to discovery. Most courts have found that such procedural barriers apply solely in state court, and so, for example, a California trade secret claim brought in federal court would not be subject to any heightened pleading standards.

Although pleading requirements and the timing and manner of discovery for federal trade secret claims under the DTSA are largely uniform across jurisdictions due to the Federal Rules of Civil Procedure, bringing claims in state court may expose a plaintiff to unique strategic challenges in terms of articulating the trade secrets that it believes have been misappropriated.

In jurisdictions such as California where the plaintiff must identify the misappropriated trade secrets with reasonable particularity before the commencement of discovery, a defendant may argue that the plaintiff's identification is insufficiently particular, such that the defendant cannot defend against the allegations of trade secret misappropriation and the court will be unable to determine the appropriate scope of discovery.

In such circumstances, a defendant may be able to extract increasingly specific disclosures that narrow the scope of the trade secrets asserted, all while staying discovery into the trade secret claims as well as other causes of action based on the same factual allegations. In some jurisdictions a plaintiff may be able to proceed well into discovery with a trade secret identification that is more general, but California courts will generally require a narrative description that provides the defendant sufficient detail to investigate how, if at all, the alleged trade secret differs from information that is publicly known or well known within the relevant industry. The degree of particularity required is highly context-specific, and California courts have discretion to require a more exacting level of particularity for more complex technologies.

Parties should therefore be prepared to submit sufficient evidence and, in some cases, declarations by expert witnesses to support their contentions as to the sufficiency of the description of the claimed trade secrets.

Although California's reasonable particularity requirement is not meant to function as a mini-

trial on the merits, a plaintiff who is unable to adequately describe the trade secrets at issue would doubtless encounter difficulties at the summary judgment stage, and therefore the process of obtaining the court's approval to proceed with discovery can provide a useful stress test of the plaintiff's misappropriation theories.

5.6 Seizure Mechanisms

The DTSA provides access to a new ex parte civil seizure provision, which allows a court to order seizure of property in order to prevent the further dissemination of the trade secrets at issue. The movant must demonstrate that extraordinary circumstances justify the seizure, which requires showing – in addition to the elements that ordinarily justify a preliminary injunction or temporary restraining order – that an injunction or other equitable relief would be inadequate to ensure compliance, and if the enjoined party were provided notice it would destroy or render inaccessible the property to be seized.

As part of the merits of the application, the movant must succeed in showing that the information sought to be protected is a trade secret and that the potential subject of the seizure order misappropriated or conspired to misappropriate the trade secret. Although the demanding burden for an ex parte civil seizure under the DTSA suggests this will be an infrequently used tool, the scope of property that may be seized is potentially quite broad compared to civil seizures in other intellectual property enforcement regimes, which are generally limited to the infringing or counterfeit goods themselves.

If the movant succeeds in obtaining an ex parte civil seizure order, the court should hold a hearing within seven days after the order issues. The burden remains on the movant to prove the facts necessary to support the seizure; if the movant fails to meet its burden, the order will be dissolved or modified.

5.7 Obtaining Information and Evidence

In federal court, once litigation has commenced, the parties can obtain discovery from each other pursuant to the Federal Rules of Civil Procedure. Each state also has its own rules governing discovery. Discovery methods in both state and federal courts typically include the following:

- interrogatories;
- requests for the production of documents and other evidence;
- requests for admissions; and
- pre-trial depositions under oath, either of individuals or of employees designated to testify on behalf of a corporate entity.

In trade secret litigation where the misappropriation of competitively sensitive documents or source code is at issue, the trade secret owner may wish to seek forensic inspection of devices in the possession of the alleged misappropriator or its employees.

5.8 Maintaining Secrecy While Litigating

Plaintiffs will need to strike a careful balance between under- and over-disclosure regarding the claimed trade secrets. For example, a plaintiff must provide sufficient detail in its complaint to survive a motion to dismiss (see **5.5 Initial Pleading Standards**), but must also avoid disclosing trade secret information in a publicly filed complaint or other pleading. Prior to exchanging any sensitive business, technical or financial information, the parties should stipulate to a protective order that limits disclosure of such information to the attorneys of record for each party as well as certain designated persons (such as senior in-house counsel or expert witnesses).

More stringent requirements may be sought for particularly sensitive material, such as software source code or technical schematics. In all circumstances, the trade secret owner should take care to properly designate the material it deems

a trade secret, and any descriptions thereof, under the appropriate degree of confidentiality provided by the stipulated protective order. Litigants should pay careful attention to jurisdiction and judge-specific rules for filing materials under seal or with redactions.

5.9 Defending against Allegations of Misappropriation

Defendants accused of trade secret misappropriation have several strategies available to them, depending on the facts of the case. One particularly strong defence is independent development: if the defendant can show that it relied entirely on its own information or publicly available information in developing the relevant product or service, the plaintiff will not be able to establish that any use of its trade secrets occurred. An advantage of this defence is that the plaintiff's definition of its own trade secrets is largely immaterial to developing the defence, giving the defendant greater control over the themes and evidence it chooses to present at trial.

In relation, defendants should investigate whether information claimed as part of the plaintiff's trade secret is already in the public domain, as such information is by definition not protectable as a trade secret. Another possible defence is to show that the plaintiff did not take proper precautions to maintain the confidentiality of the information alleged to be a trade secret. For example, if the information was shared without requiring entry into a non-disclosure agreement, or if the information was widely dispersed without adequate technological controls to keep it secure, the information may not be entitled to trade secret protection.

5.10 Dispositive Motions

Parties may bring dispositive motions at several stages of the litigation, including prior to trial and, in some cases, prior to engaging in discovery. Defendants may wish to bring a motion to dismiss at the outset of the litigation if the plaintiff has not met the initial pleading standards (see **5.5 Initial Pleading Standards**). If the defect in the plaintiff's complaint is simply that the trade secrets have not been identified with the requisite degree of particularity, courts often permit the plaintiff to amend its complaint or provide a confidential statement identifying its trade secrets in greater detail.

After discovery has concluded, parties often move for summary judgment on claims or issues for which there are no material facts in dispute and the movant would be entitled to judgment as a matter of law. Motion practice at this stage has the effect of simplifying the issues for trial, if not avoiding trial altogether. If the case proceeds to trial, a party may seek judgment as a matter of law after the opposing party has presented its case at trial if the opposing party has failed to introduce evidence supporting a reasonable conclusion in its favour.

5.11 Cost of Litigation

Litigation costs arise at every stage of the case, from the filing of a complaint to discovery to trial. Litigation costs will vary depending on the types and complexity of the trade secrets at issue, the amount and types of discovery required, the number of witnesses to depose or to prepare for depositions, the number of expert witnesses involved, and many other factors.

Costs tend to be higher in trade secret cases than in other intellectual property cases. For example, a recent survey by the American Intellectual Property Law Association discovered that the median cost of trade secret cases with USD10 million to USD25 million at risk is USD4.1 million, compared to USD3.5 million for similarly valuable pharmaceutical cases.

For trade secret cases with over USD25 million at risk, median litigation costs rise to USD7.5 million. A trade secret plaintiff (or potential plaintiff) with compelling facts may wish to consider available sources of third-party contingent litigation financing.

The litigation finance industry has seen substantial growth in recent years, although this approach is not without some controversy. A party considering third-party contingent litigation financing should also stay apprised of the fast-moving legal landscape regarding the discovery and disclosure of third-party financing arrangements.

6. TRIAL

6.1 Bench or Jury Trial

Although trade secret plaintiffs seeking damages are generally entitled to a jury trial, they should consider the likely composition of the jury pool and the pros and cons of jury trials before demanding a jury trial. Trade secret cases involving exceptionally complex technologies within narrow industries pose the risk of confusing a jury, so plaintiffs should take into account the range of educational backgrounds and industry affiliations of potential jurors.

In cases involving alleged misappropriation by a former employee, jurors may be more sympathetic to typical defensive themes such as the employee's right to take their expertise to a new job without fear of reprisal. Nevertheless, due to the comparatively higher damages awarded by juries, jury trials will often be preferable to bench trials for most trade secret plaintiffs.

6.2 Trial Process

After the close of discovery and the resolution of any dispositive motions, the case will proceed to trial on any remaining claims or issues. Depending on the jurisdiction and individual practices of the court or judge, a trial may be scheduled near the outset of the litigation at a case management conference, or it may be scheduled on relatively short notice after it is clear to the judge that the case is "trial-ready".

As in any other civil litigation, the party with the burden of proof is given the opportunity to present its case, which may consist of an opening statement, testimony of fact and expert witnesses, and a closing argument. The opposing party will generally have the opportunity to cross-examine each witness after they provide direct testimony. After the party with the burden of proof rests, the opposing party presents its case, consisting largely of the same elements. The case is then submitted to the jury to render a verdict, or to the judge for an opinion and order in a bench trial.

Trial length can vary considerably. While courts tend to allot a minimum of three to five days for trade secret trials, an exceptionally complex trial involving numerous fact and expert witnesses or novel technologies could stretch to three months or more.

6.3 Use of Expert Witnesses

Expert testimony is often important in trade secret misappropriation cases as a means of explaining complex issues to the finder of fact, especially where the trade secrets at issue are technical in nature. Experts may be used for a variety of purposes, including to support or rebut the contentions that a party possesses protectable trade secrets and takes reasonable steps to protect them, and that the defendant misappropriated and used the trade secrets in its own products or services.

Computer forensic experts may also provide valuable opinions and testimony related to the access and misappropriation of trade secrets

and computer systems and networks. As in other types of litigation, economic and financial experts to support damages remedies may be useful to estimate or forecast liability for the misappropriation of the trade secret(s) under any number of potential damages theories.

7. REMEDIES

7.1 Preliminary Injunctive Relief

To obtain a preliminary injunction, a trade secret plaintiff generally must establish that:

- it is likely to succeed on the merits of its trade secret misappropriation claim;
- it is likely to suffer irreparable harm in the absence of preliminary relief;
- the balance of equities tips in its favour; and
- an injunction is in the public interest.

To show irreparable harm, a plaintiff will need to demonstrate that monetary damages would be inadequate, which is more likely where the trade secret owner previously had market exclusivity and therefore the misappropriation results in reduced market share, lost customers, lost business opportunities and/or price erosion.

Whereas lost sales alone may be insufficient to establish irreparable harm if such losses can readily be calculated, damage to the trade secret owner's goodwill, reputation or other intangible factors, and any other harms that result in a decrease in revenue available for employee attraction and retention, or for research and development activities on which the business relies for continued profitability, may be relevant to establishing the inadequacy of monetary damages.

In some jurisdictions, a party moving for a preliminary injunction must also show that there is a risk of further dissemination of its trade secrets beyond the misappropriation already complained of. In addition, an unreasonable delay in bringing a trade secret misappropriation claim or the motion for a preliminary injunction will weigh against granting the injunction.

7.2 Measures of Damages

Damages available to a trade secret plaintiff will vary depending on the federal and state claims asserted and the theories of recovery. Under the DTSA, damages for trade secret misappropriation can be calculated in at least three ways:

- actual loss caused by the misappropriation;
- unjust enrichment caused by the misappropriation, which may be sought in addition to actual loss to the extent that damages calculations do not overlap, or in lieu of either actual loss or unjust enrichment; and
- a reasonable royalty.

Damages under the UTSA similarly include actual loss in addition to unjust enrichment not taken into account in computing actual loss, but a reasonable royalty is only available under exceptional circumstances.

In some situations, lost profits may be shown by directly establishing that certain sales expected by the plaintiff were lost to the defendant as a result of trade secret misappropriation. More commonly, however, a plaintiff will argue that the defendant's entire revenue from sales of products or services based on the misappropriated trade secret constitutes the damages base, at which point the burden shifts to the defendant to demonstrate which costs should be deducted to arrive at the net profit.

In addition, a plaintiff may need to consider pursuing other damages theories, such as the expenses the plaintiff incurred in developing its trade secrets, the reduction in market share and/or erosion in price attributable to the defend-

ant's entry into the market, disgorgement of the defendant's profits, or the value of the defendant's avoided research and development costs.

In cases where the defendant has not yet released (or has only recently begun selling) a product or service based on the misappropriated trade secret, expert analysis and testimony may be invaluable in forecasting future lost profits or unjust enrichment. As an example, a technical expert may be able to offer an opinion concerning the length of the "head start" a trade secret misappropriator obtained as a result of using the plaintiff's trade secret, which a damages expert can take into account when forecasting damages. Defendants should prepare their expert witnesses to offer opinions rebutting the damages calculations offered by the plaintiff.

If other measures of damages are inadequate, the plaintiff may seek a reasonable royalty. This measure is generally seen as a theory of last resort and can result in lower recovery than other measures. As in patent cases, courts have applied the "Georgia-Pacific" factors in order to reach a reasonable estimate of a royalty rate to which the parties would agree in a hypothetical negotiation.

Punitive damages may be available under the DTSA and for most state law claims if the defendant's conduct was gross, wilful or malicious. There are certain exceptions involving whistle-blower immunity for which punitive damages against a current or former employee may be unavailable.

7.3 Permanent Injunction

Under the DTSA, a court may issue an injunction that places some limits on an employee's subsequent employment in order to protect the plaintiff's trade secrets, but the scope of the injunction may not be so broad as to prevent an employee from entering into any employment relationship or conflict with applicable state laws prohibiting restraints on the lawful practice of a profession. Moreover, the trade secret owner must base its request for a permanent injunction on evidence of threatened misappropriation and not merely on the information that the employee knows.

As a result, a trade secret owner may have limited recourse to injunctions in states such as California or Louisiana that disfavour non-competition agreements or that have rejected the inevitable disclosure doctrine. In practice, courts have issued injunctions restricting former employees in possession of sales and marketing-related trade secrets from soliciting former clients or bidding on certain contracts.

Where the misappropriated trade secret has been used to develop a competing product or service, the trade secret owner should consider seeking a permanent injunction requiring the misappropriator to cease offering or recall the product or service. In order to succeed, the trade secret owner will likely need to show irreparable injury by putting forward evidence that other remedies, such as monetary damages, would be inadequate to compensate for the misappropriation. A finding of irreparable injury can be supported by harms that are impossible or difficult to quantify, such as a loss of good will.

7.4 Attorneys' Fees

Under the DTSA and most state trade secret laws, reasonable attorneys' fees may be awarded to the prevailing party on a showing of wilful and malicious misappropriation by the defendant or a bad-faith claim of misappropriation by the plaintiff.

7.5 Costs

Under the DTSA and most state trade secret laws, costs may be awarded to the prevailing party on a showing of wilful and malicious mis-

appropriation by the defendant or a bad-faith claim of misappropriation by the plaintiff.

8. APPEAL

8.1 Appellate Procedure

A federal district court decision (including final judgments and orders on dispositive motions) may be appealed as of right to the circuit court of appeals in the circuit in which the case was initially decided. Appeals from final ITC actions may be taken only to the US Court of Appeals for the Federal Circuit. If the ITC issues an exclusion order, an appeal cannot be filed until after a 60-day review period, during which the United States President may veto the exclusion order. If the ITC does not issue an exclusion order, any adversely affected party may immediately file a notice of appeal.

It is not unusual for the federal appellate process to take anywhere from several months to several years. The process involves substantive briefing by both parties, which itself can take several months. Circuit court appeals often involve oral arguments before a panel of appellate judges. Circuit courts have discretion in scheduling the oral argument date for an appeal. Once the briefing and oral argument have been completed, the court has discretion in the timing of issuing a decision.

A party that is dissatisfied with the panel's decision may seek a rehearing of the proceeding en banc – ie, a rehearing before all (or a substantial number) of the judges of the circuit court. En banc hearings are typically reserved for novel questions of law or issues of exceptional importance, and are more likely to be granted if the panel decision conflicts with those of other panels or circuits.

A decision of a regional circuit court of appeals or of the Federal Circuit may be appealed by filing a petition for certiorari with the United States Supreme Court, which has broad discretion to hear appeals and generally grants fewer than one hundred out of the several thousands it receives annually.

The civil court systems in each of the states consist of trial courts, intermediate courts of appeal, and a highest court of appeal, which is often, but not always, called the state supreme court. As with the federal judicial system, the intermediate court of appeal's decision may be appealed to the highest court of the state, which has discretion to hear the case. Even if a case begins in state court, an out-of-state defendant may be able to "remove" the case to federal court at the outset if federal jurisdictional requirements are met.

8.2 Factual or Legal Review

Issues on appeal are limited to those properly raised in the district court proceedings – claims, defences and/or arguments may be deemed "waived" and the appeals court will ordinarily refuse to consider them. A court of appeals defers to the district court's factual findings unless they are clearly erroneous, which only requires the district court's account of the evidence to be plausible in light of the record. Conclusions of law are reviewed de novo, which means the appellate court reviews the issues with no deference to the district court's legal analysis. This also enables a court of appeals to uphold or overturn a district court's ruling on alternative legal grounds that were not considered by the district court.

9. CRIMINAL OFFENCES

9.1 Prosecution Process, Penalties and Defences

Civil trade secret misappropriation claims often involve conduct that overlaps not only with the federal EEA but also with state and federal statutes related to criminal mail and wire fraud, digital theft or unauthorised access to protected computers. Trade secret owners should consider whether to reach out to the Department of Justice or state investigative agencies in cases of suspected or known misappropriation, especially since the trade secret owner is likely to have conducted a thorough investigation and will have access to unique information regarding its own trade secrets that would not be apparent to government authorities initiating their own investigation.

The involvement of state or federal authorities may offer the benefit of bringing additional resources to bear, although there may be some loss of control over the investigation and the timeline of the case. For a defendant in a civil trade secret misappropriation action, it is important to evaluate the likelihood that a parallel criminal case could be initiated, which may affect the strategy for responding to discovery requests and could increase the potential for self-incrimination during depositions.

10. ALTERNATIVE DISPUTE RESOLUTION

10.1 Dispute Resolution Mechanisms

The parties may settle their civil dispute at any time. Depending on the jurisdiction and the judge's individual practices, a court may require the parties to engage in one or more settlement conferences or other alternative dispute resolution (ADR) procedures prior to trial, or may offer voluntary procedures for accessing ADR resources. The parties may also voluntarily choose to engage in mediation, a non-binding ADR process whereby the parties and their attorneys meet with a neutral third party who is trained to facilitate settlement discussions.

A mediator typically helps the parties reach their own voluntary settlement by assessing the strengths of the parties' positions and identifying potential areas of agreement or disagreement. Even if the parties are not likely to reach a complete settlement, the ADR process may assist by "stress testing" a party's case and identifying any potential areas of weakness before proceeding to trial.

ADR can sometimes offer advantages over traditional litigation. For example, parties frequently resolve disputes more quickly through ADR than they would in court, which can also save costs. The parties are largely in control of the ADR schedule and therefore have more flexibility to tailor the process to their unique needs. Many types of ADR are confidential, which can be appealing to parties who do not want the details of their dispute made public through court records.

The most common forms of ADR used in trade secret disputes are mediation and arbitration. Whereas mediation is non-binding, in arbitration a neutral third party known as an "arbitrator" will typically issue a written decision resolving the case on the merits. Parties may agree to arbitrate after a conflict arises, although occasionally the parties will have agreed in a prior contract (such as a licensing, subcontracting or joint venture agreement) to resolve future disputes through arbitration.

However, if the parties have not entered into any contract containing an arbitration clause, courts are unlikely to mandate arbitration between litigants on the basis of arbitration clauses found in

contracts with a party's employees, even if those employees may have been involved in acts of misappropriation.

In an arbitration proceeding, the parties present evidence and arguments supporting their positions to the arbitrator(s). The applicable procedural and evidentiary rules are usually determined by the parties' arbitration agreement. Arbitration is generally less rigid than litigation but more formal than mediation. Depending on the type of arbitration, the arbitrator's decision can be either binding or non-binding.

In non-binding arbitration, the parties are usually bound by the decision unless one of them rejects it and requests a trial. In binding arbitration, the parties agree that the arbitrator's decision will be the final resolution of the case, and the parties will generally not have the opportunity to appeal the merits of the dispute.

Kirkland & Ellis LLP is an international law firm with 2,700 attorneys across the United States, Europe and Asia. Kirkland's trade secrets litigation practice includes approximately 75 attorneys with years of experience in representing both plaintiffs and defendants in trade secrets matters in diverse industries. Kirkland's trade secrets attorneys have litigated the broad spectrum of trade secret disputes, ranging from outright theft to violation of various agreements, including employment, R&D, joint development, and technology transfer and know-how agreements. Significant victories have been won for clients in these matters in UK courts, US federal and state courts, and in arbitrations, and the firm has worked collaboratively with law enforcement agencies to protect clients' intellectual property. The practice's success is grounded in extensive jury and bench trial experience, and it has a sophisticated appellate practice to protect clients' successes at the trial level.

AUTHORS

Claudia Ray is a partner in Kirkland's intellectual property practice group. She represents clients in litigation, arbitration and administrative proceedings involving trade secret, copyright, trade mark, internet and contact/licensing issues across a wide range of industries. Her trade secret practice includes litigation and counselling relating to software, technology, financial services and consumer products. Claudia also serves on the Intellectual Property and Technology Advisory Committee of the American Arbitration Association and the US Amicus Subcommittee of the International Trademark Association, and is the chair of the Copyright Law Committee of the Association of the Bar of the City of New York.

Joseph Loy is a partner in Kirkland's intellectual property practice group. His practice focuses on trade secret and patent infringement disputes before federal trial and appellate courts nationwide. His trade secret work includes both offensive and defensive litigation and corporate counselling. Joe has represented clients in cases involving a wide range of industries, including medical devices, pharmaceuticals, biotechnology, wireless telecommunications, petrochemicals, cruise ships, digital photography, smartphones and computer software. He is a frequent commentator on trade secret issues before intellectual property Bar associations and law school communities.

Patrick Arnett is an associate in Kirkland's intellectual property practice group. His practice focuses on trade secret and patent litigation in a variety of technical fields, including software, cloud computing, consumer electronics and semiconductor technology.

Kyle Friedland is an associate in Kirkland's intellectual property practice, whose practice focuses on trade secret and patent litigation.

Kirkland & Ellis LLP

601 Lexington Avenue
New York
NY 10022

Tel: 212 446 4800
Fax: 212 446 4900
Email: claudia.ray@kirkland.com
Web: www.kirkland.com

KIRKLAND & ELLIS

Trends and Developments

Contributed by:
Steven Blonder
Much Shelist, P.C. see p.290

Trade Secret Litigation Continues to Rise

In the face of a pandemic and with employees working remotely, the protection of trade secrets has taken on increased importance. Additionally, with communication taking place largely in a virtual world across a variety of new technological mediums, new challenges have emerged for companies that are endeavouring to protect their confidential competitive information. As workforces with access to confidential and proprietary information remain increasingly remote, the necessity for businesses to protect their confidential information is magnified.

Trade secrets are often core to a business' financial viability, if not its success, and rank among a company's most valuable assets. Well-known examples include the formula for Coca-Cola, Google's search algorithm and McDonald's secret sauce recipe, none of which enjoys patent, copyright or trade mark protection; rather, each is a protected trade secret. A trade secret enjoys significant advantages over the other forms of IP protections in that disclosure is not required and the "secret" can be protected forever. While many of the big IP litigation battles historically involved patent challenges, that is no longer the case today. Companies such as Facebook, Amazon, Peloton and Motorola (to name a few) are or have been involved in costly trade secret litigation.

Notwithstanding the pandemic, claims alleging a misappropriation of trade secrets have exacerbated in recent years, with the past year being no exception. Simply put, 2020 brought robust litigation in the trade secret space across a wide swath of industries, ranging from cannabis to fashion and retail, e-commerce and consumer products.

While trade secret claims were historically brought in state courts, since the 2016 passage of the federal Defend Trade Secrets Act (DTSA), which created a federal cause of action for trade secret theft, claims are now routinely brought in the federal courts. Over the past two years, nearly 2,000 new cases alleging trade secret misappropriation have been filed in federal court.

On the recovery side, successful plaintiffs in trade secret cases have continued to see courts award substantial damage awards. For example, Motorola obtained an award of more than USD764 million (which was later reduced by USD200 million) and a case in New York saw an award of more than USD850 million. If nothing else, 2020 proved that the damages that can and are being awarded for trade secret claims remain staggering.

So what trends are likely to define trade secret litigation in 2021? What follows are a few takeaways.

New technologies present new challenges to trade secret protection

Since early 2020, many businesses have transitioned to a remote working environment and have gone virtual. Zoom and other videoconferencing technologies have emerged as the new primary vehicle for communications both internally at companies and in their external relations with third parties. This shift has significant implications for how companies protect their trade secret information.

In a recent case, the Delaware Chancery Court ruled that a company failed to take reasonable steps to protect its trade secrets because it failed to implement appropriate privacy measures on its Zoom calls. While Zoom calls may continue as a main form of communication, if parties are going to exchange confidential information during those calls, to maintain protection they should adopt clear processes and procedures (and make sure they are followed), such as restricting access to the Zoom call information, changing the Zoom meeting code between meetings, requiring participants to use a password to enter, using a waiting room to screen participants, and having participants sign a non-disclosure agreement. These are just a few examples of the steps to be taken.

The kinds of trade secrets continue to expand

The definition of a trade secret can be quite broad. Simply put, a trade secret is defined as information used in a company's business that is not known by nor readily accessible to competitors, that is protected from disclosure through reasonable efforts to maintain its secrecy, and that either provides a competitive advantage in the marketplace or has commercial value. Many trade secret claims revolve around computer codes, algorithms and customer lists. However, recent cases span the gamut from OSHA data summarising warehouse worker illnesses and injuries to the manufacture of Botox, advertising plans for exercise equipment, proprietary information about cannabis platforms supporting a telehealth service, methods for bleaching hair and repairing hair damage, and the process of adding aromas as a perceived taste-enhancer to beverage bottles. The bottom line is that any type of information that meets the criteria of a trade secret can be protected.

Statutes of limitation will continue to be important

The federal statute provides for a three-year statute of limitation for a trade secret claim. Various states allow four or even five years within which a claim must be brought. However, the crucial inquiry relates to when the statute of limitation begins to run.

The law says that a claim arises when the injured party has actual notice of the potential misappropriation of its trade secret or when that party should have discovered the misappropriation through the exercise of reasonable diligence. Put another way, when would a reasonable person investigate whether his or her trade secrets had been stolen?

At least one court has held that the statute of limitations may begin to run when a company warns a former employee that the disclosing of its trade secrets to a new employer would constitute a crime. Other courts have noted that, in the context of a failed business transaction, inquiry notice exists when one party fails to return the other's confidential information according to the terms of a non-disclosure agreement signed by the parties. In many cases, the question of when a statute of limitation begins to run will continue to be a major source of dispute in 2021.

The question as to when the trade secret theft occurred is important for other reasons as well. For example, one change brought by the 2016 federal legislation was that trade secret misappropriation can constitute a predicate act under the Racketeer Influenced and Corrupt Organizations (RICO) statute. To qualify, a plaintiff must show that the trade secret theft occurred after 11 May 2016 – the date that the DTSA was enacted.

Where exactly did the theft occur?

The DTSA was enacted as part of the response to the theft of trade secrets by Chinese companies

and other foreign actors. Moreover, in the USA, courts have recently held that a civil action under the DTSA can arise from wrongful conduct occurring completely outside the USA. The only catch is that the wrongful activities have some nexus with activities that took place within the USA.

The US International Trade Commission has recently gotten involved in policing trade secret misappropriation that has taken place outside of the United States. The agency can enter an order excluding products from being imported into the United States, with US Customs enforcing the order. For example, the ITC issued an exclusion order and a cease and desist order for trade secret misappropriation related to methods of manufacturing Botox. The two parties involved were both Korean-based entities, and the alleged misappropriation took place outside of the United States.

Steps taken to maintain confidentiality of information can have implications for trade secret litigation years later

The DTSA and various state statutes require a trade secret owner to take "reasonable measures" to protect its trade secret information. What constitutes "reasonable measures" is not defined, and the actions that a company takes to protect its trade secret information upfront can impact the likelihood of a successful trade secret claim years later.

Coca-Cola is widely known for the efforts it undertakes to maintain the secrecy of its formula for its popular soft drink, but this is not the benchmark for what is required.

Numerous courts have dismissed trade secret claims based on the failure of the plaintiff to enact "reasonable measures" to protect its trade secrets. In some of these cases, the party seeking trade secret protection had not adequately marked the information as confidential. Other indicia of reasonable measures may include storing the information in a password-protected, limited-access server, having employees sign written acknowledgements of their obligation to keep sensitive business information confidential, and telling employees that the information was confidential.

In today's world where companies use cloud applications allowing employees to work more flexibly, the inquiry becomes more difficult. The ease with which data can be transferred in a cloud-centric world significantly changes a company's ability to maintain the secrecy of its information. For example, when an employee downloads information from the cloud to a personal device outside of the company's control, the company may lose track of its data and not be able to maintain the secrecy or confidentiality that it thought that it had.

Whether or not a company has undertaken "reasonable measures" to protect its confidential information is necessarily a fact-based inquiry; in all likelihood, this will continue to be a hotly litigated issue in trade secret litigation in 2021.

Trade secret claims involve large potential actual and punitive damages

In addition to increases in the number of cases being filed, the recoveries in trade secret claims for successful plaintiffs continue to be significant. This is often true whether the recovery results from settlement or comes in the form of a verdict after a full-blown trial. Reported decisions in state and federal courts evidence damage awards of up to eight or nine figures. Sometimes these include punitive damages, while at other times they do not.

For example, juries have awarded hundreds of millions of dollars in two recent cases. In the first, a jury awarded USD764 million in damages, which included USD418 million for punitive

damages. Although the total award was recently reduced to USD543 million, the amount is still significant. In another case, a New York jury awarded a company USD854 million, including USD570 million for punitive damages. Other reported damage awards are in the tens of millions of dollars.

Litigants in trade secret cases have flexibility in fashioning their damage theories. This is exemplified by a recent appellate court decision affirming an arbitration award containing "head start" damages. These damages represented the benefit to the defendant for the development and operational head start that it received through the misuse of the information. The "head start" damages were a means to quantify the benefit of the increase in value in the defendant's business resulting from its being several years ahead of where it would have been but for the wrongful conduct. These damages were distinct from the saved development costs, which provided an additional benefit to the defendant.

Regardless of the theory of damages, the bottom line is that – assuming a litigant can prove that misappropriation occurred – recoveries for plaintiffs in trade secret cases continue to be large, with juries showing little mercy. For companies, taking precautions to ensure that new employees do not bring with them trade secrets owned by their former employer can prevent costly litigation down the road.

Other trends to watch

A couple of other trends are worth watching. A common defence raised in trade secret cases is "unclean hands". In asserting this defence, a defendant seeks to shift the inquiry away from the alleged misappropriation toward the complaining party's conduct in order to invalidate a claim. For example, employees often access their social media accounts from work computers or other devices. Employers routinely monitor such access but, depending on how employers monitor this information and what they do with it, the facts can give rise to an "unclean hands" affirmative defence. As always, in investigating potential trade secret misappropriation, a company needs to consider the implications of its actions on any potential lawsuit.

Another issue is the interplay between patents and trade secrets. At least one recent case held that a plaintiff lacked standing to pursue trade secret claims because the alleged trade secrets were "extinguished" by the publication of patent applications involving the same technology. Other recent cases address the question of whether ownership or inventorship of a patent has an impact on the ownership of a trade secret.

At all levels, there is a growing legislative focus on non-compete agreements. President Biden has announced his intention to eliminate non-compete and no-poaching agreements that restrict employees from freely moving between employers. Soon thereafter, Washington DC enacted a law that will serve as a near-total ban on the use of non-competes in Washington DC. A number of states are contemplating similar statutes precluding the enforceability of employee non-compete agreements and non-solicitation agreements. As a result, trade secret claims are likely to increase as employee mobility remains high as companies attempt to protect their assets.

Trade secrets remain essential to the competitive success and financial viability of many businesses. Claims alleging trade secret misappropriation are likely to continue to rise. Companies would be well advised to examine their policies and procedures regarding their confidential information and the protections in place to maintain that information in confidence. Looking at these issues on the front end can lead to increased success on the back end if a claim needs to be pursued.

Contributed by: *Steven Blonder,* ***Much Shelist, P.C.***

Much Shelist, P.C. is a firm of approximately 100 attorneys, who focus on business counselling, transactional law and litigation for businesses of all sizes. The firm has offices in Chicago, Illinois and Newport Beach, California. Clients include financial institutions, private equity groups, public and private companies with a global presence, middle-market businesses, families and high net worth individuals. The attorneys help clients identify and correct potential holes in their trade secrets protection strategies; this includes audits of existing trade secrets and intellectual property as well as non-compete, non-disclosure and confidentiality agreements. The team also reviews licensing agreements, database and other electronic information protection systems, and other policies and employee training practices. Following this analysis, it recommends strategies designed to shore up weak or non-existent firewalls and to negotiate more effective agreements with business partners and allies.

AUTHOR

Steven Blonder is a member of Much's Management Committee, and a valued legal and business counsellor who focuses on complex business litigation. He has argued successfully before the federal and state appellate courts as well as the Illinois Supreme Court. Steve has a record of consistent success in motion and trial practice (both jury and non-jury) in state and federal courts and in arbitration. His clients range from Fortune 500 companies to government entities to small businesses and entrepreneurs in a variety of industries, including gaming, food and beverage, financial services and real estate.

Much Shelist, P.C.

191 North Wacker Drive
Suite 1800
Chicago
Illinois
USA
60606

Tel: +1 312 521 2000
Fax: +1 312 521 2100
Email: info@muchlaw.com
Web: www.muchlaw.com