Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Trade Secrets 2024

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

Contributing Editors
Claudia Ray and Joseph Loy
Kirkland & Ellis LLP

Chambers

Global Practice Guides

Trade Secrets

Contributing Editors

Claudia Ray and Joseph Loy

Kirkland & Ellis LLP

2024

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
Content Management Director Claire Oxborrow
Content Manager Jonathan Mendelowitz
Senior Content Reviewer Sally McGonigal, Ethne Withers
Content Reviewers Vivienne Button, Lawrence Garrett, Sean Marshall, Marianne Page, Heather Palomino, Deborah Sinclair, Stephen Dinkeldein and Adrian Ciechacki
Content Coordination Manager Nancy Laidler
Senior Content Coordinator Carla Cagnina
Content Coordinator Hannah McDowell
Head of Production Jasper John
Production Coordinator Genevieve Sibayan

Published by
Chambers and Partners
165 Fleet Street
London
EC4A 2AE
Tel +44 20 7606 8844
Fax +44 20 7831 5662
Web www.chambers.com

CONTENTS

INTRODUCTION

Contributed by: Claudia Ray, Joseph Loy, Miriam Kontoh and Andrew (Keum Yong) Lee, **Kirkland & Ellis**

Kirkland & Ellis is an international law firm with approximately 3,500 attorneys across the USA, Europe and Asia. Kirkland's trade secrets litigation practice includes approximately 85 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 secrets 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 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' IP. The practice's success is grounded in extensive jury and bench trial experience, and a sophisticated appellate practice to protect clients' successes at the trial level.

Contributing Editors

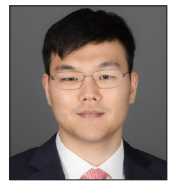
Claudia Ray is a partner in Kirkland's intellectual property practice group. She represents clients in litigation, arbitration and administrative proceedings involving trade secret, copyright, trade mark, internet and contact/licensing issues across a wide range of industries. Her trade secret practice 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 Bulletins Committee 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 autonomous vehicles, biotechnology, computer hardware and software, cruise ships, digital photography, exercise equipment, mattresses, medical devices, oil drilling, petrochemicals, pharmaceuticals, robotics, smart phones and wireless communications. He is a frequent commentator on trade secret issues before intellectual property Bar associations and law school communities.

INTRODUCTION

Contributed by: Claudia Ray, Joseph Loy, Miriam Kontoh and Andrew (Keum Yong) Lee, **Kirkland & Ellis**

Miriam Kontoh is an associate in the New York office of Kirkland. Miriam's practice focuses on litigation and counselling in the fields of copyright, trade mark, internet/social media, right of publicity, art, trade secret and advertising law. She represents and advises clients in a range of industries, including entertainment, social media, film and technology.



Andrew (Keum Yong) Lee is an associate in Kirkland's intellectual property practice group, whose practice focuses on patent litigation.

Kirkland & Ellis LLP

601 Lexington Avenue
New York
NY 10022
USA

Tel: +1 212 446 4800
Fax: +1 212 446 4900
Email: claudia.ray@kirkland.com
Web: www.kirkland.com

KIRKLAND & ELLIS

INTRODUCTION

Contributed by: Claudia Ray, Joseph Loy, Miriam Kontoh and Andrew (Keum Yong) Lee, **Kirkland & Ellis**

Global Overview

As businesses around the world evaluate their options for protecting valuable intellectual property in the context of today's dynamic technological environment and 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 USA 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 one, where the most rapidly growing sectors offer software and services, trade secret laws are more relevant than ever.

Artificial Intelligence in Full Force

Generative artificial intelligence (AI) is here to stay. Various industries have begun using large language models (LLMs) to analyse big data, create work product, and even innovate by developing novel ideas or inventions.

AI applications and LLMs raise several issues for trade secret protection. First, they may capture and store information that may be used to train and enhance the AI's ability to generate results. If one were to input a trade secret into an AI application or LLM prompt, the trade secret could be at risk of unintended exposure to the company behind the AI application depending on the terms of the application's end-user licence agreement. Second, the trade secret could be used as a training input for other problems or prompts, resulting in potential exposure to other end users of the AI application. Third, trade secrets stored by the AI application may be at risk of exposure from security breaches targeting the companies behind the AI application. Each of these issues will push trade secret owners to implement new ways to safeguard their trade secrets, such as updating employment agreements and training and carefully negotiating with companies behind AI applications to limit the use or accessibility of trade secret inputs.

Shifts in Employment Practices

Chambers Trade Secrets Global Practice Guide 2024 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 safeguard 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, shifts to hybrid and/or fully remote workplaces, even as many sectors make a push to return to traditional office-based employment, require balancing agility and innovation with appropriate confidentiality controls.

The increased focus on remote work underscores the need to create sophisticated confidentiality measures to protect trade secrets without impairing the ready interchange of ideas and information in collaborative work environments that may be necessary to promote the

INTRODUCTION

Contributed by: Claudia Ray, Joseph Loy, Miriam Kontoh and Andrew (Keum Yong) Lee, **Kirkland & Ellis**

very innovation that generates trade secrets. Long gone are the days when a company could simply lock its crown jewels in a vault and rest easy knowing its trade secrets were safe.

In addition to the lasting shift away from traditional workplaces, lawmakers from various states and the Federal Trade Commission have demonstrated increasing aversion to non-compete agreements. These changes result in an increasingly mobile workforce that may choose to pursue new opportunities and leverage experiences from prior companies, causing the risk of misappropriation to grow. Employees may feel incentivised to use knowledge and insight gained at prior employers to differentiate themselves in a new job. Without adequate training and precautions, the line between acquired skills and acquired confidential information could blur. New employers (whether leanly staffed start-ups or global heavyweights) should implement stringent procedures for insulating themselves from others' confidential information, while former employers must remain vigilant in safeguarding the improper use of their hard-earned property or risk losing it to competitors.

Litigation and ADR

Because disputes over trade secrets arise even when such precautions are taken, chapters in this guide 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 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 USA, 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 Global 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 in 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 USA are just beginning to grapple with issues of liability and damages based on conduct occurring overseas, while 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

Contributed by: Claudia Ray, Joseph Loy, Miriam Kontoh and Andrew (Keum Yong) Lee, **Kirkland & Ellis**

not inadvertently lose global protection for failure to comply with a single foreign law.

Trade secret owners conducting business in the USA should also not forget that the US International Trade Commission (ITC) can conduct investigations and recommend prohibitions against importing articles based on the theft of trade secrets. Although there was 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.

CHINA

Law and Practice

Contributed by:
Chuanhong Long, Ji Liu and Xiao Jin
CCPIT Patent and Trademark Law Office

Contents

CCPIT Patent and Trademark Law Office is the oldest and one of the largest full-service intellectual property law firms in China. The firm has more than 320 patent and trade mark attorneys, among whom more than 100 are qualified as attorneys-at-law. It provides consultation, prosecution, mediation, administrative enforcement and litigation services relating to patents, trade marks, copyrights, domain names, trade secrets, trade dress, unfair competition and other intellectual property-related matters. Headquartered in Beijing, the firm has branch offices in New York, Tokyo, Madrid, Hong Kong, Guangzhou, Shenzhen, Shanghai and Wuhan. The mission of the firm is to render tailored qualified, efficient and reliable services to clients in a cost-effective manner. The clients represent every sector of industry and commerce, ranging from start-up businesses to multinational giants.

Authors

Chuanhong Long is the president of CCPIT Patent and Trademark Law Office, which he joined in 1994, and serves as the vice-president of the Chinese Group of the AIPPI. His practice focuses primarily on prosecution, invalidation, litigation, enforcement and licensing of patents. His technical specialty covers chemistry, chemical engineering, material science, pharmaceuticals and agrochemicals, etc. Chuanhong has also counselled domestic and international clients on other IP-related matters. He was invited as an expert to participate in the formulation of the Outline of National Intellectual Property Strategy (2005 to 2007).

Ji Liu is the director of the CCPIT Patent Litigation Department and has worked as a patent attorney since 2001. He has a Master's degree in Polymer Science and studied IP law at the Cardozo School of Law, and in US and German law firms. Ji has handled dozens of infringement litigations in different trial courts across China, among which was a case selected by Tianjin Municipal High Court as one of the top ten cases of 2018. Before switching to litigation, he handled more than 1,000 patent filings covering various technical fields.

Xiao Jin joined CCPIT Patent and Trademark Law Office in 2008 and is the assistant director of the Patent Litigation Department. He studied IP law at John Marshall Law School in 2012 and at the University of New Hampshire Franklin Pierce School of Law in 2018. Xiao advises his clients on various aspects of patent enforcement, including licensing, infringement and validity opinions. He appears before all levels of court in China and has strong and extensive relationships with clients in various technology sectors, including computers, communications, electrical engineering, automatic control engineering and optical techniques.

CCPIT Patent and Trademark Law Office

10/F, Ocean Plaza
158 Fuxingmennei Street
Beijing
100031
China

Tel: +86 10 6641 2345
Fax: +86 10 6641 5678
Email: mail@ccpit-patent.com.cn
Web: www.ccpit-patent.com.cn

CCPIT PATENT & TRADEMARK LAW OFFICE

1. Legal Framework

1.1 Sources of Legal Protection for Trade Secrets

Unlike patents, trade marks and copyrights, there is no separate Trade Secret Law in China. But instead, a trade secret protection system based on the Anti-Unfair Competition Law, supplemented by the Civil Code (which integrates the former General Principles of the Civil Law and the Contract Law), the Law on Promoting the Transformation of Scientific and Technological Achievements, the Labour Contract Law, the Company Law, the Civil Procedure Law, and the Criminal Law. In the Civil Code passed in May 2020, trade secrets are, for the first time, explicitly classified as a type of intellectual property rights. The types and infringement acts of trade secrets are stipulated in Article 9 of the Anti-Unfair Competition Law. According to this provision:

- obtaining a right-holder's trade secrets by theft, bribery, intimidation, electronic intrusion or other improper means;
- disclosing, using, or allowing others to use a right-holder's trade secrets obtained by the means mentioned in the preceding paragraph;
- disclosing, using or allowing others to use a right-holder's trade secrets in violation of confidentiality obligations or the right-holder's requirements on keeping such trade secrets confidential; and
- obtaining, disclosing, using or allowing any other party to use a right-holder's trade secrets by instigating, tempting or helping any other party to violate the confidentiality obligations or the right-holder's requirements on keeping such trade secrets confidential.

At the same time, according to Article 219 of the Criminal Law, the first three acts are subject to criminal punishment when the circumstances are serious.

1.2 What Is Protectable as a Trade Secret

According to Article 9 of the Anti-Unfair Competition Law, commercial information such as technical and business information not known to the public, have commercial value, and kept confidential by the right-holder are classified as trade secrets and protected.

1.3 Examples of Trade Secrets

According to the relevant judicial interpretation of the Supreme Court:

- structure, raw materials, components, formulas, materials, samples, styles, propagation materials of new plant varieties, processes, methods or steps, algorithms, data, computer programs, and related documents related to technology can constitute the technical information referred to in the fourth paragraph of Article 9 of the Anti-Unfair Competition Law;
- creative, management, sales, finance, plans, samples, bidding materials, customer information, data and other information related to business activities can constitute the business information referred to in paragraph 4 of Article 9 of the Anti-Unfair Competition Law; and
- the customer information referred to in the preceding paragraph includes the customer's name, address, contact information, transaction habits, intentions, content and other information.

1.4 Elements of Trade Secret Protection

According to Article 9 of the Anti-Unfair Competition Law, trade secrets must meet three requirements:

- they must not be known to the public;
- they must have commercial value; and
- appropriate confidentiality measures must have been taken by the right-holder.

1.5 Reasonable Measures

A trade secret right-holder needs to prove that it has taken reasonable confidentiality measures to protect its trade secrets. Whether the right-holder has taken reasonable confidentiality measures shall be determined according to factors such as the nature of the trade secret and its carrier, the commercial value of the trade secret, the identifiability of the confidentiality measures, the reasonability of the confidentiality measures according to the nature of the trade secret, and the right-holder's will to keep the secret.

According to the relevant judicial interpretations, if one of the following circumstances is sufficient to prevent the leakage of trade secrets under normal situations, it shall be determined that the right-holder has taken reasonable confidentiality measures:

- signing a confidentiality agreement or stipulating confidentiality obligations in the contract;
- putting forward confidentiality requirements for employees, former employees, suppliers, customers, visitors, etc, who are accessible to and able to obtain trade secrets, through articles of association, training, rules, regulations, or written notices, etc;
- restricting visitors or conducting separate management for production and business sites such as workshops involving secrets;
- distinguishing and managing trade secrets and their carriers by marking, classifying, isolating, encrypting, sealing up, limiting the scope of persons who can access or obtain them, etc;
- taking measures such as prohibiting or restricting the use, access, storage, reproduction, etc, of computer equipment, electronic equipment, network equipment, storage equipment, software, etc, that can access and obtain trade secrets; and
- requiring resigned employees to register, return, remove and destroy the trade secrets and their carriers that they have accessed or acquired, and continue to undertake the obligation of confidentiality.

1.6 Disclosure to Employees

Employers can sign confidentiality agreements with employees or agree on confidentiality clauses in labour contracts. Even if the employer and employees do not specifically agree on the confidentiality obligation, the employee's obligation to keep the employer's trade secrets confidential is an implied and accompanying obligation.

However, it should be noted that the employee's implied duty of confidentiality with respect to trade secrets cannot be regarded as the employer's taking reasonable confidentiality measures. In a typical case, the Supreme People's Court held that the accompanying obligation to keep secrets derived from the principle of good faith cannot reflect the subjective will of the owner of the trade secret to take confidentiality measures for information and cannot constitute a positive behaviour of confidentiality measures.

1.7 Independent Discovery

According to the relevant judicial interpretations, if the accused infringing information is obtained through self-development or reverse engineer-

ing, it should be determined that it does not constitute trade secret infringement as stipulated in Article 9 of the Anti-Unfair Competition Law. Here, "reverse engineering" refers to disassembling, mapping and analysing products obtained from public channels, through technical means to obtain relevant technical information about the product.

However, if the party concerned has learned of the trade secrets of others by improper means, and then claims that the acquisition is legal on the grounds of reverse engineering, it shall not be supported.

1.8 Computer Software and Technology

In China, the protection of computer software and/or technology is mainly through copyright protection, but software, especially related data, can also be protected through trade secrets. For example, models formed by sorting, processing and analysing data obtained through massive public channels may sometimes not be protected by copyright law because of their low "originality", but such data and models can be protected through trade secrets.

1.9 Duration of Protection for Trade Secrets

In theory, as long as the relevant information meets the three requirements for trade secrets, there is no time limit for its protection. According to relevant judicial interpretations, information publicly disclosed in public publications or other media, or disclosed through public reports, exhibitions, etc, can no longer be regarded as trade secrets due to the loss of confidentiality. Accidental disclosure does not result in loss of confidentiality. Furthermore, controlled disclosure, such as disclosure with a signed NDA, does not result in a loss of confidentiality. After accidental disclosure, steps should be taken as soon as possible to prevent further disclosure, such as signing an NDA with a person with knowledge.

1.10 Licensing

Right-holders of trade secrets have the right to license their trade secrets to others in a non-exclusive, sole or exclusive manner and charge licensing fees. There is usually a confidentiality clause in the licence contract. Even if there is no obligation of confidentiality in the licence contract, the licensee is also obliged to keep the confidentiality according to the principle of good faith. Therefore, generally speaking, licensing does not affect the protection of trade secrets. In order to ensure that the licensee of trade secrets takes reasonable confidentiality measures, it is recommended that the licensor of trade secrets agrees on confidentiality obligations with the licensee when licensing, and verify the licensee's confidentiality measures.

1.11 What Differentiates Trade Secrets From Other IP Rights

Trade secrets are often associated with the protection of new technologies, often also protected by patents. But the nature of trade secrets and patents is very different.

- Trade secrets include all types of information, not just technically related information. For example, a company's contact list may be the subject of trade secret protection, but it is not protected by patents.
- For a technology to be patented, it must meet the requirements of novelty, inventiveness and utility. Trade secrets, on the other hand, are not required to be novel or inventive. In general, any non-public information that a party has taken reasonable steps to keep confidential is a trade secret assumed to have utility. For example, any know-how can be protected as a trade secret, even if it is not patentable due to lack of inventive step.

- Patent rights and trade mark rights are subject to administrative review and approval (eg, a Chinese patent must be filed and granted by the State Intellectual Property Office of China), while trade secret protection does not. It can be established as long as the three requirements of trade secrets are fulfilled.
- Protection for trade secrets is indefinite. A patent or trade mark right has a certain term. For example, in China, the term of protection for invention patents is 20 years, the term of protection for utility model patents is ten years, and the term of protection for design patents is 15 years, counting from the date of patent application. The protection of trade secrets has no time limit, as long as the trade secret still remains unknown to the public.
- Protection for trade secrets is relative. A right-holder of a patent right, a trade mark right or copyright can exclude others from implementing their right. However, the right-holder of a trade secret has no right to prohibit others from obtaining the information independently through lawful means (eg, through self-development or reverse engineering).
- A trade secret aims to protect non-public information, while the target objects of other IP rights are public. For example, patent and trade marks are published during administrative reviews, while the trade secrets remain unknown to the public during their whole life span.

1.12 Overlapping IP Rights

Trade secrets are often different from other types of intellectual property in the subject matter to be protected, so theoretically, intellectual property rights can be protected by combining trade secrets and other types of intellectual property at the same time. However, due to the different ways of obtaining trade secrets and patents, where the former requires the relevant technology to be kept secret, while the latter must disclose the technology in exchange for monopoly protection, the same technical content cannot be protected by both trade secrets and patents. In addition, although software for example, can be protected by both trade secrets and copyrights, the two lawsuits are concursus actionum, and only one of them can be chosen to sue.

1.13 Other Legal Theories

The types and infringement acts of trade secrets are stipulated in Article 9 of the Anti-Unfair Competition Law. According to this provision, they are:

- obtaining a right-holder's trade secrets by theft, bribery, intimidation, electronic intrusion or other improper means;
- disclosing, using, or allowing others to use a right-holder's trade secrets obtained by the means mentioned in the preceding paragraph;
- disclosing, using or allowing others to use a right-holder's trade secrets in violation of confidentiality obligations or the right-holder's requirements on keeping such trade secrets confidential; and
- obtaining, disclosing, using or allowing any other party to use a right-holder's trade secrets by instigating, tempting or helping any other party to violate the confidentiality obligations or the right-holder's requirements on keeping such trade secrets confidential.

Article 9 also stipulates that other natural persons, legal persons and unincorporated organisations other than the business operators who commit the illegal acts listed in the preceding paragraph shall be deemed as infringing trade secrets.

Therefore, an employee who violates the fiduciary duty to steal trade secrets can be subject to a lawsuit either for breach of contract or infringement of trade secrets. Trade secret infringement claims can also be brought against defendants who induce employees to breach their contractual confidentiality obligations to the right-holder/employer.

1.14 Criminal Liability

According to Article 219 of the Criminal Law, anyone who commits one of the following acts of infringing trade secrets, if the circumstances are serious, shall be sentenced to fixed-term imprisonment of not more than three years, and concurrently or solely with a fine; if the circumstances are especially serious, they shall be sentenced to fixed-term imprisonment of not less than three years but not more than ten years imprisonment and fine for:

- obtaining a right-holder's trade secrets by theft, bribery, intimidation, electronic intrusion or other improper means;
- disclosing, using, or allowing others to use a right-holder's trade secrets obtained by the means mentioned in the preceding paragraph; and
- disclosing, using or allowing others to use a right-holder's trade secrets in violation of confidentiality obligations or the right-holder's requirements on keeping such trade secrets confidential.

At the same time, well knowing the acts listed in the preceding paragraph, still obtaining, disclosing, using or allowing others to use the trade secret shall be regarded as infringement of trade secrets.

According to the relevant judicial interpretations, the implementation of the infringement of trade secrets stipulated in the Criminal Law, (i) causes losses to the right-holder of the trade secrets or the illegal gains from the infringement of trade secrets of more than CNY300,000; or (ii) directly causes bankruptcy or closing down of the right-holder of the trade secret due to major operational difficulties, it shall be deemed as "causing heavy losses to the right-holder of the trade secret". If the amount of loss caused to the right-holder of the trade secret or the amount of illegal gains due to infringement of the trade secret is more than CNY2.5 million, it shall be determined as "causing especially serious consequences" as stipulated in Article 219 of the Criminal Law.

For the infringement of trade secrets, both civil and criminal proceedings can be brought. Due to the stronger ability of the police to investigate and collect evidence, many plaintiffs will choose to report the case to the police first and obtain relevant evidence from them before proceeding with civil litigation.

1.15 Extraterritoriality

Generally, trade secrets are territorial rights and cannot be prosecuted in China for misappropriation that occurs in other countries. However, if – eg, the trade secrets of a company located in China were stolen by electronic intrusion outside of China, it is possible that Chinese courts have jurisdiction since the result of the infringement occurred in China. In addition, if the infringer steals the trade secret abroad and uses it in China – eg, using the trade secret to produce and operate, the right-holder can sue before a Chinese court for the infringement of the infringer's use of the trade secret. In addition, according to the principle of Lex Personalis of the Chinese criminal law, if the perpetrator of the misappropriation is a Chinese company or individual, even if the misappropriation occurs in another country/region, a criminal lawsuit against the Chinese company or individual can be instituted.

2. Misappropriation of Trade Secrets

2.1 The Definition of Misappropriation

In China, the condition for filing a trade secret infringement lawsuit is to prove that the plaintiff is the holder or interested party of the trade secret, generally the licensee; the alleged trade secret meets the definition of trade secret in Article 9 of the Anti-Unfair Competition Law, namely, it belongs to technical or business information not known to the public, has commercial value and been kept confidential by the right-holder by reasonable confidentiality measures; the defendant has infringed trade secrets as stipulated in Article 9 of the Anti-Unfair Competition Law. For non-employees, it needs to be proven that the defendant committed an improper means.

The right-holder does not need to prove that their trade secret has been used, but just enough to prove that the defendant obtained the trade secret without permission to file a trade secret infringement lawsuit.

2.2 Employee Relationships

If the infringer of a trade secret is an employee, who breaks the duty of confidentiality or disobeys the right-holder's requirement to keep trade secrets, and discloses, uses or allows others to use the trade secrets in their possession, it is also an act of infringement of trade secrets. Therefore, the elements of a trade secret misappropriation claim are different.

For employees, if there is a confidentiality agreement signed with the employer, the confidentiality obligation shall be fulfilled. If there is no confidentiality agreement, the employee has a negative obligation of inaction – ie, to keep the trade secret, not use it beyond the scope or authority, nor disclose or allow others to use the trade secret.

2.3 Joint Ventures

Based on the principle of good faith, joint venturers have a negative obligation of inaction – ie, the obligation to keep each other's trade secrets known during co-operation.

2.4 Industrial Espionage

At present, there are no special provisions for industrial espionage in Chinese laws. Such acts of stealing trade secrets are still dealt with in accordance with the Anti-Unfair Competition Law and Criminal Law. Similar to other intellectual property rights, remedies for trade secret infringement include damages and injunctions.

3. Preventing Trade Secret Misappropriation

3.1 Best Practices for Safeguarding Trade Secrets

Regarding the "best practice" of protecting trade secrets, the relevant judicial interpretations give some "suggestions":

- signing a confidentiality agreement or stipulating confidentiality obligations in the contract;
- putting forward confidentiality requirements for employees, former employees, suppliers, customers, visitors, etc, who are accessible to and able to obtain trade secrets, through articles of association, training, rules, regulations, or written notices, etc;
- restricting visitors or conducting separate management for production and business sites such as workshops involving secrets;
- distinguishing and managing trade secrets and their carriers by marking, classifying, isolating, encrypting, sealing up, limiting the scope of persons who can access or obtain them, etc;

- taking measures such as prohibiting or restricting the use, access, storage, reproduction, etc, of computer equipment, electronic equipment, network equipment, storage equipment, software, etc, that can access and obtain trade secrets; and
- requiring resigned employees to register, return, remove and destroy the trade secrets and their carriers that they have accessed or acquired, and continue to undertake the obligation of confidentiality.

Best practices vary by different technical fields. For example, in the field of computer software, the right-holder is usually advised to divide the development of the software into different modules, and each module is developed by different personnel, so as to avoid the developer mastering all the source code as much as possible. Another example is in the field of chemistry where codification management is usually adopted for raw materials, intermediates, products, etc.

3.2 Exit Interviews

Different companies have different strategies for exit interviews. Typically, an exit interview should include the following:

- review the terms of the NDA with departing personnel and ask them to contact the company if they have questions with respect to the NDA;
- remind employee/contractor of duty not to use or divulge company's trade secrets;
- require that the employee sign a termination certificate, if possible, acknowledging the employee's understanding and duty not to disclose trade secrets or confidential information;
- obtain trade secret materials and documents in the employee's possession or control, including, without limitation, hard copies, soft copies, home computer files, home office files, laptops, cell phones, etc; and
- require that keys and access cards be returned.

4. Safeguarding Against Allegations of Trade Secret Misappropriation

4.1 Pre-existing Skills and Expertise

At present, there is no specific definition of "employee's general knowledge and skills" in China's trade secret practice. In principle, the knowledge and skills acquired by an employee in working for the employer have become part of their personality, and the employee has the right to apply the knowledge and skills acquired in the new job, but the employee should not use trade secrets learnt from the previous employer in the work of a new employer. Usually, if an employer is concerned about the use of trade secrets by a former employee in a particular position, the employer shall enter into a non-compete agreement with the employee, requiring the employee not to engage in an industry that competes with the employer for up to two years, during which the employer must pay a reasonable fee to the employee.

4.2 New Employees

The "new" employer should first strictly manage the employment of such resigned employees and recruit such resigned employees through legal and proper means, check whether the employee to be hired has terminated the labour contract with the former employer, and whether they have the obligation of non-compete and/or confidentiality of trade secrets and ask the employee to be hired to make a written statement or commitment. The "new" employer should investigate

the similarities and differences between the original and current position of the employee to be hired and arrange the current position carefully, fully investigate the actual performance of such employees, and require employees to promise not to use the trade secrets of the previous employer in the course of their work; at the same time, most importantly, the "new" employer should archive and preserve relevant evidence, such as keeping all the materials proving that it obtained the trade secrets of others through lawful measures, such as reverse engineering.

5. Trade Secret Litigation

5.1 Prerequisites to Filing a Lawsuit

Since there is no discovery in the civil procedure in China, the plaintiff should collect evidence, including evidence of infringement and compensation, before filing a lawsuit.

To file a lawsuit for infringement of trade secrets, the following work should be done:

- determining the parties of the lawsuit – ie, the plaintiff and the defendant;
- determining the court of jurisdiction: territorial and level jurisdiction, distinguishing between technical and business information;
- carrying out necessary preservation, including evidence and conduct preservation;
- determining the scope of trade secrets;
- determining the constituent elements of trade secrets – ie, not known to the public, commercial value, and taking corresponding confidentiality measures;
- identifying basic types and scope of infringement acts; and
- determining the litigation claims, the type of civil liability: stop the infringement, compensate for losses, return or destroy the trade secret carrier, remove the trade secret information in possession.

5.2 Limitations Period

The statute of limitations does not apply to claims for cessation of the infringement of the trade secrets; for claims for damages from infringement, the statute of limitations begins to be counted when the right-holder knows or should have known the scope of infringement, the infringer and the infringing acts. In principle, the limitation period is three years, but shall not exceed 20 years from the date of infringement. At the same time, trade secret cases, like other civil cases, are subject to the relevant provisions on the suspension and interruption of the limitation of action.

5.3 Initiating a Lawsuit

As mentioned above, in China, there is no discovery in the civil procedure. Therefore, after collecting the evidence and finishing other preparations (see **5.1 Prerequisites to Filing a Lawsuit**), the plaintiff should file a lawsuit with the court. Generally, after accepting a case, the court will give both parties a time limit for producing evidence, and then organise evidence exchange and pretrial conference. Furthermore, the court will organise at least one formal trial before reaching a final conclusion. Trade secret litigation cases also often involve forensic appraisal, such as appraisal of whether the secret point is known to the public, and whether the accused information is the same as the secret point information. Forensic appraisal can be unilaterally entrusted by the plaintiff or the defendant, or may be entrusted by the court.

5.4 Jurisdiction of the Courts

In terms of territorial jurisdiction, the court of jurisdiction for cases of infringement of trade secrets includes the court at the place where the

infringement is committed (including the place where the infringement is carried out and the result of the infringement occurs) or the court at the place where the defendant is domiciled. In terms of level jurisdiction, the court for technical secret cases is the intermediate people's court designated by the Supreme Court, and the court for trade secret cases other than technical secrets is the basic court. These Supreme Court-designated Intermediate Courts include four Intellectual Property Courts and more than 20 Intellectual Property Tribunals across China. In addition, the level of jurisdiction is also affected by the amount of compensation of the lawsuit. For example, for cases with a compensation amount exceeding CNY5 billion, the provincial high court has jurisdiction.

5.5 Initial Pleading Standards

In China, civil cases follow the principle of "who claims, who gives evidence". Therefore, for trade secret cases, the plaintiff is also required to have conclusive evidence to prove the existence of infringement. However, due to the difficulty of obtaining evidence in trade secret cases, the current trend in legal and judicial practice is to reduce the difficulty of proof for plaintiffs and appropriately reallocate the burden of proof. For example, according to Article 32 of the new Anti-Unfair Competition Law, in the civil trial procedure of infringing trade secrets, the owner of trade secrets shall provide prima facie evidence to prove that they have taken confidentiality measures for the claimed trade secrets and reasonably show that the trade secret has been infringed, while the accused infringer shall prove that the trade secret claimed by the right-holder does not belong to the trade secret stipulated in this law.

Where the right-holder of a trade secret provides prima facie evidence reasonably showing that the trade secret has been infringed, and provides one of the following as evidence, the accused infringer shall prove that they have not infringed the trade secret:

- there is evidence that the accused infringer has channels or opportunities to obtain the trade secret, and the information used is substantially the same as the trade secret;
- there is evidence that the trade secret has been or is at risk of being disclosed or used by the accused infringer; and
- there is other evidence that the trade secret has been infringed by the accused infringer.

These provisions reduce the difficulty of the plaintiff's proof and reallocate the burden of proof to the defendant after the plaintiff provides prima facie evidence.

5.6 Seizure Mechanisms

The Civil Procedure Law grants the parties a right to apply to the people's court for preservation of evidence when the evidence may be lost or difficult to obtain in the future. Plaintiffs in trade secret infringement cases often take advantage of this provision of the Civil Procedure Law to file an application for evidence preservation while suing, hoping to obtain direct evidence of the defendant's infringement and relevant compensation evidence through the court. When the court examines the plaintiff's application for evidence preservation, it mainly considers the following factors:

- the plaintiff should clearly claim the specific content of the trade secret and fix relevant evidence;
- the plaintiff should provide prima facie evidence of the defendant's infringement;
- the scope of evidence preservation shall be consistent with the claim. Generally, the

scope of preservation shall not exceed the trade secrets claimed by the plaintiff nor the claims of the plaintiff. The evidence that the plaintiff can obtain or can be fixed through notarisation will not be preserved by court; and
- the guarantee provided by the plaintiff.

5.7 Obtaining Information and Evidence

As mentioned in **5.5 Initial Pleading Standards** and **5.6 Seizure Mechanisms**, even if an evidence preservation can be applied, the plaintiff should have prima facie evidence of the defendant's infringement. The plaintiff should complete the acquisition of prima facie evidence by themselves and cannot rely on other mechanisms. After the prima facie evidence is presented, on the one hand, the plaintiff can obtain further evidence through the court's evidence preservation; on the other hand, if the defendant infringes technical secrets to a serious extent and is suspected of committing a crime, the plaintiff can also report to the police. Because the police have strong investigative capabilities, the plaintiff can also obtain evidence through this channel for civil proceedings.

The evidence that the plaintiff can furnish includes evidence related to infringement and damages.

5.8 Maintaining Secrecy While Litigating

According to the relevant judicial interpretation, when the applicant's trade secret is about to be illegally disclosed, it should be determined whether it is "urgent" as stipulated in Articles 100 and 101 of the Civil Procedure Law; if yes, the applicant can require the court to make a conduct preservation ruling – ie, an injunction to order the defendant not to disclose, use or allow others to use the trade secret stolen from the applicant. Since trade secret cases are not heard in public, if the court conducts evidence preservation, the process will not be made public, and the trade secrets involved and their carriers will not be disclosed to third parties.

5.9 Defending Against Allegations of Misappropriation

Common defences in trade secret cases include the following.

- Defence against trade secrets:
  - (a) the scope of the trade secret is unclear and its carrier is not submitted;
  - (b) the secret point is unclear and incorrect;
  - (c) the trade secret was known to the public before the defendant obtained or used it; and
  - (d) the owner or the licensee of the trade secret involved did not take the corresponding confidentiality measures for the trade secret.
- Self-development or reverse engineering defence:
  - (a) Article 14 of the judicial interpretation of trade secrets;
  - (b) where the accused infringing information is obtained through self-development or reverse engineering, the people's court shall determine that it is not an act of infringing trade secrets as stipulated in Article 9 of the Anti-Unfair Competition Law; and
  - (c) the term "reverse engineering", as mentioned in the preceding paragraph, refers to the disassembly, surveying, mapping and analysis of products obtained from public channels through technical means, in order to obtain relevant technical information of the products.
- Client trust defence:
  - (a) paragraph 2 of Article 13 of the judicial interpretation of unfair competition – if a

client conducts market transactions with the employee entity based on his personal trust; after the employee resigns, if he can prove that the client voluntarily chooses to conduct market transactions with himself or his new entity, he shall be deemed not to have adopted improper means unless otherwise agreed between the employee and the original entity; and

(b) paragraph 2 of Article 2 of the judicial interpretation of trade secrets – if a client conducts market transactions with the employee entity based on his personal trust; after the employee resigns, if he can prove that the client voluntarily chooses to conduct market transactions with himself or his new entity, the people's court shall determine that the employee did not use improper means to obtain the trade secret of the right-holder.

5.10 Dispositive Motions

There are no dispositive motion-related procedures in China's civil litigation. However, in the current trend, before entering the formal trial procedure, the parties can directly conduct a mediation, and the court may also preside over the mediation. If a settlement is reached by both parties, the court can make a mediation statement accordingly, which has legal effect.

5.11 Cost of Litigation

For trade secret litigation, the attorney fees usually range from hundreds of thousands to millions depending on the difficulty of the case. For example, in the "Vanillin" case recently heard by the Supreme People's Court, the court supported a reasonable fee of CNY3.5 million for rights protection. The expenses that the plaintiff and the defendant can expect include damages, punitive compensation, and reasonable expenses for rights protection, including attorney fees, notarisation fees, translation fees and appraisal fees.

In China, risk agency is allowed for civil cases. As for litigation financing, or third-party funding, there is currently no clear determination of whether it is legal or not, but litigation financing already exists in practice.

6. Trial

6.1 Bench or Jury Trial

There is no separate jury fact-finding procedure in China. China adopts a unique system of people's assessors. In some cases, people's assessors can participate in the trial of cases. People's assessors have the same rights and obligations as judges.

6.2 Trial Process

In China, there is no difference between the trial of trade secret cases and the trial of general civil cases, except that trade secret cases are usually not heard in public. The trial process generally includes stages such as evidence exchange and cross examination, court investigation and court debate, among which court investigation and court debate are often carried out together. Except for a few cases, the witness who has given testimony shall appear and testify in court, otherwise their testimony cannot be used as the basis for independent determination of facts. Generally, trade secret cases are the same as other civil cases, the second instance is final, and the trial period is six months for the first instance and three months for the second instance. The above period may be extended.

6.3 Use of Expert Witnesses

In trade secret cases, the plaintiff and the defendant may hire expert witness to give tes-

timony on the technical issues for which they are responsible. An expert witness can provide answers to professional and technical questions and ask questions of the other party's expert witness. However, in trade secret cases, it is more common to ask a professional judicial appraisal institution to issue an appraisal report, such as whether the secret point is unknown to the public and whether the defendant's information is the same as that of the trade secret. The appraisal expert shall appear in court. Usually, according to different appraisal contents, the appraisal cost is several hundred thousand yuan.

7. Remedies

7.1 Preliminary Injunctive Relief

According to the relevant judicial interpretation, when the applicant's trade secret is about to be illegally disclosed, it should be determined whether it is "urgent" as stipulated in Articles 100 and 101 of the Civil Procedure Law; if yes, the applicant can require the court to make an conduct preservation ruling – ie, injunction to order the defendant not to disclose, use or allow others to use the trade secret stolen from the applicant. The preconditions for the preservation of the above acts include:

- the trade secret claimed by the applicant meets the constitutive requirements;
- the fact of infringement exists or is about to happen;
- irreparable damage will be caused if such an injunction is not granted;
- guarantee provided by the applicant according to law; and
- the injunction shall not harm the public interest.

If the people's court rules to implement the conduct preservation measures, it shall reasonably determine the duration of the measures according to the request of the applicant or the specific circumstances of the case and other factors.

The effect of ruling to stop the infringement of intellectual property rights is generally maintained until the judgment of the case takes effect.

The amount of guarantee provided by the applicant shall be equivalent to the losses that the respondent may suffer from the implementation of the act preservation measures, including reasonable losses such as the sales income and storage expenses of the products involved to stop the infringement.

In the process of implementing the conduct preservation measures, if the losses that the respondent may suffer as a result exceed the guarantee provided by the applicant, the people's court may order the applicant to add corresponding guarantees.

7.2 Measures of Damages

The amount of compensation for business operators who have suffered damage due to unfair competition shall be determined according to the actual loss suffered due to the infringement. If the actual loss is difficult to calculate, the compensation shall be determined according to the profits obtained by the infringer due to infringement. The amount of compensation shall also include the reasonable expenses spent by the operator to stop the infringement.

In order to obtain the above compensation, the plaintiff shall provide corresponding evidence. In order to determine the amount of compensation, the people's court may order the infringer to provide the account books and materials related

to the infringement when the plaintiff has tried their best to furnish evidence and the account books and materials related to the infringement are mainly in the possession of the infringer. If the infringer fails to provide or provides false account books and materials, the people's court may determine the amount of compensation with reference to the claims of the plaintiff and the evidence provided.

If it is difficult to determine the actual losses suffered by the right-holder due to the infringement and the profits obtained by the infringer due to the infringement, the people's court shall make a judgment to compensate the right-holder less than five million yuan according to the circumstances of the infringement.

If an infringer maliciously commits an act of infringing trade secrets and the circumstances are serious, the amount of compensation may be determined at more than one time and less than five times the amount determined in accordance with the above methods.

7.3 Permanent Injunction

Trade secret cases in which plaintiffs win usually result in a cessation of infringement and damages, unless the trade secret has already been disclosed so that the judgment prohibiting the disclosure of the trade secret is meaningless. Generally, unless the case is settled through settlement or mediation, the plaintiff cannot ask the defendant to recall the products. Since employees have the freedom of employment, it is generally impossible to restrict their subsequent employment. Employers can only restrict subsequent employment of a departing employee through a non-compete agreement for a period of no more than two years and for a fee. An injunction to cease infringement generally has no time limit until the invalidation of the trade secret.

7.4 Attorneys' Fees

Generally, the plaintiff can claim for the reasonable expenses to stop the infringement, including reasonable attorney fees, notarisation fees, translation fees, appraisal fees, etc. Claims for reasonable expenses to stop infringement require relevant evidence, usually including contracts, payment vouchers and invoices.

7.5 Costs

Successful plaintiffs can obtain damages for infringement, punitive compensation and reasonable expenses spent to stop infringement, including reasonable attorney fees, notarisation fees, translation fees, appraisal fees, etc. The plaintiff shall list the above claims in the indictment, and the judge will hear the case according to the claims. Successful defendants generally cannot obtain compensation unless the plaintiff abuses intellectual property rights.

8. Appeal

8.1 Appellate Procedure

Either or both the plaintiff and the defendant who are dissatisfied with the first instance judgment, may appeal to the higher court. For technical secret cases, the Intellectual Property Tribunal of the Supreme People's Court has jurisdiction, and for trade secrets other than technical secrets, the higher court (mostly intermediate people's courts) has jurisdiction. For the judgment, the appeal period is 15 days from the date of receipt of the judgment; for the ruling, the appeal period is ten days from the date of receipt of the ruling, and for a party who has no domicile in China, the appeal period is 30 days from the date of receiving the judgment or ruling. The trial period of the second instance is three months, which can be extended. The appeal procedure will not vary between courts.

8.2 Factual or Legal Review

The court of second instance focuses more on legal issues, but usually also ascertains factual issues. If the second-instance court finds out that the basic facts determined by the first-instance judgment are unclear, it will usually send it back to the first-instance court for retrial; if other facts are unclear, the second-instance court can also revise the judgment after finding out the facts. Usually, the second instance is not de novo and will be tried according to the appellant's grounds of appeal. For issues that need to be reserved, the appellant should clearly record it in the grounds of appeal. For most trade secret cases, the court of second instance does not merely conduct a written hearing, instead, it usually gives both parties an opportunity to present and debate.

9. Criminal Offences

9.1 Prosecution Process, Penalties and Defences

To file a criminal lawsuit against a trade secret case, it is necessary to report the case to the police first and provide preliminary evidence of the trade secret held and the infringement of the trade secret.

According to Article 219 of the Criminal Law, if the circumstances of infringing trade secrets are serious, the infringer shall be sentenced to fixed-term imprisonment of not more than three years, and concurrently or solely with a fine; if the circumstances are particularly serious, the infringer shall be sentenced to fixed-term imprisonment of not less than three years but not more than ten years and shall also be fined.

The defences in criminal cases are basically the same as those in civil cases. However, it should be noted that the proof level of evidence in criminal cases is to eliminate reasonable doubt, while civil cases adopt the high probability standard. Therefore, being recognised as infringement in civil cases is not necessarily recognised as infringement in criminal cases. Holders of trade secrets can actively provide clues, but once the police file a case, the investigation will be completed by them.

10. Alternative Dispute Resolution (ADR)

10.1 Dispute Resolution Mechanisms

Regarding ADR for trade secret disputes, the more mature mechanism in China is mediation, which includes not only court mediation, but also people's mediation and administrative mediation. The main pros of mediation include:

- mediation is simple, fast and flexible;
- the general cost of mediation is low; and
- mediation can resolve disputes in a relatively mild way, and can also reflect fairness and justice.

However, mediation also has cons, including:

- the limitations of mediation cases– ie, it is only suitable for cases with clear legal relationship and minor disputes;
- mediation cases may make the parties lose the best time to litigate; and
- poor execution of non-court mediation.

Due to the difficulty in proving evidence and the low success rate in trade secret cases, the plaintiff may consider mediation to achieve the purpose of protecting trade secrets to a certain extent for cases with pessimistic prospects for litigation. Usually, the mediation process can

guarantee confidentiality to avoid further disclosure of trade secrets.

In addition, as another ADR mechanism, if a "contract" has been signed between the right-holder and the infringer and both parties voluntarily reach an arbitration agreement, they can apply for arbitration to the local arbitration institution or the arbitration institution agreed in the arbitration agreement in accordance with the Arbitration Law of the PRC.

Alternative dispute resolution mechanisms can be used as a pre-procedure to litigation and are not inconsistent with litigation procedures, so interim measures can be obtained from the courts.

In addition, the mediation statement issued by the court according to the mediation agreement of the parties has the force of enforcement, and the parties can apply to the court of first instance or the court at the same level where the property being enforced is located for enforcement. The arbitration award issued by the arbitration institution is also enforceable, and the parties may apply for enforcement to the intermediate people's court in the place where the person subject to enforcement has their domicile or where the property subject to enforcement is located.

Trends and Developments

Contributed by:
Jerry Xia, Ning Dong and Yulu Wang
GEN Law Firm

GEN Law Firm is built on one of the fastest growing teams in the Chinese legal community. With four offices in Beijing, Shanghai, Shenzhen, and Chengdu, the firm acts as one integrated team to responsively address diverse client needs across China. Most GEN Law partners have extensive experience in prestigious foreign law firms and/or degrees from top law schools. GEN Law's practice focuses on complex dispute resolution, intellectual property, compliance (anti-monopoly, data protection, anti-bribery, etc), corporate and government affairs (regulatory trust building, crisis management, policy advocacy, regulatory communication, etc). Its clients cover domestic and foreign leading enterprises and government agencies, with team members being well recognised by legal ranking bodies.

Authors

Jerry Xia is one of the founding partners of GEN Law Firm, and the managing partner of Shanghai office and US liaison office. Mr Xia's practice focuses on providing strategic advice to local and international clients in the areas of intellectual property (both contentious and non-contentious), dispute resolution, brand licensing and technology transactions, M&A, compliance and regulatory compliance, policy advocacy and government affairs, etc. Particularly in terms of IP practice (patents, trade marks, trade secrets, copyright, etc), he is one of the IP experts in the industrial and information technology field, recognised by the Chinese Ministry of Industry and Information Technology (MIIT).

Ning Dong has more than 19 years of experience in intellectual property prosecution and litigation. His practice focuses on the representation of Fortune 500 and other companies in connection with patent matters, including litigation, invalidation and prosecution, especially in the fields of computer software and hardware, telecommunications, and consumer electronic devices. He also regularly advises clients on matters in relation to trade mark, trade secrets and unfair competition and other IP related matters.

Contributed by: Jerry Xia, Ning Dong and Yulu Wang, **GEN Law Firm**

Yulu Wang has five years of experience in intellectual property litigation and non-litigation. She specialises in patent infringement litigation and enforcement, trade secret compliance, trade mark infringement litigation, and unfair competition. Ms Wang graduated from the Intellectual Property School of Shanghai University and is qualified as both a Chinese lawyer and a patent attorney. Before joining GEN Firm, she interned at an intellectual property tribunal in a Shanghai court, where she assisted judges in handling complex trade mark and copyright infringement cases and conducted crucial case research.

GEN Law Firm

Suite 1001
China World Office 2
1 Jianguomenwai Avenue
Chaoyang District
China

Tel: +86 10 6521 5999
Fax: +86 10 6521 5900
Web: www.genlaw.com/en

China has long been regarded as the "world's factory", but over the past decade, an increasing number of Chinese enterprises have joined the competition in advanced technology, making the protection of intellectual property rights, including trade secrets, more urgent than ever. Fortunately, China has been continuously strengthening the protection of intellectual property rights, including trade secrets. To address the need for trade secret protection, China amended its Anti-Unfair Competition Law (AUCL) in 2017 and 2019, and issued a judicial interpretation for civil cases involving trade secrets (the "Civil JI") and a judicial interpretation for criminal cases involving IP infringement (the "Criminal JI") in 2020, a rarity in terms of legislative frequency in other fields.

Below we summarise the latest trends and developments of trade secret protection in China.

Changes to Jurisdictional Levels

Before 2019, civil cases involving the infringement of technical secrets, akin to those of patent infringements, fell under the jurisdiction of the Intermediate People's Court or specialised intellectual property courts such as the Beijing Intellectual Property Court at the first instance level, and were escalated to the Provincial High People's Court for appeals. Following the 2019 establishment of the Intellectual Property Court within the Supreme People's Court (SPC), appeals in technical secret infringement cases shifted to being adjudicated by the SPC, which issued dozens of influential and guiding rulings. However, by the end of 2023, likely due to the overwhelming workload, the SPC delegated the responsibility for hearing appeals in technical secret cases back to the Provincial High People's Courts. Given the complex nature of cases involving technical secrets, the lack of a unified appellate review standard from the SPC may lead to some degree of inconsistency.

Expanded Scope of Protectable Trade Secrets

The AUCL does not specify the types of information that may constitute trade secrets. Common trade secrets often include drawings, production processes, formulas, software codes, customer information, etc. However, in some recent cases, trade secret claims have expanded to include corn parent seed that can be used to cultivate hybrid seeds, reservoir attribute data defined in the databases of oil and gas extraction companies, as well as user tipping data on live streaming platforms. Any information can be treated as trade secrets as long as it meets the requirements of Article 9 of the AUCL, which stipulate that the information must not be known to the public, must have commercial value, and must have been subject to reasonable confidentiality measures by the rights-holder.

Increased Damages

China has traditionally aligned the rules for awarding damages for trade secret infringement with those for patent infringement, based on the actual loss suffered due to the infringement or the profits gained by the infringer. Due to the lack of US-style discovery, it is often challenging for plaintiffs to identify the foundation for calculating damages, resulting in the use of statutory damages in the majority of cases.

The Civil JI has introduced a system for ordering the submission of financial documents. Specifically, if the rights-holder has already provided preliminary evidence of the profits gained by the infringer from the infringement, but the account books and documents related to the infringement of trade secrets are controlled by the infringer, the court can, upon the application of the rights-holder, order the infringer to provide such account books and documents. If the infringer refuses to provide them without a justified reason, or provides false information, the

court may determine the profits gained from the infringement based on the claims and evidence provided by the rights-holder. This system can significantly reduce the burden of proof on the rights-holder, avoiding over-reliance on statutory compensation.

Additionally, after amendments in 2017 and 2019, the AUCL increased the maximum statutory compensation from CNY1 million CNY5 million. Moreover, the 2019 amended AUCL allows the court to amplify exemplary damages up to five times in cases of wilful and malicious misappropriation.

In the recent years, there has been an increase in cases with significant compensation awards. In the case of Sennics Chemical v Yuncheng Jinteng, the SPC of China, relying on the plaintiff's actual loss determined by the valuation report in the corresponding criminal case, ordered the defendant to compensate for losses amounting to CNY201.54 million (approximately USD27.6 million). Previously, in the case of Jiaxing Zhonghua Chemical v Wanglong Group, which involved the production process and equipment design of vanillin (referred to as the "Vanillin Case"), the SPC awarded the plaintiff about CNY160 million. This decision was based on the defendant's product sales profit instead of operating profit, considering that the defendant had always engaged in infringement as its sole business and had failed to comply with the court's order to produce evidence. In another case, Golden-Elephant Sincerity v Hengsheng Chemical, the SPC awarded CNY98 million in damages for trade secret misappropriation, and an additional CNY120 million RMB for patent infringement, resulting in a total of CNY218 million (approximately USD30 million). Subsequently, both parties reached a settlement of CNY440 million for other infringement activities, setting a record for compensation and settlement amounts in Chinese intellectual property dispute cases.

In Tinci v Newman, involving the production process and equipment of Carbopol products, the SPC, considering Newman's infringement as a business and its continued production even after its legal representative was held criminally responsible, as well as its refusal to provide relevant accounting books, supported the compensation amount to five times the profits from infringement.

Reduced Burden of Proof for Rights-Holders

The rule in China's Civil Procedure Law is that the burden of proof lies with the party who asserts a claim. For trade secret cases, this means the plaintiff would need to prove that the information they claim meets the criteria for being a trade secret; ie, it is not known to the public, reasonable measures have been taken to keep it secret, and it has commercial value. The rights-holder would also need to prove that the defendant carried out the misappropriation of trade secret. This is clearly a significant challenge for the plaintiff, given the covert nature of trade secret infringement.

The AUCL, revised in 2019, provides rules for shifting the burden of proof. If the rights-holder provides preliminary evidence showing that they have taken measures to keep the claimed trade secret confidential, and reasonably indicates that the trade secret has been misappropriated, the alleged infringer must prove that the trade secret claimed by the rights-holder does not fall under the protection of this law. If the trade secret rights-holder provides preliminary evidence reasonably indicating that the trade secret has been misappropriated, and there is evidence that the alleged infringer had the channel or opportunity to access the trade secret,

and the information they used is substantially the same as that trade secret, or there is evidence that the trade secret has been disclosed, used, or is at risk of being disclosed or used by the alleged infringer, then the alleged infringer must prove that they have not engaged in infringement of the trade secret.

For example, in Ingersoll-Rand v a former employee, the defendant transferred drawings containing the involved technical secrets to a personal storage device without company permission. After Ingersoll-Rand proved it had taken reasonable confidentiality measures for the technical information and that it had value, the court found that the plaintiff had fulfilled its burden of proof that the asserted technical information met the requirements for being a trade secret, and the defendant failed to provide counter-evidence. Therefore, the court recognised the asserted technical information as a trade secret. In Huasui Seed v Bosheng Seed, although the plaintiff did not submit any evidence that the defendant had obtained the asserted parental corn seeds through improper means, because the defendant could not explain the legitimate source of the corn seeds it used, the court presumed that Bosheng Seed acquired the asserted corn seeds through improper means.

Preliminary Injunctions

In China, preliminary injunction (PI) is also known as behavioural preservation. According to the Civil JI, if the respondent attempts or has already obtained, disclosed, used, or allowed others to use the trade secret claimed by the rights-holder by improper means, and failing to take behavioural preservation measures would make the judgment difficult to enforce or cause other damages to the parties involved, or would cause irreparable harm to the legitimate rights and interests of the rights-holder, the court can order the PI. When reviewing the application for PI, the court should comprehensively consider the following factors: (i) whether the applicant's request has a factual basis and legal basis, including the stability of the asserted right; (ii) whether failing to grant the PI would cause irreparable harm to the applicant's legitimate rights and interests or make it difficult to enforce the judgment; (iii) whether the harm caused to the applicant by not granting the PI exceeds the harm caused to the respondent by granting the PI; and (iv) whether granting the PI would harm the public interest.

Due to the complexity of trade secrets, these factors are not easily judged in most cases. In the case of Eli Lily and Company v Huang, Huang was found to transfer Eli Lily's confidential documents to a private storage device. Given that Huang admitted that the involved documents belonged to trade secrets and admitted to the act of transferring of those documents, the Shanghai No 1 Intermediate People's Court issued a PI to prohibit Huang from disclosing, using, or allowing others to use the content of the documents claimed to be trade secrets by the plaintiff. More PIs were issued after the first-instance court had determined the relevant infringement facts, for example, the Zhejiang High Court in the Vanillin Case and the Jiangsu High Court in the Sennics Chemical v Yuncheng Jinteng, both issued the PI along with the first-instance judgment. In Actions Technology v TaiXin Semiconductor, the SPC remanded the case to the first-instance court in light of the possibility that the involved technical information had been illegally held, disclosed, and used, and while remanding, it ordered that the defendant must not disclose, use, or allow others to use the involved technical information before a final judgment is made. Recently, the Jiangsu High Court issued a PI in the case of China Seed International v Fujitai,

which involves trade secrets of plant variety breeding materials.

Rapidly Growing Criminal Cases

According to the most recent statistical data released by the Supreme People's Procuratorate (SPP) in October 2023, during the period from January to September 2023, Chinese prosecutorial organs accepted and reviewed for prosecution over 260 individuals involved in crimes of infringing commercial secrets, which is a twofold increase from the previous year.

Article 4 of the Criminal JI lowered the threshold for criminal liability from causing a loss of CNY500,000 (about USD70,000) to CNY300,000 (about USD40,000). This article also expanded the circumstances that constitute a crime to not only include monetary standards (loss) but also provided an open list of scenarios, supplementing it with circumstances such as the rights-holder's bankruptcy or closure, repeated infringement, and other serious situations.

Article 5 of the Criminal JI specified different methods for calculating losses for different acts of trade secret infringement. In the past, situations where trade secrets were stolen but not disclosed or used before being caught made it difficult to calculate the amount of loss. According to Article 5, in such cases, the amount of loss can be determined based on the reasonable licensing fee of that trade secret. If the infringement results in the trade secret becoming known to the public or being destroyed, the loss amount can be determined based on the commercial value of the secret. Remedial expenses incurred by the rights-holder to mitigate the loss to business operations, business plans, or to restore the security of computer information systems, or other systems, should be included in the loss caused to the rights-holder.

In Xiamen City v Liao, the first-instance court determined the loss amount based on the assessed value of the licensing fee of the trade secret at CNY8.5899 million, ultimately sentencing Liao to three years in prison for infringing commercial secrets and fining him CNY100,000.

In Shanghai City v Ping, Ping illegally obtained Zuiko Company's technical drawings, disclosed and used them, and applied for patents for some of the technical information, resulting in the complete public disclosure of the trade secrets. The procuratorate brought a prosecution based on the total amount of actual losses caused to the rights-holder plus the value of the trade secrets, which was supported by the court.

In Jieyang City v Liu, the suspect, posing as a supplier staff member, entered the victim's wind turbine project site, measured, and photographed the internal structure of the units, and was caught while fleeing the scene. The first-instance judgment included the losses due to inspection fees of the turbine units and production downtime caused by the infringement, in the losses to the rights-holder.

Following the legal amendments, the lowered threshold for criminal prosecution of trade secret infringement and increasingly clear rules for calculating losses mean that more acts of infringing commercial secrets are being prosecuted and subjected to more severe criminal liabilities.

New Crime of Commercial Espionage

In December 2020, Amendment XI to the Criminal Law added the crime of "espionage or illegal provision of trade secrets for foreign entities", also known as commercial espionage. It states: "whoever steals, spies on, buys, or illegally provides commercial secrets for foreign institutions, organizations, or individuals shall be sentenced

to fixed-term imprisonment of not more than five years and may also be fined; in serious cases, the sentence shall be fixed-term imprisonment of not less than five years and a fine". Thus, any act of stealing commercial secrets for foreign entities could be prosecuted for commercial espionage without the need to meet the "serious circumstances" required for general infringement of trade secrets. This may be something that foreign companies need to pay particular attention to.

In November 2023, the Pudong New Area Court in Shanghai publicly disclosed a case under this crime for the first time: the Zheng Case. In this case, Zheng, an engineer at a company, provided consultancy services to a competitor as an industry expert consultant after leaving his job. Knowing that the consulting party was a foreign organisation, he still provided the commercial secret information he had illegally learned from his former employer to the consulting party. Zheng was ultimately convicted of commercial espionage and sentenced to 2.5 years in prison and a fine of CNY10,000.

Administrative Protection Becoming Increasingly Active

China has a route for administrative enforcement, whereby administrative authorities can also investigate and handle infringement of trade secrets. Compared to civil litigation, administrative enforcement is often more efficient. For example, in typical cases announced across various regions, administrative authorities are often able to make decisions within six months. Additionally, administrative authorities can conduct raids to investigate and collect evidence, which is very important in trade secret infringement cases.

The AUCL, revised in 2019, increased the punitive power of administrative authorities, allowing for fines ranging from CNY500,000 to CNY5 million for serious violations. In April 2023, the Chinese government organised a special enforcement action called "Guardian" against unfair competition, with the protection of trade secrets being an important component. Under the lead of the "Guardian" special action, AMRs (Administration for Market Regulation) across the country actively carried out administrative enforcement activities against infringement of trade secrets and released many typical cases. On 2 March 2022, SAMR (State Administration for Market Regulation) issued the "National Action Plan for Innovation Pilot Work on Trade Secret Protection", under which national and local AMRs and industry associations have developed and published standards for compliance management of corporate trade secrets guided by this plan.

Although rights-holders cannot obtain monetary compensation in administrative enforcement procedures, collecting evidence and quickly stopping infringement through administrative enforcement and then seeking monetary compensation in civil litigation has become a common option for rights-holders.

Conclusion

Trade secrets play a vital role in maintaining the competitive advantage and financial stability of many companies. The anticipation is that accusations of trade secret misappropriation will continue to rise. Even with the advancements in trade secret protection in China, companies are encouraged to re-evaluate their strategies and procedures for protecting their sensitive information and to take pre-emptive steps in safeguarding it before any potential claims arise.

CHINA - BEIJING

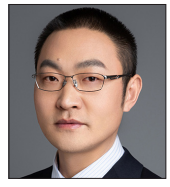
Trends and Developments

Contributed by:
Ye Zhao, Zhanjiang Zhang and Qiang Ma
Jingtian & Gongcheng

Jingtian & Gongcheng was established in the early 1990s, and is a leading independent partnership law firm in China. Renowned as one of the country's top full-service business law firms, it specialises in areas like capital markets, M&A, cross-border investments and intellectual property. The firm operates from key locations across China, including a significant presence in Hong Kong. With a team of 180 partners and 760 lawyers, many from top-tier law schools and with diverse professional backgrounds, Jingtian & Gongcheng offers unparalleled legal expertise. Reputed for innovative solutions and adapting to market trends, the firm has been instrumental in numerous pioneering deals, earning it prestigious accolades such as "Asian Law Firm of the Year" and the "China (PRC Firms) Finance Law Firm of the Year".

Authors

Ye Zhao stands as one of the foremost authorities in intellectual property and antitrust litigation in China. He possesses a wealth of experience in the courtroom, having represented clients in several landmark cases that have shaped the legal landscape of the nation. This includes pioneering cases such as the first anti-suit injunction case in China. His esteemed client roster features a multitude of premier corporations, including Intel, Huawei, and CATL. His innovative legal acumen is marked by his strategic utilisation of a diverse array of legal and policy instruments to address and resolve complex and significant client challenges.



Zhanjiang Zhang is a partner at Jingtian & Gongcheng. He received his PhD in Science from the Chinese Academy of Sciences. He is duly certified both as a Chinese lawyer and patent attorney. His career trajectory includes roles as a patent examiner at SIPO, as a lawyer and patent attorney in three well-known law firms in China, and he has 13 years of practical experience in the intellectual property field.

Contributed by: Ye Zhao, Zhanjiang Zhang and Qiang Ma, **Jingtian & Gongcheng**

Qiang Ma is a distinguished partner at Jingtian & Gongcheng, where he expertly heads the trade mark team. With an extensive academic foundation, he holds an LLB and a JSD from Renmin University, an LLM from Peking University and an LLM from the George Washington Law School. Dr Ma has over two decades of experience in intellectual property law. Specialising in trade mark, copyright, and unfair competition, he is renowned for his adept handling of complex brand protection cases. Acknowledged with multiple accolades, he is celebrated as an IP star. Dr Ma's influential cases have earned recognition in top judicial forums.

Jingtian & Gongcheng

34th Floor, Tower 3
China Central Place
77 Jianguo Road
Chaoyang District, Beijing
100025
PRC

Tel: +86 1391023 5008
Fax: +86 10 5809 1100
Email: ma.qiang@jingtian.com
Web: www.jingtian.com

競天公誠律師事務所
JINGTIAN & GONGCHENG

Overview

In 2023, China continued to uphold its commitment to stringent protection in the realm of trade secrets, striving to maintain fairness in market competition, fuel innovation, enhance the protection of technical secrets, intensify the enforcement of infringement compensations and rigorously apply the punitive damages system. Those concerted efforts unveil China's robust judicial stance on protecting intellectual property legally and uprooting the infringement of trade secrets. This overview will delve into the state-of-the-art trends and the judicial dynamics in China's trade secret sector.

Adjustment to the Appellate Jurisdiction over Technical Secret Cases by the Supreme People's Court

On 1 January 2019, the Intellectual Property Court of the Supreme People's Court ("the IP Court") was officially established, centralising the appellate jurisdiction over technical intellectual property cases nationwide, including those involving technical secrets.

In October 2023, the Supreme People's Court made a strategic adjustment to the jurisdiction of the IP Court. In accordance with the current provisions (Fa Shi [2023]No 10), as of 1 November 2023, appeals on technical secrets, within the jurisdiction of the IP Court, have been refined to cover "significant and complex" disputes over technical secret ownership, civil infringement and administrative decisions. The term "significant and complex" refers to appeals filed against decisions of first-instance cases by the High People's Courts.

Consequently, from 1 November 2023, "ordinary" appeals on technical secret ownership, civil infringement and administrative decisions, not initially tried by the High People's Courts, have reverted to the jurisdictional framework that was in place prior to the establishment of the IP Court in 2019.

Active Procuratorate Initiatives and Escalated Enforcement Against Criminal Infringement of Trade Secrets

Throughout 2023, there was a surge in criminal infringement cases of trade secrets, which were rampant in technology-intensive sectors such as information technology, bio-medicine, advanced manufacturing, and new energy.

In a concerted effort to bolster the criminal judicial protection for intellectual property, the Supreme People's Procuratorate and the Supreme People's Court jointly issued the "Interpretation on Several Issues Concerning the Application of Law in Handling Criminal Cases of Intellectual Property Infringement (Draft for comments)" (the "Draft for comments") in January 2023. The Draft for comments sets forth the threshold for criminal liability in criminal infringement of trade secrets.

In April 2023, the Supreme People's Procuratorate released the "Guidelines on Handling Intellectual Property Cases for People's Procuratorates", introducing 45 prosecutorial actions to provide specific guidance for performing case-handling duties.

Furthermore, in June 2023, the Supreme People's Procuratorate issued the "Opinions on Comprehensively Strengthening the Intellectual Property Procuratorial Work for the New Era" (the "Opinions"). The Opinions highlights enhancing the protection of trade secrets and intensifying the processing efforts for trade secret cases.

These above initiatives underscore that China is steadfast to establishing a pioneering standard

for the prosecutorial protection of intellectual property rights, showcasing the nation's determined approach towards escalating the crackdown on criminal infringement of intellectual property.

Intensified Protection of Trade Secrets and Establishment of the "Mega-Protection" Framework Through Administrative, Judicial, and Industry Collaborations

The Administration for Market Regulation in China leverages the efficient and streamlined framework of the administrative protection for trade secrets, steadfastly focusing on bolstering the oversight and enforcement against trade secret infringements.

Since 2018, the State Administration for Market Regulation has spearheaded nationwide initiatives against unfair competition for six consecutive years. The 2023 campaign, named "Guardian", specifically mandated more stringent safeguards for corporate trade secrets.

In September 2020, the Administration drafted the "Rules on Trade Secret Protection (Draft for Solicitation of Comments)", advancing the legislative agenda for administrative protection for trade secrets.

July 2022 marked the commencement of a national pilot programme for trade secret protection, with a second phase launched in October 2023. These pilot initiatives, prioritising multidimensional and effective mechanisms for trade secret protection, have used targeted efforts to drive a nationwide enhancement in protection standards.

As the Administration for Market Regulation joins hands with judicial and industry regulatory authorities, China is gradually establishing a robust "mega-protection" framework, characterised by the synergy among administrative, judicial and industry protections of trade secrets. Moving forward, China will leverage the systemic strength of the "mega-protection" framework, elevating the overall protection of trade secrets across the nation.

New Directions in Adjudication Principles for Trade Secret Cases: Insights From the Supreme People's Court's Guiding and Typical Cases

On 22 February 2024, the Supreme People's Court unveiled the "Fifth Anniversary of the IP Court: Top Ten Influential Cases and 100 Typical Cases", among which technical secret cases numbered 21, accounting for approximately 20% of the total. A review of the case types adjudicated by the IP Court in 2023 shows 3,222 civil cases are accepted in total, with technical secret cases amounting to 113, representing merely 3.5% of the overall caseload. The proportion of technical secret cases selected as model examples significantly exceeds that of other types of cases. This disparity not only reflects the Supreme People's Court's steadfast commitment to reforming the adjudication rules for technical secret cases within civil litigation but also indicates its intent to bolster technical secret protection. The highlighted cases demonstrate numerous significant shifts from traditional approaches, signalling essential developments.

Recent alterations to the practice of determining the trade secret point

As right-holders file a lawsuit, courts generally require them to clarify the content and boundary of trade secrets, namely by defining "the trade secret point". In cases where a drawing serves as a carrier for the trade secret, courts conventionally conclude that drawings, as the fixed carrier of the technical information, are ineligible

for specifying the exact nature and limits of the technical secret. As a result, the right-holder is mandated to further elucidate the specific element of the trade secret within drawings and define its composition, distinguishing it from the publicly known information. Otherwise, failure to do so may lead courts to conclude that the right-holder's claim doesn't meet the statutory conditions.

In the "Hood-Type Furnace Lifting Device" technical secret infringement case (Docket No: (2022) Supreme People's Court Zhi Min Zhong No 719), the Supreme People's Court has adopted unprecedented approaches for its judgment. In the current context, the right-holder submitted a set of 29 technical drawings, asserting that this entire collection constituted the technical secret. The first-instance court concluded that the right-holder failed to provide the detailed contents of the confidential technical solution or features within the asserted set of drawings. Given the ambiguous nature of the trade secret point within the drawings and the unclear distinction from the publicly known technical information, the court found it unfeasible to affirm the right-holder's claim that the technical information qualified as the technical secret. As a result, the court dismissed his claim. Upon appeal, the Supreme People's Court held an unconventional view, recognising the aggregation of specific technical information within 29 drawings as the technical secret beyond dispute, as the right-holder contended. Therefore, on the grounds of the above claim, the court required a review of the secrecy, value, and confidentiality of the technical information, as asserted by the right-holder.

The judicial perspective revises the traditional view when claiming that technical secrets are based on drawings, the right-holder cannot assert that all the technical information within those drawings constitutes the technical secret.

The trade secret point may correspond to components of a technical solution or the complete technical solution itself. When the trade secret involves a complete technical solution, the right-holder typically documents this solution in a single document carrier. The right-holder is then required by the court to distinguish and clarify information which is not known to the public from those which is publicly accessible. However, in the "Virus Detection Reagents" technical secret infringement case (Docket No: (2020) Supreme People's Court Zhi Min Zhong No 1889), the Supreme People's Court stepped in a different judicial direction. The Court held that the technical secret, namely a technical solution as asserted by the right-holder, could either be a complete solution documented within a single technical file or a solution developed from a reasonable summary, generalisation, and refinement of technical information which is not known to the public, across various technical documents. Right-holders are encouraged to integrate their confidential information with the prior art and common knowledge, forming a complete technical solution for protection, when summarising, generalising, and refining confidential information from their technical documents.

The above judicial stance has revised the prevailing belief that there must be a direct match between the carrier of the technical secret and its corresponding technical solution. Furthermore, it updates the standard practice of excluding publicly known information from the overall technical solution when determining the trade secret point.

Easing the burden of proof for the right-holder and establishing reasonable inference of infringements

To address challenges that right-holders face in providing evidence, the 2019 revision of the Anti-Unfair Competition Law, particularly Article 32, redefines the apportionment of the burden of proof between the right-holder and the accused infringer. This article was initially hailed as a crucial move to ease the burden of proof. Nonetheless, its implementation in legal practice has ignited significant controversy. The vagueness of phrases such as "preliminary evidence" and "reasonably indicates" has resulted in inconsistent judicial interpretations, making it challenging for right-holders to discern the extent of evidence required to satisfy the initial burden of proof and trigger a shift in this burden to the accused infringer.

Taking the determination of technical secret infringement as an example, it is common for infringers to conduct their business covertly. As a result, the secretive nature significantly hinders the right-holder's ability to produce evidence substantiating the actual use of the contested technical secret by the infringer.

In the "Vanillin" technical secret infringement case (Docket No: (2020) Supreme People's Court Zhi Min Zhong No 1667), disputed technical secrets were recorded in the carrier of 287 equipment drawings and 25 process flow diagrams for piping and instrumentation. The accused infringer unlawfully accessed 185 of these equipment drawings and 15 process flow diagrams. The difficult and focal point hinged on proving the accused infringer employed the implicated technical secrets in actual use. During the appeal, the Supreme People's Court invoked the obstruction of justice guideline and best evidence rule. Given the established facts and the right-holder's claim that the accused infringer had illicitly acquired full details of the product's process flow and entire production equipment data, thus proceeding to manufacture identical products, the court reasonably inferred the accused infringer's use of the entire technical secrets involved.

The above judicial viewpoint underscores that infringements of technical secrets can be inferred on the grounds of circumstantial evidence. According to the specific circumstances or established facts and common knowledge, the right-holder is eligible to substantiate that the accused infringer has improperly acquired, disclosed, or used technical secrets by virtue of circumstantial evidence. This case reflects a judicial approach that pioneers in addressing the challenge of producing evidence for the protection of technical secrets in a practicable manner.

Practicable enhancement of the infringement compensation and rigorous implementation of the punitive damages system

The "Melamine" invention patent and technical secrets infringement case resulted in a landmark award of CNY218 million (Docket Nos: (2020) Supreme People's Court Zhi Min Zhong No 1559 and (2022) Supreme People's Court Zhi Min Zhong No 541). Both parties reached a comprehensive settlement during the enforcement phase, with the right-holder ultimately securing CNY658 million, thereby setting a precedent in China's intellectual property rights enforcement history. The "Rubber Antioxidant" technical secret infringement case led to a compensation of CNY202 million (Docket No: (2022) Supreme People's Court Zhi Min Zhong No 816), applying the maximum judicial penalty to the company and its actual controllers for non-compliance with a preservation order. Moreover, in the "Vanillin" technical secret infringement case,

damages were set at CNY159 million, with the company's legal representative fully holding joint and several liability. These cases underline the Chinese courts' dedication to stringent intellectual property protection and their determination to intensify penalties for infringements.

The 2019 revision of the Anti-Unfair Competition Law has incorporated the punitive damages system. Over recent years, the Chinese judiciary has been proactively applying this framework.

Notably, the "Cabot" technical secret infringement case (Docket No: (2019) Supreme People's Court Zhi Min Zhong No 562) was recommended as the 219th guiding case in the 39th batch issued by the Supreme People's Court in 2023. This case is a pioneering example of the IP Court's application of punitive damages. During the appeal, the Supreme People's Court concluded that the accused infringer, who was guilty of deliberate and direct infringement, made the infringement his profession, characterised by an extensive scale, prolonged duration, substantial profit, and obstruction of justice, warranting the maximum fivefold punitive damages. This case represents a crucial step in correlating the severity of the infringement with the punitive damages multiplier, significantly contributing to the precise and effective application of the punitive damages system for intellectual property rights infringement.

GERMANY

Law and Practice

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

Contents

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

SZA Schilling, Zutt & Anschütz (SZA) has been one of the most reputable German law firms for almost a century. With more than 120 attorneys, it advises domestic and international clients in all areas of corporate and commercial law. The IP/IT department of SZA is located in Mannheim and Frankfurt and currently practises with ten attorneys in all areas of IP and IT, as well as data protection law. With the establishment of its Asia desk, SZA provides consultation for Asian 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 trademarks, designs, patents and trade secrets. 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 Asia.

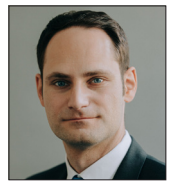
Authors

Thomas Nägele is a partner at SZA Schilling, Zutt & Anschütz, specialising in intellectual property, trademarks and unfair competition, patent litigation, IT, cybersecurity and data protection; he also 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 counsel at SZA Schilling, Zutt & Anschütz, specialising in copyright law, unfair competition law, law of trade secrets, trademark law, IT law and litigation. He is a member of the Deutsche Vereinigung für gewerblichen Rechtsschutz und Urheberrecht (GRUR) e.V and sits on its Data and the Law Committee. He has authored or co-authored over 90 publications, particularly in the field of copyright law, unfair competition law, trademark law and trade secrets law; he is co-editor and co-author of a commentary on the German Trade Secret Act.

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

Jonathan Drescher is a senior associate at SZA Schilling, Zutt & Anschütz. His practice covers copyright, unfair competition law, trademark and design law, trade secret law, IT law, media law and litigation. He has made several contributions to German law journals, particularly in the field of trade secrets law, and is co-author of a commentary on the German Trade Secret Act.



Alexander Stolz is a principal associate at SZA Schilling, Zutt & Anschütz, specialising in copyright, patent law, trademark law, IT law, media law and litigation. He is a lecturer for civil law at Duale Hochschule Baden-Württemberg and has made several contributions to German law journals, particularly in the field of trade secrets law and data privacy law. He is co-author of a commentary on the German Trade Secret Act.

SZA Schilling, Zutt & Anschütz

Otto-Beck-Strasse 11
D-68165 Mannheim
Germany

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

SZA SCHILLING, ZUTT & ANSCHÜTZ

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 (Directive (EU) 2016/943) (the "EU Trade Secrets 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 seq) and the legal consequences of an infringement (Section 6 et seq). Furthermore, it establishes specific rules to protect trade secrets in (civil law) litigation (Section 15 et seq) and stipulates certain conduct regarding trade secrets as a criminal offence (Section 23).

While the TSA is the main act with regard to trade secrets, there are several provisions throughout different acts of German law that may provide supplementary 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 seq of the German Criminal Code (GCC) (*Strafgesetzbuch,* or StGB)), the integrity of electronic data (Section 202a et seq, GCC) or postal and telecommunications secrecy (Section 206, GCC) – 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
- information where the fact itself (eg, a particular process) is not secret, but the company that uses the process 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 at all is not covered by the protection of 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, in the authors' opinion, 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 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 it 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, which came 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), as set out below.

- 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.
- 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. While more and more court decisions regarding the question of how much effort is required for qualifying the steps taken as the required level of reasonableness have already been rendered, this question 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. As some of the first courts seem to follow this view, it is strongly recommended to conclude appropriate NDAs (this also applies to third parties who get access to 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 controlled 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 and can go up to imprisonment for up to five years or a fine, 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. 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 their 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 competition 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 relation to the first opinion (above) 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.

2. Misappropriation of Trade Secrets

2.1 The Definition of Misappropriation

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

The first is the unlawful acquisition of the secret. A trade secret shall not be obtained 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; or
- any other conduct that, under the circumstances, is considered contrary to honest commercial practices.

This 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 variant 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 not entirely clear due to relatively few court decisions (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, as of yet only few court decisions have been rendered on this subject and for "best practices" one should 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 (see **1.5 Reasonable Measures**).

Organisational Measures

The basis of a know-how protection concept is always an analysis of the requirements for protection, in which the information that needs to be kept secret is defined. It is recommended that the information be classified as "secret", "confidential" and "openly accessible" and that clear rules for handling classified information are established. 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). 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 in the risks of espionage. Finally, measures to increase employee commitment to the company can help prevent employees from disclosing secrets.

Technical Measures

These include IT security measures – for example, firewalls, password protection, virus scanners, encryption of data carriers, network con-

nections 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 their general knowledge and acquired skills, whereas factual knowledge (eg, the composition of a specific product or customer lists) is solely assigned to the employer. 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 imposed (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 arises 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 that the court 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. This requires the claimant to convince the court of their claim up to a point where the court does not have any reasonable doubts.

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 judgment. 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 benefit 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, these special protection measures only apply if the claim is based on a trade secret infringement and, in principle, may not be applied in other civil proceedings (even if a trade secret may need to be disclosed).

Furthermore, 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. However, 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 – eg, 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, 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 their 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 shall usually 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 approximately 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 the experts 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 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 the following 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 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. Ultimately, however, 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 lawyers' fees, 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 longer, depending on the complexity of the case. Further extensions require the consent of the other party. The Higher Courts of Appeal review the case on points of law and with regard to the facts. With regard to the latter, they enjoy a considerable degree of discretion as 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 on points of law.

At the first appellate level, as a general rule, the duration of the proceedings will usually take at least six 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

At 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 pre-

sumptions 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 third party's trade secret. However, if the perpetrator defends themselves by saying that they 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 them – 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 (ADR)

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.

The parties are then free to agree on the language used in the arbitral proceedings, the place of arbitration, 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, particularly 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.

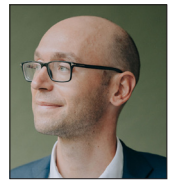
Trends and Developments

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

SZA Schilling, Zutt & Anschütz (SZA) has been one of the most reputable German law firms for almost a century. With more than 120 attorneys, it advises domestic and international clients in all areas of corporate and commercial law. The IP/IT department of SZA is located in Mannheim and Frankfurt and currently practises with ten attorneys in all areas of IP and IT, as well as data protection law. With the establishment of its Asia desk, SZA provides consultation for Asian 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 trademarks, designs, patents and trade secrets. 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 Asia.

Authors

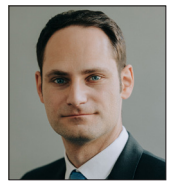
Thomas Nägele is a partner at SZA Schilling, Zutt & Anschütz, specialising in intellectual property, trademarks and unfair competition, patent litigation, IT, cybersecurity and data protection; he also heads the IP/IT department. He is a lecturer at the University of Heidelberg and a member of numerous 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 counsel at SZA Schilling, Zutt & Anschütz, specialising in copyright law, unfair competition law, law of trade secrets, trademark law, IT law and litigation. He is a member of the Deutsche Vereinigung für gewerblichen Rechtsschutz und Urheberrecht (GRUR) e.V and sits on its Data and the Law Committee. He has authored or co-authored over 90 publications, particularly in the field of copyright law, unfair competition law, trademark law and trade secrets law; he is co-editor and co-author of a commentary on the German Trade Secret Act.

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

Jonathan Drescher is a senior associate at SZA Schilling, Zutt & Anschütz. His practice covers copyright, unfair competition law, trademark and design law, trade secret law, IT law, media law and litigation. He has made several contributions to German law journals, particularly in the field of trade secrets law, and is co-author of a commentary on the German Trade Secret Act.



Alexander Stolz is a principal associate at SZA Schilling, Zutt & Anschütz, specialising in copyright, patent law, trademark law, IT law, media law and litigation. He is a lecturer for civil law at Duale Hochschule Baden-Württemberg and has made several contributions to German law journals, particularly in the field of trade secrets law and data privacy law. He is co-author of a commentary on the German Trade Secret Act.

SZA Schilling, Zutt & Anschütz

Otto-Beck-Strasse 11
D-68165 Mannheim
Germany

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

SZA SCHILLING, ZUTT & ANSCHÜTZ

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

Five Years of the TSA: Relevant Changes to the Protection of Trade Secrets in German Law

Almost five years have passed since the EU Trade Secrets Directive (Directive (EU) 2016/943) (ETSD) was implemented into German law in the form of the German Trade Secret Act (*Gesetz zum Schutz von Geschäftsgeheimnissen, GeschGehG* – the TSA), changing the legal protection of trade secrets from a criminal law-centric system to a dedicated law for the protection of trade secrets, which is dominated by a civil law concept.

It is no surprise that such a paradigm has led to considerable uncertainty among courts, legal practitioners and companies alike. While the legal literature initially took some time to take serious note of the TSA, in recent years more and more articles have appeared dealing with various facets of the TSA – including the correct draft of non-disclosure agreements, "best practices" for company know-how protection systems and the impact of the TSA on employment contracts.

Several court decisions on the TSA have also been issued, dealing mainly with the question of what requirements must be fulfilled in order to ensure "appropriate confidentiality measures" for information to be protected as trade secrets and the use of trade secrets by former employees. Further changes are also on the horizon at the legislative level. According to a key issues paper from 2023, German lawmakers are planning to extend the provisions on the confidentiality of trade secrets in court proceedings, which have so far only been contained in the TSA, to general civil procedure law.

The purpose of this article is to shed some light on some of the most relevant changes which the TSA has brought to German law on the protection of trade secrets, to highlight relevant court decisions and recent legislative action in this context.

Secrecy and Economic Value

Protection under the TSA is only granted to information that is neither generally known nor otherwise readily accessible. This raises the question of how many people need to have knowledge of an information for it to be "generally known" and no longer a trade secret. To this regard, the Higher Regional Court of Dresden and the State Labor Court of the state of Baden-Württemberg found that access to a trade secret of only a small group of persons is not enough to qualify as "general knowledge". Therefore, an information may still qualify as a trade secret if such information was passed on to the parties involved in a legal dispute as part of court proceedings or if only a certain group of employees within a company has access to information. However, in both cases the group of person with access to the trade secret could be identified from records, which means that the decisions may have been different in cases where there are spectators in the court room or the employees in question can no longer be individually identified.

The protection as a trade secret under the TSA also requires the information having commercial value. The Dresden Higher Regional Court clarified that information does not have a commercial value simply because it is kept secret but that economic value is rather a separate element. It is required that a piece of information has an actual or future market value or that it can influence the financial or commercial interests of an enterprise. While there is no specific value limit or de minimis threshold for "economic value", in the case at hand, the plaintiff could not prove that information on holiday leave taken by employees

of a company has any commercial value, as it did not allow any conclusions to be drawn about the number of employees or the company's holiday or salary structure. However, it needs to be emphasised that the question of whether information has a commercial value can only ever be answered by a case-by-case assessment.

Appropriate Confidentiality Measures

Information can 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". This means that in the event of a legal dispute, the owner of a trade secret must prove that appropriate security measures to protect confidentiality were taken with regard to the secret in question.

However, neither the TSA nor the underlying ETSD provide an answer to the question of what is "appropriate" in this context. With view to this legal uncertainty, it does not come as a surprise that by far the largest part of the court decisions issued since the TSA came into effect – and most scholarly contributions on the subject of trade secret protection – dealt with the issue of appropriate confidentiality measures.

One of the most detailed decisions concerning this issue was issued by the Schleswig Higher Regional Court in 2022. In this decision, the Court evaluated the underlying legal acts, the official rationale by the German government and scholarly contributions, and found that "adequate" protection does not require the best possible protection. Rather, the type and scope of measures depend on the significance of the information for the company. This approach has now become standard in case law as more and more courts follow it. As such, the Schleswig Higher Regional Court referred to a three-level classification, distinguishing between top secret (the "crown jewels" of information, the disclosure of which would threaten the existence of the company), important (information the disclosure of which could cause a permanent economic disadvantage) and sensitive information (information the disclosure of which could cause a short-term economic disadvantage).

After having determined the level of secrecy for the information in question, the Schleswig Higher Regional Court discussed whether the measures taken by the owner of the secret were appropriate. Since only trade secrets of relatively minor importance, which were created as a result of a one-off incident, were affected in the case, even minor secrecy measures were deemed to be sufficient for trade secret protection, such as TLS email encryption and the appropriate selection of a group of persons permitted to have knowledge of the secret (a "need to know"-basis). As the owner had provided such measures, the information was considered a trade secret. The fact that the non-disclosure agreement may have been invalid made no difference because the court also found that the ineffectiveness of a confidentiality clause does not automatically rule out the protection as a trade secret if other protection instruments compensate for this omission.

In 2023, the Higher Regional Court of Dresden emphasised that protective measures need not only prevent unauthorised access from the outside, but that measures with respect to the company's own employees are also necessary. According to the Baden-Württemberg Higher Labour Court, technical organisational precautions can qualify as appropriate confidential measures, for example in the form of access, entry and availability controls to secure data processing as well as the documentation of infor-

mation retrieval. This also includes the creation of a data protection manual and technical and legal requirements, eg, employment contract provisions on confidentiality or the agreement of obligations to hand over documents immediately.

As can be seen from the decisions referred to above, legal certainty is increasing. However, as long as the Court of Justice of the European Union (CJEU) has not decided under the ETSD which steps need to be taken to ensure the required level of reasonable protection measures, many details (eg, on the validity of so-called catch-all clauses and the proper design of non-disclosure agreements) are still unclear, controversial and the subject of lively discussion. It can be assumed that this question will continue to be one of the dominant issues in the future. Such a future decision of the CJEU will also be binding on the German courts when applying the TSA.

Scope of Application of the TSA

Several decisions have dealt with questions relating to the scope of application of the TSA, primarily regarding the temporal scope of application and the question of whether the statutory definition of the term "trade secret" (and the associated need to maintain appropriate confidentiality measures) also applies in other areas of law. For example, some provisions of commercial and corporate law, as well as public law, still refer to the outdated term of "business and trade secrets". The Federal Administrative Court considered that the definition of a trade secret as laid out in the TSA also applies with regard to secret information in public law proceedings. The Higher Administrative Court of the Federal state of Nordrhein-Westfalen also referred to the definition of the TSA for guidance when interpreting a public law provision of cartel law. In civil law, the Düsseldorf Higher Regional Court ruled that the requirements stipulated by the TSA do not apply when deciding on the disclosure of a written expert opinion within the framework of independent proceedings for taking evidence.

Furthermore, the Düsseldorf Higher Regional Court found that orders for the protection of trade secrets stipulated in the TSA cannot be considered if the claims asserted are not based on infringement of a trade secret; however this may change in the future due to changes in the legislative framework (see below, Confidentiality in Civil Proceedings).

Third-Party Liability and Legal Consequences

The TSA significantly extended third-party liability under former German law on trade secrets, the use or disclosure of a trade secret by a third party in a merely negligent misjudgment of a prior breach of secrecy was no infringement.

Under the TSA, the acquisition, use or disclosure of a trade secret is also considered to be 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 (i) the production, offering or placing on the market of infringing goods, or (ii) 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 for recall or removal of secret-infringing goods 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.

In contrast, the TSA allows for claims of the trade secret owner for recall and removal of infringing products, whereby even those products which 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 combination of these options 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 when manufacturing products 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 – regardless of whether this person has knowledge of the secret or whether it is embodied in the product itself.

On the other hand, however, there is now a significant risk that third parties may get caught in the "undertow" of a breach of secrecy through no fault of their own, which results in substantial liability risks. Particularly the recall and destruction of infringing products can be very problematic because while the manufacture and distribution of products are often long-term and require a long preparation phase, the required knowledge, by contrast, can also be obtained subsequently simply from a respective notification from the trade secret owner. Therefore, as soon as the trade secret owner notifies the "indirect offender" of the unlawful nature of its conduct, the latter may no longer manufacture or distribute the products to avoid a conflict with the trade secret owner.

Confidentiality in Civil Proceedings

Another major issue addressed by the TSA concerns confidentiality in civil proceedings. The owner of a trade secret asserting claims under the TSA must demonstrate and prove that the information in question is a trade secret. Therefore, the content of the trade secret will 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 such a case, the owner of the secret would lose both the secret and the lawsuit since the trade secret lacks the required secrecy.

Although the owner of a trade secret could apply for the public to be excluded from a court hearing under former German law, the decision to do so was subject to the courts' reasonable discretion – and the courts were very reluctant in this matter, as the publicity of court proceedings enjoys high priority under German law. The TSA has considerably mitigated this issue by providing additional instruments to exclude 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 do not only apply 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 confidentiality obligation on the opposing party (punishable by a fine), this only prohibited the disclosure of the information, but did neither provide pro-

tection against the opposing party's own use nor against negligent disclosure of the secret.

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 suit to the taking of evidence in the oral proceedings to the pronouncement of judgment throughout the entire infringement proceedings.

This problem has been partially mitigated by the TSA. The trade secret owner cannot only prohibit the opposing party from using the secret, but 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.

Although the TSA's provisions on secrecy in civil proceedings represent a step forward, they are not (yet) entirely sufficient. On the one hand, a restriction to use or disclose 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. 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 regrettable 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 and that the courts seem reluctant to apply these provisions outside of the TSA.

It is therefore a welcome development that the German Federal Ministry of Justice (FMJ), after having already extended the confidentiality provisions of the TSA to patent proceedings, according to the Key Issues Paper on Strengthening the Courts in Commercial Disputes and the Introduction of Commercial Courts dated 16 January 2023, plans to further extend and apply them to all civil law proceedings. Furthermore, the protection of trade secrets shall begin at the time at which the lawsuit is filed and information classified as confidential is not only not to be disclosed outside of legal proceedings but is also not to be used. This proposal is currently under discussion in parliament (in the German *Bundestag*), while the federal states (in the so-called *Bundesrat*) have not yet objected to the proposal.

Former Employees and the Allocation of Know-How

While the TSA has led to numerous changes and significant improvements in the protection of trade secrets under German law, there are some issues that the TSA does not address. Apart from the question of which criteria should be used to assess the value of a trade secret, this concerns in particular 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 trade secrets, whose ownership remains with the employer. In practice, however, this differentiation has almost exclusively been based on whether the employee had to have access to

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 allowed to use it).

In one of the first decisions on this subject under the TSA, the Düsseldorf Labour Court continued to apply this schematic distinction and ruled that an employee who has left the company may use trade secrets that they have acquired in the course of their work without restriction, even to the detriment of their former employer, if and to the extent they reproduce them from their memory. However, this does not include information which is only known to them because they can extract it from documents which they have drafted during the employment period, including documents that are still available to them, eg, in the form of private records or a file stored in a private notebook.

It remains to be seen whether other courts and most importantly the CJEU will also 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 more 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 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 of experience and skills honestly acquired in the normal course of their employment".

In a decision that was more differentiated according to considerations mentioned above, the Karlsruhe Higher Regional Court dealt with a former employee who conducted research on customer satisfaction after the end of their employment relationship and used customer data (and thus trade secrets of his former employer) for this purpose. The court found that such use violates the post-contractual duty of loyalty and violates the TSA because the former employee's enquiries with the employer's customers could cause irritation among the latter, which could possibly have an impact on the customers' trust in the employer.

An Important Step Forward

Altogether, the protection for trade secret owners in Germany has improved significantly since the TSA came into force and this protection is further substantiated with each court decision. Even if the TSA does not provide solutions for all problems and there are still challenges remaining for practitioners, the provision of largely uniform Europe-wide protection of trade secrets is an important and overdue step forward.

INDIA

Law and Practice

Contributed by:
Pravin Anand, Achuthan Sreekumar and Rohil Bansal
Anand and Anand

Contents

Anand and Anand is a full-service intellectual property law firm, providing all-round IP solutions; its forte is developing new law and precision-navigation of grey areas. Its principal office is in New Delhi, with other offices in Noida, Mumbai and Chennai. The firm provides a comprehensive IP service encompassing protection, enforcement, advisory, licensing and litigation for patents, designs, trade marks, copyrights, trade secrets, domain names, geographical indications and more. Credited with lawsuits that have transformed the IP landscape in India, the firm's litigation arm has decades of unmatched experience in dispute resolution. It has maintained a patent grant rate of over 93%, while its trade mark team recently recorded over 1,800 successful trade mark oppositions.

Authors

Pravin Anand is Anand and Anand's managing partner and head of litigation. Presented with the AIPPI Award of Merit and INTA's President's Award, and recognised as the "Most Innovative Lawyer" for Asia-Pacific by the Financial Times, Pravin has appeared in more than 3,000 cases in over 43 years' practice as an IP lawyer. He has been involved in lawsuits transforming the Indian IP enforcement regime, and has engendered many original facets of IP, including trade secrets. He is the author of "Halsbury's Laws of India on Intellectual Property" and the India chapter in "Trade Secrets Throughout the World", and engages extensively in spreading the message of IP through the Raj Anand Moot Court Competition.

Achuthan Sreekumar is a partner in Anand and Anand's litigation department. He started his career at Anand and Anand in 2008, handling matters involving traditional IP such as trade marks, copyrights and patents, as well as borderline IP issues such as trade secrets, tortious issues, hyperlinking, spamming, defamation and IT. Over the past few years, he has focused on expanding his practice areas to a range of subjects, including white-collar and IP crime. He represents several business conglomerates and individuals who have faced issues in these areas and has obtained favourable results on their behalf. He also specialises in formulating strategies, interfacing and following up with relevant governmental and other authorities.

Rohil Bansal is an associate with over three years of litigation experience in core and complex aspects of IP. He started his career with Anand and Anand in 2021, and has since handled matters involving traditional IP trade marks, copyrights, patents, etc. Rohil has also been involved in a wide array of matters related to white-collar crime, arbitration and civil disputes. He has a BBA LLB (Hons) from the National Law University, Jodhpur.

Anand and Anand

B-41, Nizamuddin East
New Delhi 110013
India

Tel: +91 120 4059300
Email: email@anandandanand.com
Web: www.anandandanand.com

ANAND & ANAND

1. Legal Framework

1.1 Sources of Legal Protection for Trade Secrets

The Indian legal system follows a common law system based principally on customs, precedents and legislation. India does not have a specific statute or Act for protecting trade secrets. Trade secrets are protected through a series of precedents and legislation comprising various laws, such as:

- the Patents Act, 1970;
- the Trade Marks Act, 1999;
- the Copyright Act, 1957;
- the Designs Act, 2000;
- the Geographical Indications of Goods (Registration and Protection) Act, 1999;
- the Plant Variety Protection and Farmer's Rights Act, 2001;
- the Biodiversity Act, 2002;
- the Semiconductor Integrated Circuits Layout Designs Act, 2000;
- the Information Technology Act, 2000;
- the Indian Contract Act, 1872;
- the Competition Act, 2002; and
- the Indian Penal Code, 1860 (with effect from 1 July 2024, this will be known as Bharatiya Nyaya Sanhita).

Being a signatory to the TRIPS Agreement, India is obligated under Article 39 to protect "undisclosed information". Further, as Article 10bis of the Paris Convention and Article 39(2) to 39(3) of the TRIPS Agreement allows member states to have sui generis mechanisms, Indian courts have availed of common law principles to protect such "undisclosed information".

The National IPR Policy, 2006 states in Objective 3.8.4 that protection of trade secrets is pivotal for strong and effective intellectual property (IP) laws to balance the interests of rights-owners with larger public interest.

Trade secrets have been protected through various means, such as:

- constitution of confidentiality clubs;
- non-disclosure agreements; and
- other contractual obligations.

In the case of breach of such contractual agreement, the owner of trade secrets can bring an action for (among others):

- specific performance;
- the tort of misappropriation under common law;
- criminal breach of trust;
- theft; and
- damages.

Therefore, trade secrets have been given the status of an equitable right. In Pawan Kumar Goel v Dr Dhan Singh and Another, CS (COMM) 672/2022, the Delhi High Court held that formation of a confidentiality club is necessary to facilitate access to commercially sensitive documents/information, as this is an effective approach for sharing sensitive information (such as a defendant's trade secrets) while addressing confidentiality concerns.

The Indian government has been taking various measures to protect trade secrets, personal data, etc, while clearly noting the economic loss that can result from its leakage and misuse. In early August 2023, the Indian Parliament passed the Digital Personal Data Protection (DPDP) Act, 2023. The new law is the first cross-sectoral law on personal data protection in India.

1.2 What Is Protectable as a Trade Secret

Whether certain information constitutes trade secrets depends on the facts of each case. For information to be given protection as a trade secret, it should be confidential in nature and should not be in the public domain.

To protect certain information as confidential, the following conditions should be met, as held in Beyond Dreams Entertainment v Zee Entertainment Enterprises (2016) 5 Bom CR 266:

- the information must be confidential;
- it must have been disclosed in circumstances from which an obligation of confidentiality arises; and
- the confidant should be attempting to use or disclose the information.

Black's Law Dictionary, 8th Edition defines trade secrets as a "formula, process, device, or other business information that is kept confidential to maintain an advantage over competitors; information including a formula, pattern, compilation, program, device, method, technique or process […] that derives independent economic value, actual or potential, from not being generally known or readily ascertainable by others who can obtain economic value from its disclosure or use, and […] that is the subject of reasonable efforts, under the circumstances, to maintain its secrecy".

The above definition was relied on by the Calcutta High Court in Tata Motors v State of WB; WP No 1773 of 2008.

In Burlington Home Shopping v Rajnish Chibber; 1995 PTC (15) 278, the Delhi High Court held that a trade secret is information that would cause real or significant harm to the owner if disclosed to a competitor. This was also upheld in Linde v Kerr (1991) 1 All ER418. Therefore, trade secrets include not only secret formulae of product manufacturing, but also, in appropriate cases, the names of customers and the goods which they buy.

In Seager v Copydex (1967) 1 WLR 923, the court noted that "the essence of this branch of the law, whatever the origin of it may be, is that a person who has obtained information in confidence is not allowed to use it as a spring-board for activities detrimental to the person who made the confidential communication, and spring-board it remains even when all the features have been published or can be ascertained by actual inspection by any member of the public".

In LifeCell International v Vinay Katrela; 2020 SCC OnLine Mad 15343, the Supreme Court referred to the decision in Hi-Tech Systems v Suprabhat Ray; [2015 SCC OnLine Cal 1192], to hold that whether certain information is confidential is dependent on several factors.

In Saltman Engineering v Campbell Engineering, reported at (1963) 3 All ER 413, the Court of Appeal held that the "confidential" information:

"[M]ust not be something which is public property and public knowledge. On the other hand, it is perfectly possible to have a confidential document, be it a formula, a plan, a sketch, or something of that kind, which is the result of work done by the maker on materials which may be available for the use of anybody; but what makes it confidential is the fact that the maker of the document has used his brain and thus produced a result which can only be produced by somebody who goes through the same process. A trade secret or a business secret may relate to a financial arrangement [or] the customer list of

a trader and information in this regard would be of a highly confidential nature as being potentially damaging if a competitor obtained such information and utilised [this] to the detriment of the giver of the information. Business information such as cost and pricing, projected capital investments, inventory marketing strategies and a customer's list may qualify as his trade secrets. Similarly, business information, such as cost and pricing, projected capital investments, inventory marketing strategies and a customer's list may also qualify as trade secrets."

In Navigators Logistics v Kashif Qureshi; 2018 SCC OnLine Del 11321, the court, referring to Star India v Laxmiraj Seetharam, 2003 SCC OnLine Bom 27, held that everyone in any employment for a certain period would know certain facts and information without any special effort; such persons cannot be said to know trade secrets or confidential information, and knowledge of such facts cannot be labelled as trade secrets.

In Ambiance India v Naveen Jain; 2005 SCC OnLine Del 367, it was stated that written day-to-day affairs of employment that are in the knowledge of many and are commonly known to others cannot be called trade secrets. It was further held that in a business house the employees discharging their duties come across so many matters, but all these matters are not trade secrets or confidential matters or formulae, the divulgence of which may be injurious to the employer; and if an employee on account of employment has learned certain business acumen or ways of dealing with the customers or clients, this does not constitute trade secrets or confidential information.

In Konrad Wiedemann v Standard Castings; [1985] (10) IPLR, the court relied on the observations in the *Saltman Engineering* case to note that:

"The information to be confidential must, I apprehend, apart from contract, have the necessary quality of confidence about it, namely, it must not be something which is public property and public knowledge. On the other hand, it is perfectly possible to have a confidential document, be it a formula, a plan, a sketch or something of that kind, which is the result of work done by the maker upon materials which may be available for the use of anybody; but what makes it confidential is the fact that the maker of the document has used his brain and thus produced a result which can only be produced by somebody who goes through the same process."

In Indian Farmers Fertiliser v Commissioner of CE; 2007 (116) ECC 95, the tribunal defined a trade secret as follows:

"A trade secret is such sort of information, which is not generally known to the relevant portion of the public, that confers some sort of economic benefit on its holder and which is the subject of reasonable efforts to maintain its secrecy."

In Bombay Dyeing v Mehar Karan Singh; 2010 (112) BomLR375, the Bombay High Court held that for information to be classified as a trade secret, the following factors may be considered:

- the extent to which the information is known outside the business;
- the extent to which it is known to those inside the business – ie, by employees;
- the precautions taken by the holder of the trade secret to guard its secrecy;
- the savings affected and the value to the holder in having the information against competitors;

- the amount of effort or money expended in obtaining and developing the information; and
- the amount of time and expense it would take others to acquire and duplicate the information.

Recently, in HCL Technologies v Sanjay Ranganathan, order dated 27 July 2023 in CS (COMM) 502/2023, a former employee of the plaintiff copied certain information, which was personal and confidential to the plaintiff, into his own personal Gmail account. The court took a prima facie view that an employee of a company has no business to transfer into his personal account any data of the company without the company's permission. If such practice is permitted and issues of confidentiality are thereafter sought to be raised, this could be seriously prejudicial to the functioning of corporate enterprise.

Furthermore, in Rochem Separation Systems v Nirtech Pvt Ltd; Commercial IP Suit L No 29923/2022, the Bombay High Court passed an order dated 30 March 2023 stating that there has to be clear-cut, specific descriptions and data with the court pertaining to the information in which the plaintiff claims confidentiality. In the absence of such clear-cut information and material, furnished by the plaintiff before the court, there would be no basis for examining the allegations levelled against the defendants, owing to the fact that the plaintiff had not placed on record the specifics of the confidentiality before the court.

1.3 Examples of Trade Secrets

Please see **1.2 What Is Protectable as a Trade Secret**.

1.4 Elements of Trade Secret Protection

There is no codified law in India defining the elements of trade secret protection. The *Bombay Dyeing* case (supra) identifies the elements essential for information to be classified as a trade secret, as detailed in **1.2 What Is Protectable as a Trade Secret**.

Various case laws have unanimously laid down that the quality of confidentiality makes the information eligible for legal protection as a trade secret. It is very important for the owners of confidential information to show that reasonable efforts were expended by them to maintain secrecy. If such efforts cannot be proved, the owners risk losing the quality of confidence even if such information is obtained by third parties without permission.

An important element for confidential information to be categorised as a trade secret is an obligation on any other person who receives it to maintain its secrecy, if they have received it with the knowledge of obligation of confidence.

1.5 Reasonable Measures

It is important for the owner of a trade secret to show that they took reasonable measures to maintain secrecy regarding such information. Trade secrets are protected in India either under contract law or through the equitable doctrine of breach of confidentiality, by way of:

- restrictive covenants;
- non-disclosure agreements; and
- other contractual means.

In Navigators Logistics v Kashif Qureshi; CS(COMM) 735/2016, the Delhi High Court rejected the claimant's claim and complaint as it did not clearly identify the trade secret in issue, the secrecy regarding such data and what steps (apart from the secrecy clauses under the appointment letters with the defendants) the plaintiff took to maintain secrecy/confidentiality.

Additionally, trade secrets can be protected by an action against misappropriation under common law. Misappropriation of trade secrets may occur by way of breach of an obligation of confidence (whether arising impliedly or expressly) as well as by theft.

The parameters for determining whether the rights-owner of a trade secret has taken reasonable measures for protection of their trade secret vary from case to case. While there is no "straight jacket" formula, the following are a few illustrative measures a rights-holder can adopt.

It is reasonable for owners of trade secrets to insert clauses into a technology transfer or other licence agreement, stating that the technology transferred is of a confidential nature and that the licensee is obligated to maintain confidentiality, during the pendency as well as after its termination.

Moreover, the owner may mandate the licensee to enter into appropriate secrecy agreements with their employees, sub-contractors and visitors to their factory, to maintain secrecy about such trade secrets. Owners of trade secrets may even insert a cautionary notice into all technical manuals clearly stating that the information contained therein is of a proprietary and confidential nature.

However, an ex-employee cannot be prohibited from divulging or using their skill set for a competitor of the owner of a trade secret. In *Ambience India*, the High Court of Delhi held that day-to-day affairs of employment in the knowledge of many and commonly known to others cannot be called trade secrets.

1.6 Disclosure to Employees

Disclosure of a trade secret to employees does not mean the information has lost confidentiality. The presence of a non-disclosure agreement with the employees is not a mandatory requirement for protecting the owner's rights in a trade secret. This is judged from the facts and circumstances of each case.

Trade secrets are protected, irrespective of contract, against misuse by the employees or ex-employees, contractors or sub-contractors, licensees or ex-licensees. The case of *Konrad Wiedemann* states that trade secrets are protected against misuse by any party who may have a relation with the claimant, irrespective of contract, based on the broad principles of equity.

In Hi-Tech Systems v Suprabhat Ray (supra), the High Court of Calcutta held that a principal – in order to protect the utilisation of trade secrets and to prevent damage, if it cannot be compensated in money – can seek restrictions on its agents. In such a situation, equity would step in and prevent any damage from being caused to the business of the principal.

Nonetheless, the owner of such trade secret or a licensee is expected to take all reasonable measures to maintain secrecy, and to ensure that such confidential information is imparted to their employees in circumstances importing an obligation of confidence on them as well.

1.7 Independent Discovery

If a discovery can be proved as independent, a previously existing trade secret having some connection with such discovery will be inconsequential. Needless to say, if the claimant shows mala fides on the part of the defendant and proves that the defendant had access to

the claimant's trade secret – and therefore that the discovery, rather than being independent, is a product of reverse engineering – the court will not accept the respondent's claims and may hold the respondent guilty of misappropriating the claimant's trade secret.

Also, such a process will have to stand the test of trial, and courts will see whether or not the means adopted by the defendant were bona fide and honest. Firstly, the court will examine whether the results of such bona fide independent discovery or reverse engineering have resulted in something worthy of being recognised as a trade secret. If so, the plaintiff's claim for injunction may not survive, owing to dilution of the trade secret.

Furthermore, if it is found that the means adopted by the defendant to discover the trade secret were not independent and rather were fraudulent, the court will not allow the use thereof by the defendant. The courts in John Richard v Chemical Process Equip, AIR 1987 Delhi 372 and in the *Konrad Wiedemann* case held that trade secrets are protected against misuse by any party who may have a relation with the claimant, irrespective of contract, based on the broad principles of equity.

1.8 Computer Software and Technology

Computer software is eligible for the following IP protection.

- Section 13 of the Copyright Act, 1957 states that copyright subsists in various works, including literary works – and a computer program is a literary work. Reference can be made to the Supreme Court's order in TCS v State of AP, Appeal(C) No 2582 of 1998.
- Patents can be registered as regards computer programs only if such program is attached to a physical device. Standalone computer programs are not entitled to patent protection (order of the IPAB in Ferid Allani v Assistant Controller of Patents, OA/17/2020/PT/DEL).
- Trade secrets are also protected through contracts and non-disclosure agreements (NDAs).
- The claimant may also approach the concerned court or police for necessary protection.

1.9 Duration of Protection for Trade Secrets

Trade secret protection lasts as long as the secrecy is maintained.

Once the confidential information enters the public domain, it ceases to be a trade secret.

If the disclosure of confidential information is made to employees or agents under contractual obligation to maintain secrecy, they are duty-bound to ensure that secrecy is maintained.

Controlled disclosure will depend on the terms and circumstances under which the disclosure was made – ie, on:

- what control the claimant exercises while making disclosure;
- what amount of information was given and retained; and
- the understanding of the parties as regards such information.

In the event of accidental disclosure, the information loses the attribute of secrecy and ceases to be a trade secret.

A rights-owner of such confidential information can approach the courts in India for prohibitive reliefs against persons who without authorisa-

tion acquire such information. The courts will only pass prohibitive orders if it is shown that the defendant obtained the confidential information fraudulently.

1.10 Licensing

General principles of contract law in India govern the licensing rights of an owner of a trade secret. They may license them to any party on any agreed-upon terms, subject to the condition that the agreement should not be contrary to the law of the land. As per Section 10 of the Indian Contract Act, all agreements are contracts if they are made with the free consent of parties competent to contract, for a lawful consideration and with a lawful object.

For the sake of caution, the owner may enter into an NDA with the licensee to ensure that the latter is under a contractual obligation to maintain secrecy as regards such trade secrets that have been handed over to them in confidence, and such NDAs may be built into the licence agreement to make it watertight.

The main objective is to ensure that trade secrets are handed over to the licensee under circumstances implying trust or confidence as regards their non-disclosure or unauthorised use.

1.11 What Differentiates Trade Secrets From Other IP Rights

IP rights in India are protected under various codified statutes or acts (see **1.1 Sources of Legal Protection for Trade Secrets**). Trade secrets, on the other hand, are not protected through a codified statute but through contract law or the equitable doctrine of breach of confidentiality.

IP rights have specified terms of protection as per the following statutes.

- Section 23 of the Copyright Act – the term of copyright for a work published anonymously is 60 years from the beginning of the calendar year following the year in which the work was first published. For a work concerning a disclosed author, the period is 60 years from the death of the author.
- Section 53 of the Patents Act – the term of every granted patent is 20 years from the date of filing of the application for the patent.
- Section 25 of the Trade Marks Act – the registration of a trade mark is valid for a period of ten years, and thereafter may be renewed from time to time.
- Section 11 of the Designs Act – a design registration is valid for ten years, and may be extended for another five years.

However, for a trade secret, the rights of its owner persist so long as its secrecy is maintained.

While the owner of an IP right can apply for registration of their title with the concerned governmental authority, this is not available for trade secrets.

Finally, the costs associated with maintaining secrecy and protection of a trade secret can be much higher in certain cases, compared to IP rights, which are registerable.

1.12 Overlapping IP Rights

Trade secrets and IP rights are two different aspects, even though their genesis may be the same.

The rights accrue to an owner of a trade secret either by virtue of a contract or in accordance with the principles of equitable relief under the common law, and it remains a trade secret till such time as the relevant conditions are fulfilled and it is not in the public domain.

However, upon registration of an IP right (such as a patent or design right) with the governmental authority, the owner is rewarded with a monopolistic right to the exclusion of others in rem for a certain period of time, after which any person from among the public can use the technology that was once the subject matter of said IP right.

1.13 Other Legal Theories

It is possible to bring a claim for breach of fiduciary duty against an employee who steals a trade secret, and against a defendant for tortious interference where it has induced an employee to breach a contractual confidentiality obligation to the owner/employer.

As previously mentioned, trade secrets in India are protected by virtue of contractual obligations that are regulated by the Indian Contract Act, 1872. Therefore, if there is a specific agreement with the employee to maintain confidentiality of any information given to them in the course of business, which renders exclusivity to their employer's business, such employee can be injuncted by the court from disclosing such confidential information to a third party without the express consent of their employer.

In AIA Engineering v Bharat Dand, AIR 2007 Gujarat (NOC) 1456, the court held that "it is no doubt true that, under common law, a servant can be prevented from diverting the trade secret and, even in a given case, a third party can also be restrained from acting in any manner on the basis of receiving such trade secret".

A rights-holder of a trade secret can also bring an action against the defendant for tortious interference where it has induced an employee to breach a contractual confidentiality obligation to the employer, as the court cannot allow misuse of a trade secret by a third party under the broad principles of equity, which stipulate that whoever has received information in confidence may not take unfair advantage of it (upheld in the *John Richard* and *Konrad Wiedemann* cases).

As regards claims founded on unlawful interference with the business of the claimant or of enticement to breach of contract, it is important to show that there was a clear violation or wrongful gain that has been caused to the employee, as well as wrongful loss caused to the employer. It should also be shown that there was some trade secret or confidential information that was taken without authorisation by the employee.

However, where it is impossible to identify the reasons behind the breach of the existing contract by the employee and the reasons for the employee joining a new employer, the court has opined that the claim cannot be enforced (see Modicare Limited v Gautam Bali CS (Comm) 763/2016)).

1.14 Criminal Liability

There is no specific offence of trade secret misappropriation under Indian law. The offences of criminal breach of trust, theft or cheating may apply, as per the facts of a particular case. See the detailed analysis in **9.1 Prosecution Process, Penalties and Defences**.

The owner of a trade secret may simultaneously initiate civil and criminal proceedings against misuse of their trade secrets.

A civil action can lead to damages (refer to **7.2 Measures of Damages**) and injunctive reliefs (refer to **7.3 Permanent Injunction** and **7.5 Costs**).

1.15 Extraterritoriality

A civil dispute concerning a trade secret claim can be brought before any civil court in India where the defendant resides, carries on business or personally works for gain, or where the cause of action wholly or partly arose.

If the person who indulged in misappropriation that occurred in another country is located in India, or if a part of the cause of action arose in India, the concerned Indian civil court will have jurisdiction to entertain a claim for injunctive relief, damages, costs, etc.

Furthermore, if a trade secret misappropriation is carried out outside India by a person located in India or through a computer system located in India, a criminal action can also be simultaneously filed against the wrongdoer by the claimant in India. See also **9.1 Prosecution Process, Penalties and Defences**.

2. Misappropriation of Trade Secrets

2.1 The Definition of Misappropriation

The courts in India have passed a catena of judgments identifying the essential elements to be established by the rights-holder when proving trade secret misappropriation.

The word "misappropriation" finds mention in Section 403 of the Indian Penal Code, which states that a person who dishonestly misappropriates or converts the movable property of another for their own use shall be punished with imprisonment of a term that may extend to two years and/or with a fine.

In Beyond Dreams v Zee Entertainment (2016) 5 Bom CR 266, the Bombay High Court held that, in order to establish trade secret misappropriation, the owner of the rights must prove the following:

- the information was a secret, and was not known generally or was not readily accessible to persons who deal with such information;
- the individual or owner of such information took reasonable steps to ensure and maintain its secrecy, and the information was imparted in circumstances importing an obligation of confidence; and
- there was unauthorised use of that information to the detriment of the party communicating it, or there was a threat to use it.

Section 101 of the Indian Evidence Act (with effect from 1 July 2024, this will be known as Bharatiya Sakshya Adhiniyam) states that the onus of proving a claim is on the person who makes it. Hence, the burden of proving trade secret misappropriation is on the person alleging it.

It is not mandatory for an owner of a trade secret to prove that their confidential information has been misused by the defendant. The very fact that the defendant misappropriated the claimant's trade secret demonstrates that the misappropriation was not just to steal the trade secret but to also acquire some unlawful gain from it, which gives rise to credible apprehension of future misuse by the defendant, entitling the claimant to take legal recourse.

In a civil proceeding, the rights-owner of a trade secret is merely required to show that the defendant has without authorisation accessed their trade secrets, as a prohibitory order of injunction by a civil court can be passed against the defendant, even in the absence of malice.

2.2 Employee Relationships

Trade secrets law in India does not differentiate between an employee and a third party. The essence of the law vests in the obligation to maintain secrecy in such confidential information that is not available in the public domain, and which ought to not be used without a licence from the rights-holder.

For an employee, the terms of employment may include a non-disclosure covenant, prohibiting them from disclosing confidential information they were privy to during the course of employment.

Such a contractual obligation may not be present between the rights-owner and an independent third party. However, even then, such a third party shall be prohibited by courts in India from misappropriating the trade secret.

In Zee Telefilms v Sundial Communications; (2003) 5 Bom CR 404, the Bombay High Court held that the obligation of confidence does not apply only to the original recipient but also to any other person who receives such information with the knowledge of obligation of confidence.

The courts must see that the information sought to be protected was not available in the public domain, and was communicated to the employee or the third party with a clear obligation to maintain secrecy, which they violated.

Therefore, employees would know certain facts and information without any special effort that cannot be termed as trade secrets, and a court may not entertain a claim to injunct the employee from using said information (see the *Star India* case).

2.3 Joint Ventures

No codified law recognises the existence of any obligations between joint venturers with respect to trade secrets. The parties can determine such rights and obligations concerning the exchange of trade secrets. Such agreements are governed by the Indian Contract Act.

Irrespective of the relation between parties with respect to sharing or use of confidential information, in the case of a dispute courts are guided by principles of equity, whereby whoever has received information in confidence may not take unfair advantage of it.

2.4 Industrial Espionage

As industrial espionage includes misappropriation of trade secrets, theft, cheating, etc, civil and criminal claims can be made by the claimant.

A detailed analysis of civil claims is covered in **7.2 Measures of Damages**, **7.3 Permanent Injunction** and **7.5 Costs**. Criminal claims are set out in **9.1 Prosecution Process, Penalties and Defences**.

3. Preventing Trade Secret Misappropriation

3.1 Best Practices for Safeguarding Trade Secrets

In transactions involving trade secrets, the owner of such information can take the following steps to ensure their interests are safeguarded:

- inform the recipient that the information is confidential in nature and that the giver has all proprietary rights to said information;
- expressly inform that confidentiality of the information should be maintained at all times

and that it should not be divulged to any third party without the consent of the giver; and
- clearly inform that, if the information is leaked, immense prejudice and harm will be caused to the giver.

Further, in cases where confidential information is involved, parties can form a confidentiality club by making a request to the court that confidential documents should only be accessible to members who are part of the club, and such members should undertake not to disclose or misuse such documents or information. The concept of confidentiality clubs has been discussed and upheld in various cases, such as:

- Pfizer v Unimark Remedies, order dated 4 May 2016 in Misc Petition (L) No 56 of 2016;
- Sivasamy v M/s Vestergaard A/S [FAO (OS) 206/2009];
- Mvf3 v Sivasamy [CS(OS) 599/2007] in IA No 10268/2009, CS (OS) No 599/2007;
- Roche v DCGI [CS (OS) 355/2014]; and
- Dolby International v GDN Enterprises [CS (Comm) 1425/2016].

Relying on the above judgments, the Delhi High Court passed an order in Ericsson (Publ) v Xiaomi Technology to the effect that "the reason probably is, in today's world of globalisation, where competition is at its peak, organisations may not be inclined to disclose trade secrets/confidential agreements or their details they had entered [into] with different parties lest [this] may cause serious prejudice to such parties because of competition involved".

The Delhi High Court (Original Side) Rules, 2018 introduced a rule on "confidentiality clubs", under Chapter VII Rule 17.

3.2 Exit Interviews

The manner of conducting exit interviews will vary across industries and across hierarchy. However, highlights would include the following:

- the departing employee shall not part with the confidential information they may have received during the employment;
- they ought not have in their power or possession any company property that may be tangible or intangible; and
- they may be required to sign a non-compete agreement, by virtue of which they would agree to not engage in a competing business by themself or join any other person who engages in such competing business.

In Krishan Murugai v Superintendence Co, AIR 1979 Delhi 232, the court held that an injunction can operate after termination of employment only if it is confined to the divulgence of trade secrets. There can be no restriction on the employee from joining a competitor post-termination. However, a negative covenant operating against the employee during the period of service was held to be legal.

4. Safeguarding Against Allegations of Trade Secret Misappropriation

4.1 Pre-existing Skills and Expertise

Indian law surrounding trade secrets clearly differentiates between the trade secret of an employer and the general knowledge and skill set that the employee hones during employment. As upheld in the *Star India* case, employees who have been working for an employer would know certain facts and information without any special effort and which cannot be termed as trade secrets of the employer, and a court may

not entertain an employer's claim to injunct the employee from using said facts and information.

In Bombay Dyeing v Mehar Karan, the court relied on the judgments of the US Court of Appeals, Tenth Circuit in Rivendell Forest v Georgia Pacific 31 USPQ 2d1472 and in Kodekay Electronics v Mechanex Corp 486 F 2d 449 (Tenth Circuit 1973), and held that something which is known outside the business or to those inside the business (ie, the employees), and for the guarding of which no steps have been taken and for the development of which no effort or money has been expended, cannot be a trade secret.

Therefore, while an employer cannot restrain an ex-employee from joining a competing business or from starting a competing business, it can certainly prohibit the ex-employee from disclosing information exclusively imparted to the employee by the employer during the course of employment, which is not part of public knowledge and which, if divulged by the employee, will lead to adverse consequences for the employer.

The doctrine of inevitable disclosure is not recognised in India as such. However, if the employee unintentionally discloses a trade secret of their former employer to their current employer, the former employer may be able to bring a claim for damages and injunctive relief against the ex-employee and their current employer. Please refer to **2.1 The Definition of Misappropriation**.

4.2 New Employees

The practices followed by companies while hiring employees from competitors vary. The following precautions may be taken to reduce the chances of being subject to a trade secret misappropriation claim:

- a written undertaking from the employee confirming that they have not retained any trade secret of their previous employer;
- a written declaration from the employee clearly stating that the current employer did not seek any trade secret of the previous employer from the employee; and
- a written undertaking whereby the employee indemnifies the current employer from any harm resulting from any act or omission of the employee as regards any confidential information pertaining to the previous employer.

5. Trade Secret Litigation

5.1 Prerequisites to Filing a Lawsuit

The procedure is as follows:

- The defendant(s) needs to be identified.
- The rights-holder should collect all relevant documents, such as contracts, correspondence with the defendant, etc, to show that the information in question can be considered "trade secrets".
- Evidence to show violation or misappropriation by the defendant needs to be tendered.
- One also has the option of filing a case against an unknown defendant (ie, a "John Doe") and subsequently adding a party once their identity is ascertained through discovery.
- If documents in support of the plaintiff's case are to be taken from various other parties, appropriate requests seeking interrogatories need to be filed.
- If the details are to be taken from intermediaries such as domain registrars, banks, etc, they can be made pro forma for the defendant to the suit.
- The rights-holder should have an authorised representative in India to sign and file papers on their behalf. Such an authorisation can be made by way of a simple power of attorney.

5.2 Limitations Period

A claim against a defendant would accrue on knowledge of said wrongdoing by the plaintiff.

The limitations period in a straightforward civil case involving trade secrets is three years from the date on which the cause of action arose. The limitations period for suits of tortious claims is one year.

In certain cases, the claimant can show that the cause of action is recurring in nature. In Bengal Waterproof v Bombay Waterproof; 1997 (17) PTC 98 (SC), the Supreme Court upheld the concept of recurring cause of action in relation to a trade mark dispute, and held that each time a defendant deals in an infringing product bearing the plaintiff's mark, they commit a recurring act of breach, giving a recurring and fresh cause of action at each transaction entered into by the defendant.

5.3 Initiating a Lawsuit

Please refer to **5.1 Prerequisites to Filing a Lawsuit**.

5.4 Jurisdiction of the Courts

As per Section 20 of the Code of Civil Procedure, a civil dispute concerning a trade secrets claim can be brought before any civil court in India where the defendant resides, carries on business or personally works for gain, or where the cause of action wholly or partly arose.

Matters involving trade secrets would fall within the definition of "commercial disputes" under Section 2(c) of the Commercial Courts Act, 2015. Before the Commercial Courts, timelines must be strictly followed for expeditious disposal of a commercial suit. If precisely followed, a commercial suit can be wrapped up as per the following timeline.

- Filing of suit.
- 30 days – plaintiff's additional documents.
- 120 days – written statement/reply from defendant.
- 60 days – inspection.
- 15 days – admission denial.
- 30 days – case management hearing:
  - (a) issues are framed;
  - (b) list of witnesses is filed;
  - (c) fixing of schedule for simultaneous filing of evidence;
  - (d) fixing of schedule for trial;
  - (e) fixing of schedule to file written note of arguments;
  - (f) fixing of date for final arguments; and
  - (g) fixing of schedule for final arguments.
- 180 days – closing of arguments.
- 90 days – judgment.

A criminal case concerning theft of trade secrets may also contain ingredients of criminal breach of trust, cheating, causing wrongful gain/loss and using IT resources for cheating, and can be filed before the police or the magistrate within whose jurisdiction the alleged illegal act wholly or partly took place, or where the accused person is located.

5.5 Initial Pleading Standards

The following are the main ingredients of a trade secrets claim:

- who the claimant is;
- the claimant's ownership of the confidential information;
- evidence to show that the information is confidential/a trade secret;
- who the defendant is;
- evidence of misappropriation; and
- evidence of damage costs.

In a civil action, Order VI Rule 2 stipulates that every pleading shall contain a concise statement of the material facts on which the party relies for their claim or defence. The evidence can be attached separately.

Also, a civil action may be filed based on information and belief supported by an affidavit. However, after initiation of the proceeding and discovery, if no evidence is gathered in support of the plaintiff's claim, the suit may be dismissed for want of cause of action against the defendants.

In Church of Christ v Ponniamman; AIR 2012 SC 3912, the Supreme Court held that cause of action is a bundle of facts which, taken with the law applicable to them, gives the plaintiff the right to relief against the defendant. Every fact that is necessary for the plaintiff to prove the claims made by them against the defendant and to enable the plaintiff to obtain a final decree should be set out in clear terms.

Even in a criminal action involving trade secrets, the complaint should be concise, and should contain the basic facts leading to the dispute and not provisions of law, precedents, etc.

Finally, the standard of proof in a civil case is preponderance of probability, while in a criminal case it is beyond reasonable doubt.

In Amica Financial Technologies Pvt Ltd v Hip Bar Pvt Ltd and Others, the Madras High Court held that, for an applicant to ask for protection of its trade secrets, it must prima facie establish through some material that such information was communicated to the person against whom protection is sought. Moreover, the applicant will also have to prima facie establish that the information in question is confidential in nature. Further, the applicant must also show that the confidential information is under threat of being used without authorisation by the respondent for wrongful gains.

5.6 Seizure Mechanisms

Under Order 26, a Civil Court has the power to appoint commissioners to:

- seize and take into custody incriminating evidence and material;
- inspect/investigate;
- examine accounts; and
- conduct scientific investigation, etc.

In a criminal case, summons to produce, searches and seizures, etc, are allowed as per Sections 91, 93 and 94 of the Code of Criminal Procedure (with effect from 1 July 2024, this will be known as Bharatiya Nagarik Suraksha Sanhita).

While applying for the above seizure orders against the accused/respondent at an ex-party stage, the court must be convinced of the following:

- that there is high likelihood of the opposite side destroying/fudging evidence if notice is given;
- that the evidence collected through such seizure is to be secured for adjudicating a dispute between the parties; and
- that the subject matter of the dispute will be preserved and not destroyed or tampered with.

The powers of a civil court in this regard have been contemplated in Orders 26 and 39 of the Code of Civil Procedure.

5.7 Obtaining Information and Evidence

Evidence can be collected as follows.

Under Order XI Rule 2 of the Code of Civil Procedure, 1908, a party can seek interrogatories. If certain important evidence or facts are not produced before the court, the party concerned is obligated to produce these.

As previously stated, under Order 26, the court has the power to appoint commissioners to:

- seize and take into custody incriminating evidence and material that may be found in their power and possession;
- inspect/investigate;
- examine accounts; and
- conduct scientific investigation, etc.

As per the Commercial Courts Act, 2015, both the claimants and the respondents must provide an undertaking that:

- all documents in their power, possession, control or custody pertaining to the facts and circumstances of the case have been placed on record;
- they have not made any false statement or concealed any material fact, document or record; and
- they have included all information that is relevant for the purposes of adjudication of the case.

If a party gives a false undertaking, it would be committing perjury and would invite penal consequences.

5.8 Maintaining Secrecy While Litigating

Please refer to **3.1 Best Practices for Safeguarding Trade Secrets**.

5.9 Defending Against Allegations of Misappropriation

The relevant defences are provided in **9.1 Prosecution Process, Penalties and Defences**.

5.10 Dispositive Motions

In India, the following options are available for narrowing down or eliminating a claim, completely or partially:

- where a baseless trade secrets suit is filed, the respondent can file under Order VII Rule 11 of the Code of Civil Procedure, seeking dismissal of the complaint on grounds such as non-disclosure of any cause of action, etc;
- as per Order VI Rule 7, the court may at any stage of the proceeding strike out or amend any pleading that may be unnecessary, scandalous, frivolous or vexatious, or which may tend to prejudice, embarrass or delay the fair trial or cause abuse of the process of law or the court; and
- sometimes, the court exercises its power and frames the main issues to be proved through trial, thereby ensuring the matter reaches a logical conclusion (see Order XIV Rule 1).

5.11 Cost of Litigation

The approximate cost for a trade secrets litigation (civil commercial suit) before the Delhi High Court, from start to finish, would be based on various factors, such as:

- court fees;
- lawyer's fees;
- fees of local commissioners and independent expert witnesses; and
- photocopying, travel, mail/courier and such ancillary expenses.

There is no specific law that bars third-party funding of litigation in India. One of the earliest cases in this regard was the judgment of the Privy Council in Ram Coomar v Chunder Canto; High Court of Judicature at Fort William in Bengal, where the court held that there is no law that declares it illegal for one party to receive and another to give funds for the purposes of carry-

ing on a suit. However, such agreements should not be contrary to public policy.

In the case of BCI v AK Balaji; AIR 2018 SC 1382, the Supreme Court of India held that advocates in India cannot fund litigation on behalf of their clients. However, there appears to be no restriction on third parties (non-lawyers) funding the litigation.

In Rangadurai v Gopalan; 1979 AIR 281, the court held that the relationship between a lawyer and their client is highly fiduciary in nature, requiring a high degree of fidelity and good faith.

Also, various provisions of the Bar Council of India Rules clearly state the following.

- Rule 9 – an advocate must not act or plead in any matter in which they have a pecuniary interest.
- Rule 18 – an advocate must not be a party to the fomenting of litigation.
- Rule 20 – an advocate must not stipulate a fee contingent on the results of litigation or agree to share the proceeds thereof.
- Rule 21 – an advocate must not buy, traffic in, stipulate or agree to receive any share or interest in any actionable claim. Nothing in this rule shall apply to:
  (a) stocks, shares and debentures of government securities;
  (b) any instruments that are, for the time being, by law or custom, negotiable; or
  (c) any mercantile document of title to goods.
- Rule 22 – an advocate must not directly or indirectly bid for or purchase, either in their own name or in any other name, for their own benefit or for the benefit of any other person, any property sold in the execution of a decree or order in any suit, appeal or other proceeding in which they were in any way professionally engaged.
- Rule 22A – an advocate must not directly or indirectly bid in court, auction or acquire by way of sale, gift, exchange or any other mode of transfer, either in their own name or in any other name for their own benefit or for the benefit of any other person, any property which is the subject matter of any suit appeal or other proceeding in which they are in any way professionally engaged.

Section 49(1)(c) of the Advocates Act, 1961 categorically mentions the standard of professional conduct and etiquette to be observed by advocates. Non-compliance can invite disciplinary proceedings and even debarment from practising law.

6. Trial

6.1 Bench or Jury Trial

There is no jury system in India. Cases are decided by judges, who are the presiding officers. The parties do not have a say in whether a judge or a jury decides a claim.

6.2 Trial Process

A trade secrets case does not have a special trial process. It is governed by the law pertaining to civil commercial lawsuits, as previously discussed. The trial process can be briefly summarised as follows.

- It commences with the court framing the main issues.
- Thereafter, the plaintiff is directed to file evidence by way of an affidavit of its witnesses. This is followed by cross-examination of the plaintiff's witnesses by the defendant's advocate.

- The defendant then files the affidavits of its witnesses, who will be cross-examined by the plaintiff's advocate.
- Once the cross-examination of the witnesses of both parties concludes, the matter is listed for final arguments.
- After hearing the final arguments, the court passes the final judgment.

6.3 Use of Expert Witnesses

Expert witnesses do appear before Indian courts on a regular basis.

The first kind of expert witness is a private expert witness, who appears on behalf of a private party (ie, plaintiff/defendant). For instance, in cases involving pharmaceuticals or telecommunications patent issues, parties file the evidence affidavit of an independent expert witness, who is someone of stature (such as the dean of a university, etc). Their testimony (ie, evidence affidavit) is also prepared in the same way as for other witnesses. An expert witness of one party will be cross-examined by the advocate of the other party, and vice versa. Independent experts charge fees depending on their expertise, experience and stature.

Under Section 45 of the Indian Evidence Act, when a court/judge is confronted with an issue that requires expert advice and opinion for resolution, they can refer that issue to an expert (eg, an expert on handwriting, fingerprinting, foreign law, etc).

7. Remedies

7.1 Preliminary Injunctive Relief

In Dr Sudipta Banerjee v LS Davar and Company and Others, FMAT 735 of 2021, the Hon'ble Calcutta High Court held that the remedies available to the owner of trade secrets include:

- an injunction preventing the licensee from disclosing the trade secret;
- return of all confidential and proprietary information; and
- compensation for any losses suffered owing to disclosure of such trade secret.

As opined by courts in India and by the Supreme Court in Kashi Math v Sudhindra; AIR 2010 SC 296, it is well established that, in order to obtain preliminary injunctive relief, the party seeking the granting of such an order has to prove that:

- they have made out a prima facie case for trial;
- the balance of convenience is in their favour; and
- they will suffer irreparable loss if the injunction is not granted.

The purpose of passing injunctive relief is to ensure that evidence is not destroyed and that further damage to the plaintiff is prevented.

Usually, when the court passes preliminary injunctive relief, it is valid till such time as the matter is finally argued or till the court vacates or modifies it. Also, if the injunctive relief is contingent on certain other facts, it can vary accordingly.

In a straightforward civil case involving trade secrets and confidentiality, under normal circumstances there is no need for the claimant to post a bond.

7.2 Measures of Damages

The following damages can be claimed in a trade secrets case:

- actual/compensatory – based on actual loss caused to the plaintiff and actual profits made by the defendant from misappropriation;

- punitive/exemplary – to set an example for other wrongdoers; and
- aggravated damages – on account of the extreme mala fide actions of the defendant, especially when actual/compensatory damages are disproportionately dwarfed in comparison to the actual amount recoverable by the plaintiffs.

The principles governing proof of actual damages, aggravated damages, and punitive damages in IP disputes are enshrined in the decision of Hindustan Unilever v Reckitt Benckiser, 2014 (57) PTC 495 [Del] [DB]. This was further upheld in Koninlijke Philips v Amazestore CS (COMM) 737 of 2016. The court also noted that the damages should be granted based on the degree of mala fide conduct.

7.3 Permanent Injunction

A permanent injunction will be granted if a claimant is successful in their civil action.

If it is practically possible for the defendant to recall a product, the court may pass an order directing recall. In a typical case, there is no limitation on the duration of a permanent injunction, and the defendant is injuncted for all times to come.

It is not possible to limit an employee's subsequent employment in most cases. As observed in the *Star India* case, any person in any employment for a certain period would acquire knowledge of certain facts without any special effort.

The courts in *Ambience India* and in Krishna Murgai v Superintendence Co; AIR 1979 Del 232 held that an employee, particularly after the cessation of their relationship with their employer, is free to pursue their own business or to seek employment with someone else. However, during the subsistence of their employment, they may be compelled to not engage in any other work or to not divulge the business/trade secrets of their employer to others, especially competitors. In such a case, a restraint order may be passed against an employee, as Section 27 of the Indian Contract Act is no bar in such a situation.

However, routine day-to-day affairs of an employer that are commonly known to others cannot be called trade secrets. Trade secrets can be formulae, technical know-how or a peculiar mode or method of business adopted by an employer which is unknown to others.

Nonetheless, the courts in John Richard v Chemical Process Equip and in Konrad Wiedemann v Standard Castings held that trade secrets are protected against misuse by any party who may have a relationship with the claimant, irrespective of contract and based on the broad principles of equity, whereby whoever has received information in confidence may not take unfair advantage of it.

7.4 Attorneys' Fees

If the claimant is successful in their suit, they may claim litigation costs, including attorney's fees, and not just damages.

Once the court concludes that the claimant is entitled to costs, it may ask the claimant to file a detailed memo of costs, and may then pass an order directing the defendant to pay such costs.

7.5 Costs

Costs can include:

- court fees;
- attorney's fees;
- fees of expert witnesses/investigators;

- travel expenses;
- fees of court commissioners; and
- photocopying/postal expenses, etc.

In the event of the respondent proving that the claimant's case is without any merit and was filed to harass the former, the court may award costs to the respondent for harassment and injury suffered.

Section 35 of the Code of Civil Procedure gives courts the discretion to impose costs. Section 35A discusses compensatory costs in respect of false, vexatious claims or defences.

8. Appeal

8.1 Appellate Procedure

If the trade secrets case is filed before the Delhi High Court, the suit will be listed and heard by a single judge. An appeal from the order can be filed before the Appellate Division, comprising two judges (Division Bench). If any party is not satisfied with the order of the Division Bench, an appeal may lie before the Supreme Court of India.

The time period for filing an appeal is 60 days, as per Section 13 of the Commercial Courts Act, 2015. Section 14 of the Act mentions that the appellate court should endeavour to dispose of appeals within a period of six months from the date of filing. Further, an appeal before the Supreme Court would be by way of a Special Leave Petition. As per Section 133(C) of the Schedule to the Limitation Act, 1963, the limitations period for appeal is 90 days from the date of the judgment or order.

It is also possible to appeal interim orders.

8.2 Factual or Legal Review

Appellate courts in India are the Hon'ble Supreme Court and the various High Courts (25 in number).

As a rule, appellate courts in India deal only with points of law. However, in certain cases where a question of fact was argued before the trial court but was still not considered by the judge, the appellate court can consider said fact.

In Wander v Antox; 1990 Supp (1) SCC 727, the Supreme Court of India held that the appellate court will not interfere with the exercise of discretion of the court of first instance and substitute its own discretion, except where the discretion is shown to have been exercised arbitrarily, capriciously or perversely, or where the court ignored the settled principles of law. The appellate court will not reassess the material and seek to reach a conclusion different from the one reached by the court below, if the one reached by such court was reasonably possible based on the material.

Under Indian law, review of an order is usually sought before the same judge who passed the order, and a petition seeking review of an order is allowed only if any of the following factors are proved:

- the order had an error apparent on the face it; and
- discovery of a new and important matter or evidence, which, despite the exercise of due diligence, was not within the knowledge of the party seeking review and could not be presented before the court when the order was passed.

While exercising its review jurisdiction in Northern India v Governor of Delhi; AIR 1980 SC 674, the Supreme Court of India held that a party is

not entitled to seek a review of a judgment delivered by this Court merely for the purpose of a rehearing and a fresh decision on the case.

If a court feels that a certain issue must be decided for the dispute to reach its logical conclusion, both parties can come to a common consensus, settle and thereby waive an issue, and the matter can proceed as regards the other issues.

All appeals have to be filed physically (ie, on paper) followed by oral arguments from both sides before a final order is passed.

The Supreme Court of India Rules, Orders XLVII and XLVIII state that certain proceedings before the apex court, such as a review petition and curative petition, would not entail a physical hearing unless specifically directed by the court.

9. Criminal Offences

9.1 Prosecution Process, Penalties and Defences

In the case of trade secrets theft, a complaint can be filed before either the concerned magistrate or police officer, for the following offences.

- Theft – Section 379 of the Indian Penal Code: with imprisonment of either description for a term that may extend to three years, or with a fine (or both).
- Cheating – Section 417 of the Indian Penal Code: with imprisonment of either description for a term that may extend to three years, or with a fine (or both).
- If the misappropriation is in violation of a contractual agreement, as per Section 406 of the Indian Penal Code one can claim criminal breach of trust: with imprisonment of either description for a term that may extend to three years, or with a fine (or both).
- If computer resources were involved in the misappropriation, this will also attract the provisions of the Information Technology Act, 2000:
  (a) Section 66B – punishment for dishonestly receiving stolen computer resources or communications devices, with imprisonment of either description for a term that may extend to three years, or with a fine that may extend to INR1 lakh (or both);
  (b) Section 66D – punishment for cheating by personation using computer resources, with imprisonment of either description for a term that may extend to three years, and liability to a fine that may extend to INR1 lakh; and
  (c) Section 72 – penalty for breach of confidentiality and privacy, with imprisonment for a term that may extend to two years, or with a fine that may extend to INR1 lakh (or both).
- Causing wrongful gain and wrongful loss.
- Copyright infringement – Section 63 of the Copyright Act, 1957: with imprisonment for six months to three years, and with a fine of between INR50,000 and INR2,00,000.

The accused can adopt various defences as follows, which may be nearly the same in both civil and criminal cases:

- that the information was not confidential or proprietary;
- that the information was in the public domain;
- absence of mens rea or criminal intent; and
- absence of any fiduciary relationship demanding exercise of a duty of care.

If aggrieved by lackadaisical police investigation, the claimant/complainant can approach the concerned magistrate seeking orders against the police under the provisions of Section 156(3) of the Criminal Procedure Code. There are dedicat-

ed police departments for dealing with economic and cyber offences.

10. Alternative Dispute Resolution (ADR)

10.1 Dispute Resolution Mechanisms

In Bawa Masala Co v Bawa Masala Co Pvt Ltd, CS (OS) No 139 of 2002, the High Court of Delhi passed an order referring the parties to a panel of neutral evaluators. They were directed to go through the papers and consider each side's position, and to render an evaluation of the case, thereby giving an unbiased understanding on the case's strengths and weaknesses.

One can apply for pre-litigation mediation before the Arbitration and Mediation Centre of the Delhi High Court under Section 12(A) of the Commercial Courts Act, 2015. Such proceedings are effective in cases with a high likelihood of settlement. Moreover, all discussions in such proceedings are confidential and are conducted without prejudice.

In a contractual agreement that has an arbitration clause, either party can seek interim orders under Section 9 and/or Section 17 of the Arbitration and Conciliation Act, 1996, in the event of a dispute.

JAPAN

Law and Practice

Contributed by:
Aya Takahashi, Miki Goto, Ryo Murakami and Akihito Ishii
Anderson Mori & Tomotsune

Contents

Anderson Mori & Tomotsune is a full-service law firm formed by the winning combination of three leading law firms in Japan: Anderson Mori, one of the largest international firms in Japan which was best known for serving overseas companies doing business in Japan since the early 1950s; Tomotsune & Kimura, particularly well-known for its expertise in international finance transactions; and Bingham Sakai Mimura Aizawa, a premier international insolvency/restructuring and crisis-management firm. This combined firm provides an extraordinarily powerful value proposition. Housing all of these synergistic practices under one roof, and further increasing its resource scale, it has the capability to: (i) serve a multinational client base, (ii) on in-bound, out-bound and domestic projects, (iii) by providing expert, timely and cost-efficient advice, (iv) across a full range of legal issues, and (v) in the largest, most complex, cross-sector transactions.

Authors

Aya Takahashi is a special counsel at Anderson Mori & Tomotsune, with 15 years of experience. She advises on IP and technical laws, and has assisted clients in numerous cross-border IP litigation and patent invalidation proceedings.

Ryo Murakami is a partner at Anderson Mori & Tomotsune, advising on IP and technical laws, and has assisted clients in numerous cross-border IP litigation and patent invalidation proceedings.

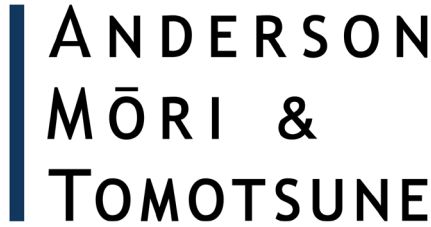
Akihito Ishii is a special counsel at Anderson Mori & Tomotsune, advising on IP and technical laws, and has assisted clients in numerous cross-border IP litigation and patent invalidation proceedings.

Miki Goto is a partner at Anderson Mori & Tomotsune, with an exceptional background as a Japanese lawyer and an academic background in both science and engineering, as well as professional experience working in the intellectual property department of a major electronics company. His practice covers a wide range of complex intellectual property and technology-related matters, including disputes concerning trade secrets and patents. He also has broad experience in various regulatory matters as well as product liability issues involving chemical substances, pharmaceutical products and other industrial products. Since 2017, he has been serving as the vice chair of the Standing Committee on Trade Secret of AIPPI.

Anderson Mori & Tomotsune

Otemachi Park Building
1-1-1 Otemachi
Chiyoda-ku
Tokyo 100-8136
Japan

Tel: +81 3 6775 1000
Web: www.amt-law.com



1. Legal Framework

1.1 Sources of Legal Protection for Trade Secrets

The statute Unfair Competition Prevention Act (UCPA) specifically provides for the protection of trade secrets in Japan.

Trade secrets may also be found to be protected under the general rule of torts, unjust enrichment, and contracts set forth in the Civil Code.

UCPA is understood to be a specific and prevailing rule under the general rule of torts, and the general aspects of the exercise of rights under the UCPA may be governed by the Civil Code.

1.2 What Is Protectable as a Trade Secret

A "trade secret" is defined in the UCPA as "a production method, sales method, or any other technical or operational information useful for business activities that is under management as a secret and is not publicly known".

- Controlled under management as a secret (protective measures) – The information must be under management as a secret by appropriate measures that are deemed reasonable under the specific circumstance, in a manner that the owner's intention to maintain secrecy can be objectively recognised by those having access to the information, such as the employees. The owner's subjective intention to keep the information as a secret is not sufficient to meet this requirement.
- Usefulness (commercial value) – The actual use of the information in an ongoing business activity by the owner is not essential; however, the owner must show that the information is at least potentially useful for business activities in the future based on objective standards.
- Not being generally known to public (secrecy) – The information must not be publicly accessible or easily obtainable by a third party.

1.3 Examples of Trade Secrets

Article 2 Clause 6 of the UCPA defines trade secrets as "production method, sales method, or any other technical or operational information useful for business activities". Production method is understood to include information such as the manufacturing methods, blueprints, and other technical know-how regarding manufacture. Sales method is understood to include information such as price lists, customer and supplier information, and sales manuals.

In a case involving bidding information obtained unlawfully, the court has found that such information does not deserve protection as a trade secret because the use of such information is adverse to the public interests.

1.4 Elements of Trade Secret Protection

To seek injunctive relief under the UCPA Article 3.1 against misappropriation of trade secrets, it is generally required that:

- the information satisfies the elements of a trade secret (as provided in **1.2 What Is Protectable as a Trade Secret**); and
- there is an act of misappropriation (as provided in **2.1 The Definition of Misappropriation**).

To seek damage compensation under the UCPA Article 4, it is additionally required that:

- there was intention or negligence of the misappropriating party;
- its business interests were harmed by the misappropriation; and
- the amount of damage suffered by the owner.

If the owner seeks damages based on the general rule of tort, the elements will be similar to where it seeks damages based on UCPA Article 4, except the subject information will not be strictly required to fulfil all of the elements of a trade secret, and the harmed interest of the owner shall not be limited to business interests.

If the owner seeks injunctive relief or damages based on breach of contract, the showing that the treatment of the relevant information by the actor violates the contractual obligation it owes to the owner shall be generally required.

If the owner seeks recovery of unjust enrichment by the infringer, the owner must establish that the misappropriating party has gained without legal basis, the owner has suffered loss, and there is causation between such gain and loss.

1.5 Reasonable Measures

The owner of a trade secret must show that it has taken reasonable measures to keep the information under management as a secret in order to enjoy trade secret protection, due to the management requirement explained in **1.2 What is Protectable as a Trade Secret**. The reasonableness of the measure shall be determined taking into consideration the specific circumstances, including whether taking such measures are commercially reasonable, the scale of the owner, or the nature of business and the information.

In general, courts tend to find that reasonable measures have been taken where the information is clearly marked as confidential, access to the information was limited to specific employees and required entering of passwords or was physically locked. In contrast, it is often found that reasonable measures were not taken in situations where the information lacked clear markings, free and unrestricted access was allowed to all employees, the protective measures such as passwords or locks were substantially meaningless in practice, or if the information could physically be taken out of its place of storage.

1.6 Disclosure to Employees

Disclosure of a trade secret to an employee will not necessarily disqualify the information from receiving protection as a trade secret, as employees are generally regarded to be under the control of the employer, and thus disclosure will not compromise the secrecy of the information. However, as explained in **1.5 Reasonable Measures**, there must be reasonable protective measures employed to keep the information under management as secret.

1.7 Independent Discovery

If the relevant information can be revealed through reasonable efforts, such as by conducting analysis on a product in the market by generally available means whose costs are not overly expensive, such information will fail to satisfy the secrecy requirement and not be protected as a trade secret. On the contrary, if the information is only available through extensive reverse engineering by experts requiring significant time and costs, it is understood that it may still satisfy the secrecy requirement.

1.8 Computer Software and Technology

Although by definition it does not fall under trade secret protection, UCPA offers protection to so-called "big data" that does not qualify as trade secrets, and provides similar remedies as trade secrets against misappropriation of such data.

1.9 Duration of Protection for Trade Secrets

Trade secret protections shall last perpetually as long as the legal elements required for trade secret protection remain satisfied. Even if the information is disclosed to a third party, the secrecy requirement is satisfied if the information is not deemed to be publicly accessible or easily obtainable by a third party. This includes cases where the information is disclosed under confidentiality obligations.

The effect of accidental or inadvertent disclosure is likely to be determined on a case-by-case basis, however if there is fault on the owner's side as to the cause of such disclosure, this may be found to demonstrate that the owner did not employ reasonable measures to keep the information under management as secret.

1.10 Licensing

In the context of trade secret protection, licensing is significant in that it involves disclosure to third parties. If the disclosure is not made in a manner that ensures secrecy of the information, such as upon securing of a non-disclosure agreement, the information may be deemed as publicly accessible and lose its protection.

Further, the owner should be mindful that, in order to assert misappropriation falling under the fourth bullet in **2.1 the Definition of Misappropriation**, the misappropriating party must have a "trade secret disclosed by the business operator", as opposed to obtaining such information as its own knowledge through transaction with the owner. From this perspective, it is advisable for the owner to identify the information as a trade secret, and demonstrate its intent to provide such information subject to it being treated as confidential.

1.11 What Differentiates Trade Secrets From Other IP Rights

In general, whereas intellectual property rights such as patent rights or copyrights are linked and to a specific invention or creative work and thus considered as a kind of property right, trade secret protection is rather understood as a restriction focusing on the act of exploitation.

Trade secret protection is also unique in that it requires secrecy, whereas intellectual property right regimes tend to encourage the holder of right to share or publish their invention or creation.

1.12 Overlapping IP Rights

Information subject to other intellectual property rights may also enjoy protection as a trade secret as long as such information fulfils the elements of a trade secret. Even if the scopes of the rights do not exactly overlap, there may be cases where a single act may trigger trade secret infringement and infringement on other intellectual property rights at the same time. For

instance, copying a customer list to obtain it unlawfully may constitute both an infringement of the copyright and trade secrets.

In such instance the plaintiff may assert claims based on trade secrets and claims based on copyrights in combination.

1.13 Other Legal Theories

As described in **1.4 Elements of Trade Secret Protection**, owners may also rely on general tort, contractual obligations, or unjust enrichment to seek remedies against misappropriation of trade secrets.

As described in **2.2 Employee Relationships**, employees generally owe a contractual obligation to their employer to keep their business secrets confidential.

1.14 Criminal Liability

Criminal penalties are imposed upon infringers of trade secrets only where there is wilful infringement, and additional elements such as purpose of wrongful gain or causing harm to the owner, a violation of the duty of information management, or an act of fraud exists.

Domestic misappropriation subject to criminal penalties is punishable by imprisonment of up to ten years and/or a fine of up to JPY20 million.

Misappropriation with international aspects, such as unlawful acquisition of trade secrets for use outside Japan or unlawful disclosure of trade secrets to a person outside Japan, are punishable by imprisonment of up to ten years and/or a fine of up to JPY30 million.

Further, when such misappropriation was done by an employee in relation to the business of its employer, the employer who is a corporation shall be subject to a fine of up to JPY50 million for domestic misappropriation and JPY100 million for international misappropriation (if the employer is an individual, the employer shall be subject to the same fines as the actor).

1.15 Extraterritoriality

With respect to damages and injunction claims based on trade secret misappropriation, there are several approaches to the applicability of UCPA on extraterritorial acts. Several court decisions have adopted the approach to determine the applicability of UCPA to extraterritorial acts pursuant to the general conflict of laws rule regarding torts. According to such rule, the laws of Japan shall apply if the result of the wrongful act occurred in Japan, or, if the occurrence of the result in Japan was ordinarily unforeseeable, if the wrongful act was committed in Japan. Under this approach, the UCPA may apply to extraterritorial acts of misappropriation if the result of the misappropriation occurred in Japan.

With respect to the criminal aspects of trade secret misappropriation, the UCPA specifically sets forth criminal sanctions against certain extraterritorial acts of misappropriation of trade secrets held by an owner doing business in Japan.

2. Misappropriation of Trade Secrets

2.1 The Definition of Misappropriation

Misappropriation of trade secrets is a part of the broader concept of “unfair competition” defined in the UCPA. Unfair competition involving trade secrets include the following categories:

- acquiring a trade secret by theft, fraud, duress or any other wrongful method (col-

lectively, "wrongful acquisition"), or using or disclosing a trade secret acquired through wrongful acquisition. The latter includes disclosure to a specific third party in confidence;
- acquiring a trade secret with the knowledge, or without the knowledge due to gross negligence, that wrongful acquisition was involved with such trade secret, or using or disclosing a trade secret acquired in that way;
- using or disclosing an acquired trade secret after becoming aware, or failing to become aware due to gross negligence, that wrongful acquisition was involved with such trade secret;
- using or disclosing a trade secret disclosed by the business operator holding such trade secret for the purpose of acquiring an illicit gain or causing damage to the holder;
- acquiring a trade secret with the knowledge, or without the knowledge due to gross negligence, that the trade secret is disclosed through improper disclosure or that improper disclosure was involved with such trade secret, or using or disclosing a trade secret acquired in that way. "Improper disclosure" is defined as disclosure of a trade secret as described in the fourth bullet point above, or in breach of a legal duty to maintain its secrecy;
- using or disclosing an acquired trade secret after becoming aware, or failing to become aware due to gross negligence, that improper disclosure was involved with such trade secret; and
- selling, delivering, displaying for the purpose of sale or delivery, exporting, importing or providing through telecommunication a product produced by using a technical trade secret in a way described in the bullet points above. This does not include cases where a transferee of such product engages in any of the foregoing acts if the transferee is not aware, without gross negligence, that the product was produced through such improper use of technical trade secret.

2.2 Employee Relationships

An employment relation is generally understood to impose certain inherent obligations upon the employee, whether explicitly provided in the employment contract or not. One of such duties is the fiduciary duty, or duty of good faith, which requires the employee to avoid unjustly harming the interests of the employer. Obligations to keep the employer's business secrets confidential and non-competition obligations are a part of this fiduciary duty, and the breach of such duty would constitute a breach of the employment contract. Information of the employer may be protected under this regime, even if it did not satisfy all of the elements of the trade secrets described in **1.2 What Is Protectable as a Trade Secret**.

2.3 Joint Ventures

The UCPA does not provide any specific rules focused on joint ventures.

2.4 Industrial Espionage

The UCPA does not provide any specific claims or remedies focused on industrial espionage. However, acts of industrial espionage are broadly captured under the misappropriations described in **2.2 Employee Relationships**.

3. Preventing Trade Secret Misappropriation

3.1 Best Practices for Safeguarding Trade Secrets

The Ministry of Economy, Trade and Industry (METI) has issued a Guideline on the Management of Trade Secrets, which demonstrates the

minimal standard required to receive protection under the UCPA.

Although the guideline recognises that the required measure would vary depending on the circumstances, it gives the following as examples of typical protective measures to be employed for the media containing trade secrets:

- in general – distinguishing trade secrets from other information;
- paper documents – confidentiality markings, storage in lockable cabinets or safes;
- electronic files – markings on media, file names and the content of electronic files, locking the storage of media, password protection, access authorisation control;
- trade secrets adhered to items such as manufacturing equipment, prototypes, or moulds – provide "do not enter/authorised persons only" signs, control entrance to the facility, prohibit photos; and
- knowledge of employees – enable visibility by creating written lists and descriptions of trade secrets.

In addition to such measures, it is also advisable to:

- implement internal information security policies and regulations;
- track use, transmission and copy of confidential information;
- only granting access to those that are in actual need of access to the information;
- ensure that employees have executed an employment agreement that contains confidentiality clauses, or a separate confidentiality agreement;
- ensure execution of confidentiality agreements with business partners;
- encourage employees not to leave confidential information on desks or other places visible from outside; and
- respond to information leakage swiftly.

3.2 Exit Interviews

Exit interview practices shall vary by the individual employers, but it is common for an employer to request the employee to submit a covenant confirming the confidentiality obligations of the employee upon departure. Such covenant often includes a description of the confidential information, including trade secrets, that the employee had access to during its employment. It may also include non-competition obligations, which typically restrict the employee from engaging in competing business for a term of around six months to 24 months. However, the validity of such non-competition covenant or agreement is strictly reviewed by the court based on its reasonableness.

4. Safeguarding Against Allegations of Trade Secret Misappropriation

4.1 Pre-existing Skills and Expertise

It is recognised in court decisions that employees shall not be barred from utilising the knowledge and skill obtained through the work performed by the employee during employment if it were of a universal nature, and would have been obtained by the employee if it engaged in similar work at other employers, in the context of non-competition agreements. This finding suggests that universal knowledge and skill can be distinguished from trade secrets, which are required to be controllable and non-accessible from outside the owner.

The doctrine of inevitable disclosure is not established in the Japanese courts. Rather, the courts tend to find that any non-competition agreement between the employee and employer that exceeds the scope of reasonable restriction shall be invalid because it violates the freedom of an individual to choose its profession, which is a fundamental right recognised in the constitution, and thus against the public order. The reasonableness of the restriction is decided by considering various elements such as the scope of restriction (the term of duration and territorial limitation), the interest of the former employer, the position of the former employee and the provision of compensation. In general, non-competition agreements setting forth a term that endures longer than two years after departure are likely to be found invalid.

4.2 New Employees

It would be prudent for the new employer to confirm with the candidate employee that no trade secrets or other confidential information of the former employer should be brought into or disclosed to the new employer, and that employment by the new employer will not violate any obligation that the candidate employee owes to its former employer, including any non-competition obligations. It is also advisable to obtain a covenant from the new employee to this end. The new employer should be mindful not to knowingly or with gross negligence allow the disclosure of trade secrets of the former employer by its new employees, as this may cause the new employer to fall under the second or third bullet points described in **2.1 The Definition of Misappropriation** if the trade secrets were unlawfully obtained by the new employee, or the fifth and sixth bullet points in **2.1 The Definition of Misappropriation** if the trade secrets were lawfully obtained but unlawfully disclosed.

5. Trade Secret Litigation

5.1 Prerequisites to Filing a Lawsuit

There is no special procedure required before bringing a litigation based on infringement of trade secrets, and the plaintiff may file its complaint immediately to the court.

5.2 Limitations Period

In general, the right to seek damages arising from general tort extinguishes:

- if the right is not exercised within three years after the claimant becomes aware of the damage and the tortfeasor; or
- upon passing of 20 years from the time of the tortious act.

The right to seek contractual remedies extinguishes:

- five years after the claimant becomes aware that the right is exercisable; or
- ten years after the right becomes exercisable.

For continuous misappropriation, under the rules of general tort, the loss or damage is understood to realise every day. Therefore, even if more than three years passed from the knowing of the damage and the tortfeasor, the damaged party may still bring a claim for its damages incurred during the most recent three years.

However, the UCPA provides that rights under UCPA to seek an injunction of continuous misappropriation extinguish:

- if the right is not exercised within three years after the claimant becomes aware of the damage and the tortfeasor; or
- upon passing of 20 years from the time of commencement of the tortious act.

5.3 Initiating a Lawsuit

To initiate a trade secret lawsuit, the owner should file a complaint to the court having jurisdiction, as explained in **5.4 Jurisdiction of the Courts**.

5.4 Jurisdiction of the Courts

The Code of Civil Procedure does not provide any exclusive jurisdiction of specialised courts for trade secret claims. Therefore, within the territory of Japan, a plaintiff can file a lawsuit in a court that has jurisdiction over the litigation in general (eg, a court that has jurisdiction over the place of domicile of the defendant, the place of the act of misappropriation or the place of realisation of loss or damage to the plaintiff).

It should be noted that a plaintiff is entitled to bring a trade secret claim based on the UCPA to the Tokyo District Court or the Osaka District Court as an alternative to any court in eastern Japan and western Japan respectively, in its discretion, even if these courts otherwise had no basis of jurisdiction over the case in its discretion. This is to ensure the opportunity of the plaintiff to utilise the special divisions in these two courts that exclusively handle intellectual property-related cases.

5.5 Initial Pleading Standards

Trade secret claims are subject to ordinary standards in relation to the initial pleading. In general, the plaintiffs are expected to establish a prima facie case with their initial pleading. Formally, the plaintiff is also required to assert the amount of damages incurred by the misappropriation. However, in practice, hard evidence for damage amounts is not required by the court upon the filing of the complaint.

5.6 Seizure Mechanisms

Seizure of evidence may be done through the means explained in **5.7 Obtaining Information and Evidence**.

Further, although this does not seize the items for the owner, Article 3.2 of the UCPA provides that the owner of a trade secret may obtain an order obligating the defendant to take measures necessary for the cessation and the prevention of the infringement, including disposal of items constituting the infringing act (including those produced by the infringing act) and the removal of facility used for the infringing act if its business interest has been, or is threatened to be, infringed by the misappropriation of its trade secret by such party.

5.7 Obtaining Information and Evidence

General discovery of relevant evidence is not available under the Japanese procedure. The UCPA provides the following means for the parties to gather information and evidence.

- A party may move for a court order obliging the other party to produce documents held by the other party that are necessary for proving misappropriation or calculating the amount of damages.
- The owner of the document may provide justifiable reasons and be exempt from such obligation.
- A failure to comply with the order does not lead to any sanctions, but may cause the judge to suspect that the party is trying to conceal certain facts unfavourable to such party.
- The same set of rules apply to the submission of objects (eg, accused products) for inspection by the court.
- The court may, upon a motion by a party to a lawsuit, order an expert to give their opinion

on the calculation of damages. The parties will be obliged to provide explanations necessary for the opinion.

Further, a party may seek the following means provided under the Code of Civil Procedures.

- A party may move for a court to issue a request for voluntarily producing documents. This is used when a third party (non-party to the lawsuit), especially a public agency, corporation or legal entity holds the relevant documents. Although this is not a legally binding order, such a third party often voluntarily fulfils the request because the request is made in the name of the court.
- A party may move for a court order obliging the other party or a third party to produce documents held by it. A violation may lead to certain sanctions. However, documents containing technical or occupational secrets are exempted from such order, and the usefulness of this order may be limited in trade secret litigation.
- The same set of rules applies to the submission of objects (eg, accused products) for inspection by the court.
- To preserve relevant evidence before a lawsuit is filed, a party may file a petition for an examination of evidence in advance.
- For example, if the misappropriating party is expected to destroy data once a lawsuit is filed, the judge may visit its factory and record the data stored there.

5.8 Maintaining Secrecy While Litigating

Under the Code of Civil Procedure, a party may move for a court decision to prohibit persons other than the parties to the litigation from inspecting or making copies of the case records (which are generally available to the public for inspection) on the ground that the records contain a trade secret.

The UCPA provides that the parties may move for a court to issue a protective order to preserve the secrecy of trade secrets contained in briefs and evidence. The addressees of such order may include the parties and their representatives, officers, employees or attorneys.

The moving party must make a prima facie case showing that the use of such trade secret for purposes other than to carry out the lawsuit, or the disclosure of such trade secret, would harm the party's business activities using such trade secret.

A person who violates a protective order will be subject to criminal sanctions.

When a party to the trade secret litigation is called as a witness to such litigation, and unable to give sufficient testimony regarding the trade secrets because of the harm to its business activities, and such testimony is essential for an appropriate judicial decision on whether there has been a misappropriation, the court may conduct such testimony in a non-public hearing upon the unanimous decision of all the judges constituting the panel.

The UCPA provides for several measures for protecting trade secrets in criminal proceedings, including an order not to disclose matters that will result in the identification of trade secrets in the public courtroom, limitation of questions in testimonies, non-public testimonies, and attorney's-eyes-only disclosure of evidence.

5.9 Defending Against Allegations of Misappropriation

Defences that a trade secret defendant may assert in a trade secret litigation include the following:

- existence of publicly available information similar to the trade secret;
- independent discovery:
  (a) misappropriation is defined as the exploitation of information belonging to another, and the use of independently discovered information shall not be included; and
- lawful acquisition:
  (a) only wrongful acquisition, improper disclosure and exploitation of trade secrets wrongfully acquired or improperly disclosed are defined as misappropriation. Use of information acquired through lawful means, including reverse engineering, shall not be included;
- statute of limitations;
- abuse of right or bad faith;
- negligence of the owner:
  (a) the amount of damages may be reduced depending on the degree of contribution; and
- exception to protection.

It is advisable for potential defendants to secure evidence on the process of independent discovery or lawful acquisition.

5.10 Dispositive Motions

The Japanese litigation process does not have a direct equivalent to what is referred to as dispositive motions in other jurisdictions. However, a case may be resolved before going into the merits if the claim is dismissed on procedural grounds, such as lack of jurisdiction.

5.11 Cost of Litigation

A party to trade secret litigation would incur costs such as the court costs (primarily stamp fees) and attorneys' fees. The court fees are calculated based on the monetary value of the remedies sought by the plaintiff.

Attorneys' fees vary depending on the arrangements with the law firm. Contingency fees are permitted as long as they are reasonable. A combination of fixed fees (payable upon the commencement of the case) and contingent fees (a certain percentage of the amount of award) is common in Japanese practice, aside from time-based fees.

The Code of Civil Procedure provides that payment of court fees can be extended upon a court's decision if a party to a lawsuit is suffering economic difficulties. Also, the Japan Legal Support Centre provides economic support to persons who do not have the ability to pay attorneys' fees.

6. Trial

6.1 Bench or Jury Trial

Jury trial is not conducted on litigation based on trade secret claims in Japan.

6.2 Trial Process

In typical Japanese civil lawsuits, including trade secret cases, oral hearing sessions are held in the open court one to several times at the beginning and ending of the litigation procedure. During the period in between, private preparatory hearings are regularly held at the court, and the parties exchange briefs and submit evidence to the court in a preparatory manner. When an oral hearing is held after the preparatory procedure, parties state that they restate the results of the preparatory procedure, and the arguments in their former briefs will be deemed to have been presented in the court.

If a live witness testimony is given, it must be given in one of the formal oral hearings.

Typically, it takes approximately six to 12 months from filing a complaint to obtain a final decision at the first instance.

6.3 Use of Expert Witnesses

Written witness statements by experts are not given separate treatment to other evidentiary documents, and may generally be submitted by the parties in a civil action so long as they are relevant to the case. Live witness testimony by expert witnesses is also admissible as long as it is relevant and the court considers it necessary; however, in practice, expert evidence is not often offered by parties in Japanese trade secret lawsuits. Admission of expert evidence in a particular lawsuit and (even if admitted) the evidentiary evaluation thereof is up to the court's discretion.

7. Remedies

7.1 Preliminary Injunctive Relief

Preliminary injunctions are available under the Civil Provisional Remedies Act. To obtain a preliminary injunction, an owner must make a prima facie showing of:

- the owner having the right to seek a permanent injunction (which corresponds to the requirements for a permanent injunction); and
- the necessity of a preliminary injunction, which would be substantial detriment or imminent danger that would occur to the owner if a preliminary injunction were not awarded.

Further, in most cases, courts require the owner to post a bond to compensate for the potential damages suffered by the counterparty if the permanent injunctions were not obtained in the end.

7.2 Measures of Damages

The UCPA provides three ways to calculate damages.

- If a certain product misappropriates a trade secret of the owner, the profit per unit of the owner's product that could have been sold by the owner (if the misappropriation had not occurred), multiplied by the number of the misappropriating party's products that have been actually sold, can be used as the amount of damages.
  - (a) If the misappropriating party proves that the owner could not have sold a certain number of products for any reason (eg, actual sales of the misappropriating party are because of its own marketing efforts, or there are competitive alternatives in the market), the amount of profit corresponding to such number shall be excluded from the aforementioned amount of damages.
  - (b) However, the owner is still entitled to recover damages equivalent to what it would have received as royalties for the amount that the owner could not have sold itself.
- If the misappropriating party has made a profit through an act of misappropriation of a trade secret, such profit can be presumed to be the amount of damages incurred by the owner.
  - (a) The misappropriating party may rebut the presumption by proving that its profit has been brought by something other than the trade secret, such as the misappropriating party's marketing efforts, brand image and the quality of the products or services irrelevant to the misappropriated trade secrets.

(b) The owner can also seek damages equal to the amount of reasonable royalties for the use of the relevant trade secrets.

In addition, if the owner has proved that it suffered certain loss or damage, but it is extremely difficult to prove the amount, the court may determine the reasonable amount of damages.

There is no award of punitive damages in Japan.

7.3 Permanent Injunction

Article 3.1 of the UCPA provides that the owner of a trade secret may obtain a permanent injunction against a party if its business interest has been, or is threatened to be, infringed by the misappropriation of its trade secret by such party. Unlike damage claims, the intent or negligence of the infringing party is not required. Such injunction may order the infringing party to cease infringing acts, and/or to refrain from engaging in infringing acts in the future. The injunction order may have a defined effective term, and in such case, the duration of the injunction shall be limited to such term.

In addition, if the misappropriation constitutes a breach of contract, the owner of the trade secret may seek permanent injunction on this basis as well. Specifically, if an owner of a trade secret proves that the misappropriating party owes a contractual duty of confidentiality with regard to the trade secret and has breached such duty, the owner may obtain a permanent injunction ordering compliance with the duty based on the Civil Code.

7.4 Attorneys' Fees

It is generally considered that compensation for reasonable attorney fees can be included in the damages claim based on tort. In practice, the amount of such attorneys' fees granted by the courts are usually around 10% of the proved amount of damages, as described in **7.2 Measures of Damages**, incurred by the owner.

7.5 Costs

The court may award successful litigants the court costs (eg, stamp fees for filing a complaint and witness fees) it incurred in whole or in part, upon its discretion. The awarded party may recoup this by initiating a separate proceeding to calculate the amounts thereof.

8. Appeal

8.1 Appellate Procedure

A trade secret case is generally decided in the district court for the first instance. A district court decision can be appealed to a high court that has jurisdiction over the place where the district court sits. The high court decision can be appealed to the Supreme Court as of right if there is a fundamental defect in the decision or in the procedure. The party may also file a petition for the acceptance of the appeal by the Supreme Court if the high court decision conflicts with a preceding Supreme Court decision (or with another high court decision in the absence of such Supreme Court decision), or if there is an important legal issue in the case.

8.2 Factual or Legal Review

When the high court reviews the case at the second instance, it reviews both the finding of facts and the application of law. Parties are allowed to provide additional evidence and arguments, although this may be dismissed by the court if such addition is found as untimely, due to fault of the submitting party, or causing undue delay in procedure.

The Supreme Court only reviews legal issues, and the parties may not file additional evidence.

9. Criminal Offences

9.1 Prosecution Process, Penalties and Defences

The owner whose trade secret has been misappropriated may file an offence report or a formal criminal complaint with the police or prosecutor's office, but this does not warrant that an investigation or prosecution will be initiated. The potential criminal penalties are as described in **1.14 Criminal Liability**.

10. Alternative Dispute Resolution (ADR)

10.1 Dispute Resolution Mechanisms

It is common that a Japanese court handling the case would separately conduct a settlement process within the court proceedings. It is typical to take place after several hearings and exchange of briefings, and the presiding judge discloses to the parties the court's tentative findings and thoughts on the merits of the case, and encourages both parties to agree to an amicable resolution. Terms of settlement reached in this process will be recorded in the court files.

The parties may also utilise mediation by the court. The mediation panel is composed of three mediators, one of which is a judge and the other two may be lawyers or other knowledgeable persons. Private mediation may also be an option for the parties. Confidentiality may be agreed as a part of the settlement terms.

The parties may agree to resolve the case by arbitration, and the arbitral award will become enforceable with the involvement of a court. It should be noted that it would depend on the arbitration rules whether the parties are under confidentiality obligations in relation to the process.

Trends and Developments

Contributed by:
Seiro Hatano, Rikiya Sato, Keiichiro Umino and Tomohiro Kuribayashi
TMI Associates

TMI Associates has grown from its establishment 30 years ago and its original 11 members to become the second-largest law firm in Japan, with more than 720 attorneys, including patent/trade mark attorneys, based in 17 offices. TMI has comprehensive transactional and dispute resolution capabilities, a distinctive regulatory focus and a renowned IP practice. In addition to the firm's locations in Japan, TMI has overseas bases in Cambodia, China, France, Indonesia, Myanmar, Singapore, Thailand, Vietnam, the UK and the USA, and has desks focused on Brazil, India, Kenya, Malaysia, Mexico and the Philippines. TMI's unique and unparalleled ability to form collaborative teams combining lawyers as well as patent and trade mark attorneys has enabled it to become a leading law firm in Japan and worldwide in the practice areas surrounding IP, media, sports, entertainment, and telecommunications and technology.

Authors

Seiro Hatano is a partner whose practice covers contentious and non-contentious IP-related work, with particular focus on trade marks and unfair competition, including trade secrets. He has considerable experience with contentious work, including litigation representing foreign-based clients. In addition, he has expertise in IP transactions for brand management through licensing and M&A. Mr Hatano has experience in trade secrets and copyright disputes, and his work also covers a wide range of sectors, including the TMT sector and protection of industrial data. He has worked at the Intellectual Property Policy Office in the Ministry of Economy, Trade and Industry of the Japanese government.

Rikiya Sato is a partner at TMI Associates, and his practice focuses on IP matters (especially trade marks, design, copyright, unfair competition and trade secrets). He has a vast amount of experience in invalidation and cancellation proceedings, business negotiations and IP infringement litigation. Notably, he has a wealth of experience earned from working in the Intellectual Property Policy Office of the Ministry of Economy, Trade and Industry as a fixed-term government officer from 2007 to 2010. He has also been a lecturer on IP Law at Keio Law School since 2020. Such experience enables Rikiya to offer his clients highly specialised services for a variety of IP matters.

Keiichiro Umino is a partner at TMI Associates, who handles both contentious and non-contentious aspects of IP law, with a focus on trade marks, design, copyright, unfair competition, trade secrets, labour and risk management. Drawing from his experience while seconded to the Ministry of Economy, Trade and Industry (where he was involved in the revision of the Unfair Competition Prevention Law), a major Japanese company, and the Tokyo 2020 Organising Committee, he also specialises in the fields of labour, trade secrets and compliance, etc.

Tomohiro Kuribayashi is a senior associate at TMI Associates, who handles both contentious and non-contentious aspects of IP law, with a focus on trade marks, design, copyright, unfair competition and trade secrets. Drawing from his experience while seconded to a major listed IT company in Japan, he also specialises in the field of IT law and TMT matters, including data privacy, e-commerce, and software and technology agreements.

TMI Associates

23F, Roppongi Hills Mori Tower
6-10-1 Roppongi Minato-ku Tokyo 106-0123
Japan

Tel: +81-3-6438-5511
Fax: +81-3-6438-5522
Email: info_general@tmi.gr.jp
Web: www.tmi.gr.jp

Contributed by: Seiro Hatano, Rikiya Sato, Keiichiro Umino and Tomohiro Kuribayashi, TMI Associates

Overview

In recent years, trade secret infringement cases in Japan have become larger in scale, more international and more complex. Security risks have also increased due to the expanding internationalisation of business, mobility of employment and digitalisation. Criminal cases relating to trade secret infringement have also been increasing, meaning that investigative authorities are more active than ever.

In light of these circumstances, several amendments to the Unfair Competition Prevention Act (UCPA), which provides protection for trade secrets, have been enacted to strengthen such protection, and to facilitate and encourage enforcement actions against trade secret infringement cases in both criminal and civil proceedings – though there remain some difficulties and limitations in seeking protection of trade secrets in Japan.

Trade Secret Infringement in Litigation

Trade secrets are protected under the UCPA as well as under confidentiality obligations by contract. Due to certain benefits provided under the UCPA in relation to the burden of proof or calculation of damages, claims under the UCPA are more common in practice against the misappropriation of a trade secret. In order to bring a civil claim under the UCPA, the plaintiff must first establish that the information qualifies as a "trade secret" as provided under the UCPA – ie, the information must be:

- controlled as a secret;
- useful for business; and
- unknown to the public.

Among the requirements for trade secrets, the confidentiality requirement is often a particularly significant issue in practice.

Confidentiality Requirement

In order to meet the confidentiality requirement, the information at issue must be appropriately controlled as confidential information. There is no clear threshold for the level of control, and it is determined by the courts on a case-by-case basis taking into account the various factual circumstances, including the nature of the business or information. In recent court decisions, confidentiality is generally considered as requiring that the information be controlled as a secret, to the extent that it is recognisable as confidential information, such as by way of access control for the information and confidentiality obligations.

The significance of the commercial value as confidential information has also been taken into account in recent court decisions, as it renders the information more recognisable as confidential information. Nevertheless, the determination of confidentiality is largely at the discretion of the presiding judge, as there are no detailed criteria for establishing confidentiality. Therefore, establishing whether or not confidentiality management exists is comprehensively based on the content and trends of the respective court cases.

Trends in Court Decisions on Confidentiality Requirements

In the past, courts tended to strictly apply the confidentiality requirement and quite often denied the protection of trade secrets. However, it is to be noted that confidentiality has become more easily recognised in recent years, though there is still a significant number of cases in which the existence of sufficient confidentiality was denied. For those who have not been particularly focused on security management, establishing confidentiality could be a challenging requirement. Some companies may be reluctant to file litigations against trade secret

infringement from fear that the court will deny the existence of confidentiality, which clearly indicates that sufficient or appropriate security management has not been implemented.

There are relatively few court cases that find trade secret infringement, and this may give the impression that the courts are still very strict in their consideration of the applicable standards for establishing trade secret infringement. It should be noted, however, that many trade secret litigations are resolved by settlement, and this also applies to trade secret infringement cases. In particular, if the court finds trade secret infringement, the court often encourages the plaintiff and defendant to settle the case to avoid such trade secret being disclosed to the public in a judgment.

In light of this, the fact of many court judgments denying the confidentiality threshold having been met is less to do with the Japanese courts' strict determination of this issue (as it may at first appear) and ultimately more about the protection of trade secrets. In the authors' experience, such matters are highly dependent on the presiding judge's views, with some adopting a broad interpretation of applicable standards, leading to the required confidentiality being found to exist.

Misappropriation of Trade Secrets

Further, in addition to the confidentiality issue, misappropriation of trade secrets is often contested in practice. There are no adequate procedures for compelling the disclosure of evidence held by the other party, as is the case in the US discovery system. As misappropriation of trade secrets typically occurs internally within a company and in confidence, identifying such instances and collecting evidence is not easy. Although certain measures are available – such as evidence preservation procedures under the Civil Procedure Code and the UCPA, providing a shifting of the burden of proof (as described below) – in many cases, they do not work well for collection of sufficient evidence and for proving the misappropriation of trade secrets.

In practice, therefore, it is often necessary to allege a range of facts that may be available – such as the other party's unusually shorter product development period, or the similarity between the developed and already existing products – in order for the court to infer the misappropriation of trade secrets. Therefore, when litigating trade secret infringement in Japan, it is necessary to bear in mind the difficulty of gathering such evidence on the use of trade secrets.

Trends in Criminal Cases

Under Japanese law, there are two approaches against the misappropriation of trade secrets, as in many other jurisdictions:

- civil injunctive and damages remedies; and
- criminal prosecution.

In Japan, criminal penalties for trade secret infringements were introduced in 2003 with the amendment of the UCPA. The criminalisation of trade secret infringements has been actively pursued since a trade secret infringement case between a major Japanese steel manufacturer and a major Korean steel manufacturer, about ten years ago. In 2012, the Japanese steel manufacturer filed a lawsuit against its competitor Korean company for damages for the unauthorised acquisition of technical information on certain new and innovative products. The lawsuit settled in 2015 with a substantial victory for the plaintiff, with the defendant paying a settlement of approximately JPY30 billion to the plaintiff.

The revelation and settlement of this issue had a significant impact on Japanese companies' awareness of the protection of trade secrets against their competitors. This case also led to the extensive 2015 amendments of the UCPA, to expand the protection of trade secrets and the scope of penalties for trade secret infringements. These changes in industry awareness and extensive legal reforms led to an increase in criminal proceedings against trade secret infringements.

Examples of Criminal Cases

In line with this trend, several important criminal court decisions on trade secret infringements have been issued in recent years. Among others, one case attracted particular attention, as not only the individual who stole the trade secret but also the company who acquired it from such individual were prosecuted and found guilty. In this case, a former employee of a major sushi restaurant unlawfully took information on the costs and suppliers of the restaurant and shared it with the restaurant's competitor. The former employee was sentenced to two years and six months of imprisonment, and was fined JPY1 million for taking such information and for other acts. The competitor company was also fined JPY30 million for obtaining and using this confidential information. This case demonstrates the recent trend in judicial decisions strictly judging the misappropriation of trade secrets.

Please note, however, there have been instances of acquittals on the grounds that the information in question did not constitute trade secrets. For example, in a case where former employees were prosecuted for divulging technical information on the manufacturing process of equipment, the court held that such technical information was merely a selection and combination of items of common knowledge, and thus did not constitute trade secrets, with the case resulting in an acquittal. In another acquittal case, a former employee was prosecuted for divulging trade information on customers and suppliers, and, despite him having been found guilty in the first instance, the appeal court overturned the district court's decision and denied that the information in question was a trade secret, as it was not controlled as confidential information.

Trends in Civil Cases, and Overview of the 2023 Amendment

Punitive damages cannot be awarded in civil litigation in Japan. In addition, litigation costs can be awarded as damages only to a very limited extent. For example, attorneys' fees may be recoverable only up to around 10% of the awarded damages amount. Furthermore, the amount of damages awarded in trade secret infringement litigation is generally modest, partly because it is not easy to prove that damage was caused by trade secret infringement.

While trade secret infringement cases have become more complex and substantial in recent years, and the amount of damages claimed has tended to increase, when reviewing the court decisions in civil cases rendered over the past two years, in nearly half of them the plaintiff's claim has been dismissed on the grounds that reasonable steps were not taken or that the defendant's use of the trade secret was not found. In addition, even when the court ruled in the plaintiff's favour, the amount of awarded damages was only around a few million Japanese yen, which is a small amount compared to other jurisdictions.

As discussed above, there have been court cases where the owner of trade secrets hesitated to take legal action for misappropriation of trade secrets, taking into account the difficulty, costs

of proof and risk of the awarded damages being insignificant. Furthermore, the increasing complexity and internationalisation of cases in recent years also underlies the hesitation towards taking legal action. In light of these issues, the UCPA was amended in 2023 to introduce a number of systems making it easier to use civil court proceedings in trade secret infringement cases (the "2023 Amendment"). The following three points should be noted as being particularly important under the 2023 Amendment.

Expansion of presumption of trade secrets misappropriation

As mentioned above, the Japanese Civil Procedure Act does not provide for a strong system of evidence collection comparable to the discovery process, which can complicate the process of proving misappropriation of trade secrets as this tends to occur privately, resulting in cases where trade secret owners abandon legal proceedings. In numerous recent court cases, the court dismissed the plaintiff's claims, holding that misappropriation of trade secrets was not sufficiently proven.

With awareness of this hurdle, the UCPA provides for presumption of the defendant's use of trade secrets with respect to certain technical information, and the 2023 Amendment expanded the scope of application of this presumption in order to ease the plaintiff's burden of proof. Under the former UCPA, the presumption of misappropriation of technical information by a defendant was only applied in cases of high maliciousness (such as so-called industrial espionage), but under the 2023 Amendment the presumption of misappropriation is also applied to:

- persons who originally had access to the trade secret; or
- persons who were aware that the trade secret was illegally acquired but failed to relinquish the acquired trade secret.

Expansion of presumption of damages amount

In Japan, the amount of damages awarded in trade secret infringement cases tends to be lower than in other jurisdictions (as mentioned above), partly because punitive damages are not awarded, leading to some parties' hesitation in taking legal action against trade secret infringement in Japan. In this respect, the UCPA provides for the presumption for the amount of damage suffered by the plaintiff due to misappropriation of trade secrets.

Under the former UCPA, the portion exceeding the production and sales capacity of the plaintiff was not presumed to be the plaintiff's damages, which was one reason why the amount of awarded damages tended to be lower. The 2023 Amendment aims to increase the amount of damages, and presumes that the amount equivalent to reasonable licence fees is appropriate as the damages amount for the portion exceeding the production and sales capacity of the plaintiff.

Clarification of governing law and jurisdiction

As trade secret infringement cases are becoming increasingly international, it is still unclear whether or not owners of trade secrets can be tried in a Japanese court under Japanese law in cases where (for example) the trade secrets managed in Japan are taken and misused outside Japan. This is another important reason behind the reticence in taking legal proceedings.

In this respect, the 2023 Amendment clarifies that if civil litigation is brought by the owner of trade secrets conducting business in Japan,

and if such civil litigation concerns trade secrets managed under a control system in Japan, such owners can utilise Japanese court proceedings under Japanese law.

Thus, in the past, there were cases where owners of trade secrets were hesitant about bringing civil claims for misappropriation of trade secrets, due to:

- the onerous burden of proof;
- the uncertainty of the applicable law and jurisdiction; and
- the risk of the amount of damages awarded being so insignificant that taking legal action would be cost-prohibitive.

However, through use of the system introduced by the 2023 Amendment and the criminal proceedings described below, there is now a system in place that facilitates instituting civil claims for trade secret infringement cases.

Approaches Through Both Criminal and Civil Proceedings

It has been pointed out that, in Japan, civil liability is the main form of protection for trade secrets, while criminal penalties are expected to play a complementary role in malicious cases. However, in recent practice, the use of criminal proceedings in relation to the misappropriation of trade secrets has not only played a complementary role but has also gained importance in terms of efficient evidence collection for civil proceedings against malicious acts.

Japanese civil proceedings do not offer a robust method for evidence collection (such as discovery) and it is particularly difficult to collect evidence relating to the misappropriation of trade secrets by the defendant in trade secret infringement cases. As a result, in practice, there are many cases where the plaintiff fails to prove the defendant's misappropriation of trade secrets and decides against continuing legal proceedings, or loses the case.

Therefore, in recent years, a rising number of cases have been observed where owners of trade secrets adopt the approach of initiating criminal proceedings first, followed by the civil proceedings, to utilise the evidence gathered by police and prosecutors through their compulsory powers in the criminal proceedings. In the above-mentioned dispute between the Japanese steel manufacturer company and its Korean competitor, it is suggested that the testimony of a former employee of the Korean competitor in the Korean criminal trial contributed significantly to the company's substantial victory. The employee was prosecuted in South Korea for leaking technical information of the Korean competitor to China. In the course of the trial, the employee stated that the technical information leaked to China originally belonged to the Japanese steel manufacturer company, which became important evidence of misappropriation of technical information of the Japanese company by the Korean competitor, in the Japanese company's proceedings against such Korean competitor.

Criminal Case or Civil Case?

It is advisable for owners of trade secrets to apply for criminal proceedings to be held first, so that evidence collected in such criminal proceedings can be applied in civil proceedings cases in which collection of evidence is complex and difficult. However, the following points should be noted when civil proceedings are preceded by criminal proceedings.

To initiate criminal proceedings, trade secret owners are first required to file a complaint to the police. Whether and when an investigation

starts largely depends on the discretion of the police, such as regards how serious the case is considered to be, and the police availability at the relevant time. Therefore, from the perspective of efficient use of criminal proceedings, it is necessary to prepare a persuasive complaint and to provide as much evidence as possible to explain how serious the case is and how urgent the investigation is. Otherwise, it may take a very long time to initiate such investigation (in some cases, more than six months or a year), or a case may even fail to be established in the first place.

Therefore, in cases where records indicate that misappropriation of trade secrets has taken place but where no concrete damage has yet arisen, or in cases where it is not clear that the suspect's use of trade secrets is evident, owners of trade secrets should not overly rely on police action and criminal proceedings. In such cases, it is more efficient and beneficial to minimise the damage through civil measures.

Dealing With Employees

A recent survey shows that most trade secret infringements in recent years have been caused by employees taking confidential information out of the company. In particular, there are many cases of employees illegally copying and taking information with them when they leave the company. In Japan, employees are obliged to maintain the confidentiality of company information through employment regulations, non-disclosure agreements (NDAs) or confidentiality undertakings.

The obligation to maintain the confidentiality of company information after leaving the company is basically not recognised unless it is clearly stated in the employment regulations or NDA. It should be noted that, while disciplinary action could be taken against the employees for breaching confidentiality obligations, Japanese labour law provides strong protection for employees against employers, even in cases of trade secret infringement. Therefore, the degree of disciplinary action should be carefully considered, and it should be borne in mind that it might not be permissible to summarily dismiss the employees who have committed trade secret infringement.

Strategy Against Trade Secret Infringement in Japan

The 2023 Amendment strengthened legal protections for confidential information, leading to an increase in both civil and criminal cases involving trade secret infringement. However, legal protection is not always available due to issues related to confidentiality or evidence collection.

Therefore, in order to protect trade secrets and efficiently pursue civil or criminal actions against trade secret infringement, it is crucial to review security management practices to ensure that the information is adequately treated as confidential. In the event of breach of confidentiality, it is imperative to verify the facts and gather as much evidence as possible as the first step, and the appropriate actions should then be contemplated in light of the legal protections available for the trade secrets.

MEXICO

Law and Practice

Contributed by:
Marina Hurtado Cruz, Carlos Davila Peniche and Daniel Villanueva Plasencia
Baker McKenzie

Contents

Baker McKenzie has, over 60 years, built a strong presence in five Mexican states: Mexico City, Guadalajara, Juárez, Monterrey and Tijuana. The firm provides the broadest IP coverage to clients across the country and, as a full-service firm, is able to bring expertise from all its practice areas to its IP advice. Five partners and counsels, with nearly two decades of expertise in the IP field, lead the practice group, which includes 13 lawyers, eight paralegals and three engineers. The IP team also works on related lines of business such as technology, privacy and life sciences. Areas of expertise include trade mark, patent and copyright prosecution and enforcement, as well as IP transactions and advisory.

Authors

Marina Hurtado Cruz leads Baker McKenzie's patent practice in Mexico. With more than a decade of experience handling sophisticated intellectual property matters, she advises on a broad range of areas including prosecution, licensing, and litigation of patents, utility models, industrial designs and trade secrets. In addition to this, Marina has extensive experience in life sciences, advertising and consumer law. In October 2019, Marina was appointed by the Secretary of the Mexican Ministry of Foreign Affairs as ad honorem external advisor on intellectual property issues to collaborate on the development of IP public policy in Mexico.

Carlos Davila Peniche is a partner in Baker McKenzie's North American intellectual property practice group. He provides strategic consulting on copyright, distinctive signs, domain names, trade secrets protection, unfair competition prevention, branding, advertising and protection in the digital environment, and privacy issues litigation. Carlos also implements and develops anti-piracy actions, handling undercover investigations and operations in counterfeiting matters. Carlos' professional practice spans the full range of IP law. His practice covers the drafting, negotiation, review and enforcement of licensing and franchising agreements as well as technology and intangible assets transfer.

Daniel Villanueva Plasencia is a partner of the intellectual property practice group at Baker McKenzie Guadalajara. He has extensive experience in data privacy, information and cybersecurity matters; in regulatory issues related to information technologies and consumer protection; and in intellectual and industrial property, especially focused on the digital environment, including the use and licensing of trade marks, patents and copyrights. Daniel is a Certified Information Privacy Administrator (CIPM) by the International Association of Privacy Professionals. Before joining the firm, he was a founding partner of a local firm in Guadalajara. Daniel has taught the intellectual property class at the Tecnológico de Monterrey, one of the most prestigious universities in Mexico.

Baker McKenzie

Edificio Virreyes
Pedregal 24
12th floor Lomas Virreyes
Molino del Rey
11040
Mexico City
Mexico

Tel: +52 55 5279 2900
Fax: +52 55 5279 2999
Email: marina.hurtado@bakermckenzie.com
Web: www.bakermckenzie.com

1. Legal Framework

1.1 Sources of Legal Protection for Trade Secrets

The Federal Law for the Protection of Industrial Property (FLPIP or "the Law") governs trade secrets in Mexico. The FLPIP entered into force on 1 July 2020 and replaced the former Industrial Property Law that had been in force since 1994. The FLPIP seeks to grant greater protection to industrial property rights, and significantly changes trade secrets protection.

The FLPIP is aligned with the provisions of Article 10bis of the Paris Convention and paragraphs 1 and 2 of Article 39 of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS). Likewise, the Law is in compliance with further obligations placed on Mexico as a result of other international agreements, most notably the United States, Mexico and Canada Agreement (USMCA), which entered into force on 1 July 2020.

The FLPIP:

- provides greater clarity on what can be considered a trade secret;
- states the scope of misappropriation;
- modifies and increases penalties for misappropriation, use or disclosure of trade secrets; and
- establishes new lines to enforce rights and obtain damages.

1.2 What Is Protectable as a Trade Secret

Under the FLPIP, a trade secret consists of any confidential information of industrial or commercial application that is kept by a person exercising legal control over it. This information must enable a trade secret's owner to obtain or maintain a competitive or economic advantage over third parties. It is also necessary that sufficient means are adopted to maintain the confidentiality of the information.

This confidential information may be kept in documents, electronic or magnetic media, optical discs, microfilms, films or in any other medium known or to be known. Furthermore, the following will not be considered a trade secret:

- information that is in the public domain;
- information that is generally known or easily accessible to persons within the circles in which said information is used; or
- information that must be disclosed by legal provision or by court order – this excludes information that is provided to any authority by a person exercising legal control over a trade secret, for the purpose of obtaining licences, permits, authorisations, records, or any other acts of authority.

1.3 Examples of Trade Secrets

There are no legal precedents yet regarding the types of information that are protectable under the FLPIP.

However, the definition in the new law of what can be protectable subject matter is much broader than in the previous law. Under the new FLPIP, any confidential information of industrial or commercial application can be considered a trade secret.

In contrast, the previous law was restricted to information related to specific categories:

- the nature or characteristics of products;
- their production methods or processes; and
- the means for commercialising products or services.

In addition, it was required that the information was not obvious to a technician in the field, similar to the inventive step requirement for patents. All these limitations were eliminated in the new FLPIP to allow for a broader definition.

1.4 Elements of Trade Secret Protection

The following elements have to be met for information to be protected as a trade secret:

- the information shall be confidential;
- the information shall be related to a commercial or industrial application;
- a person must be exercising legal control over the confidential information;
- the information must serve to obtain or maintain a competitive or economic advantage for its owner over third parties in carrying out economic activities; and
- the owner must adopt sufficient means or systems to preserve the confidentiality of the information and restrict access to it.

1.5 Reasonable Measures

In Mexico, a trade secret owner is required to adopt sufficient means or systems to preserve the confidentiality of the information and restricted access to it. Although there is no definitive list, some measures required by law are:

- the existence of a person exercising legal control over the confidential information;
- keeping the confidential information in documents, electronic or magnetic media, optical discs, microfilms, films or in any other medium known or to be known;
- entering into confidentiality agreements with persons or employees who may have access to trade secrets, specifying the aspects that are considered confidential; and
- prior notice to the third parties that have access to the trade secret informing them of its existence and its confidential nature.

In addition, some good practices may include:

- entering into confidentiality agreements with all persons who may have access to the industrial secrets;
- specifying in confidentiality clauses what information is considered to be a trade secret and what should be considered confidential;
- conducting training with employees who have access to trade secrets;
- marking as confidential all the information that has that characteristic; and
- keeping confidential information in a restricted place.

1.6 Disclosure to Employees

Under the law, an employee who has access to a trade secret and who has been warned about its confidentiality, must refrain from disclosing it without the consent of the person exercising legal control over it, or its authorised user.

1.7 Independent Discovery

In accordance with the FLPIP, misappropriation will not be considered in the following cases:

- the independent discovery or creation of the information that is claimed as a trade secret;
- the observation, study, disassembly or testing of a product or object that has been placed on the market/made available to the public or that is lawfully in the possession of the person obtaining the information, as long as it is not subject to any obligation of confidentiality regarding the trade secret; or
- the acquisition of information from another person in a legitimate manner without an obligation of confidentiality or without knowledge that the information was a trade secret.

1.8 Computer Software and Technology

There is no specific trade secret protection for computer software and/or technology. General

trade secret rules apply to computer software and technology.

1.9 Duration of Protection for Trade Secrets

A trade secret will be valid for as long as the requirements for its protection remain in force and the information does not enter the public domain. The law establishes that information that is in the public domain or that turns out to be generally known or easily accessible to persons within the circles in which said information is used will not be considered a trade secret. The law does not distinguish between deliberate disclosure by the person who has legal control of the information or accidental disclosure.

1.10 Licensing

The person who exercises legal control over a trade secret may transmit or authorise its use to a third party. The authorised user will have the obligation not to disclose the industrial secret by any means.

In the agreements through which technical knowledge, technical assistance, or provision of basic or detailed engineering are transmitted, confidentiality clauses may be established to protect trade secrets. These clauses shall specify the aspects that are to be confidential.

1.11 What Differentiates Trade Secrets From Other IP Rights

One of the main differences between trade secrets and other industrial property rights, such as patents, is that it is not necessary to register the trade secret before any authority to obtain protection, reducing costs. In addition, trade secrets are confidential and will not be made public by the authority; however, a trade secret cannot be enforced against a third person who obtained the information by means of discovery or reverse engineering.

On the other hand, unlike other intellectual property rights, a trade secret can protect commercial information (not necessarily industrial, technical or aesthetic) that is confidential and that represents a competitive advantage over third parties for its owner.

1.12 Overlapping IP Rights

It is possible for a plaintiff to assert trade secret rights in combination with other types of intellectual property rights. Since the Mexican Institute of Industrial Property (*Instituto Mexicano de la Propiedad Industrial* or IMPI) is the authority in charge of resolving, in the first instance, administrative offences related to trade secrets, patents, utility models, industrial designs, trade marks, and geographical indications, among others. It is possible submit an infringement request to IMPI involving these rights. In practice, it is common to file separate lawsuits according to the type of rights.

1.13 Other Legal Theories

The FLPIP imposes particular penalties for breach of fiduciary duty against an employee who steals a trade secret and for companies who hire an individual, whether an employee, ex employee, consultant or someone in a similar position, with the purpose of obtaining industrial secrets. In addition, the rightful owner of the trade secret may sue for civil damages.

1.14 Criminal Liability

The FLPIP imposes criminal penalties in a number of different circumstances:

- disclosure of an industrial secret, which is known by reason of one's work, position, performance of one's profession, business relationship or by virtue of the granting of a licence for its use, without consent, having been warned of its confidentiality, with the

purpose of obtaining an economic benefit or causing damage;
- taking possession of an industrial secret without right and without consent, with the purpose of obtaining an economic benefit or with the purpose of causing harm;
- using an industrial secret, which one knows by virtue of one's work, office or position, exercise of one's profession or business relationship, without having the consent of the person exercising their legal control over the secret or of the authorised user of the secret, or which has been disclosed to by a third party who did not have the consent of the person exercising their legal control over the secret or of the authorised user of the secret, for the purpose of obtaining an economic benefit or with the purpose of causing harm; and
- appropriating, acquiring, using or unduly disclosing an industrial secret through any means, without consent, with the purpose of causing harm or obtaining an economic benefit for oneself or for a third party.

1.15 Extraterritoriality

The provisions of the FLPIP are of public order and of general observance throughout Mexico; therefore, they do not have extraterritorial application. In addition, Mexican courts are only competent to assess a claim based on misappropriation that happens in Mexican territory.

2. Misappropriation of Trade Secrets

2.1 The Definition of Misappropriation

In Mexico, misappropriation means the acquisition, use or disclosure of a trade secret in a manner contrary to good practices and industry standards involving unfair competition, including the acquisition, use or disclosure of a trade secret by a third party who knew, or had reasonable grounds to know, that the trade secret was acquired in a manner contrary to such practices and standards. Therefore, the owner is required to show that its trade secret was actually appropriated, used or disclosed, as it would not be sufficient to show that the defendant accessed the trade secret without permission. However, taking possession of a trade secret without having a right to do so and without consent, to use it or disclose it to a third party, with the purpose of obtaining an economic benefit for oneself or for the third party or with the purpose of causing harm to the owner, is considered a crime.

2.2 Employee Relationships

The FLPIP explicitly recognises an employee's obligation to protect trade secrets. However, it is important that employees are notified of the nature of the information and of their confidentiality obligation. The burden of proof that the employee was so-informed falls on the employer.

2.3 Joint Ventures

Similar to the obligations for employees, any person who, in the course of their business relationship, such as joint ventures, has access to a trade secret of whose confidentiality they have been warned, must refrain from disclosing it without consent.

2.4 Industrial Espionage

Under the FLPIP, individuals or companies are prevented from hiring an employee who is working or has worked – or a professional, advisor or consultant who provides or has provided services for – another person, with the purpose of obtaining industrial secrets from the latter. In addition, under the Criminal Code anyone who, without just cause, to the detriment of another and without the consent of the person who may be harmed, discloses any secret or reserved

communication that they know or have learned because of their employment, office or position would be responsible for the commission of a crime. Increased penalties are available where such disclosure is made by anyone rendering professional or technical services or by a public official or employee, or when the secret disclosed or published is of an industrial nature.

3. Preventing Trade Secret Misappropriation

3.1 Best Practices for Safeguarding Trade Secrets

Because, even in cases of compliance with the legal nature of the trade secret (being secret, confidential and providing a competitive advantage), the burden of proof (that the recipient was duly informed of the nature of the information and its confidentiality) lies on the owner of the trade secret, it is highly recommended to do the following.

- Warn the recipient of the nature of the information as a trade secret – this can be achieved through the use of stamps in documents (eg, "confidential information" or "trade secret").
- Produce evidence of the receipt of the same and an acknowledgement by the recipient of the nature of the same – this can be achieved through the execution of a receipt, signed by both the owner of the trade secret and the recipient.
- Maintain the confidentiality and secret nature of the information – in this respect, the owner should:
  (a) have the necessary mechanisms, technological or not, to maintain the secrecy and confidentiality (eg, passwords, locks or vaults); and
  (b) execute non-disclosure or confidentiality agreements with the recipients.

It is worth mentioning that because the nature of the trade secret requires the owner to have control over its disclosure, the legal obligation to maintain the confidentiality of a trade secret must not be term-limited and should be effective indefinitely or for as long as the trade secret remains secret. Otherwise, at the end of the term of the confidentiality obligation, the owner of the trade secret would be left with no control over the information.

3.2 Exit Interviews

The nature of exit interviews and the assurances employers seek from departing employees depends on the industry, the size of the company and the position that the employee is leaving. While it is common practice for employees to sign a non-disclosure or confidentiality agreement when they first join a company, this is not the case when they leave. Nonetheless, employees in regulated industries, such as the financial or pharmaceutical sectors, often execute agreements with regard to their confidentiality obligations when they leave their employers. Considering that employees are often required to execute non-disclosure or confidentiality agreements when they first join a new job, it is also somewhat common that those documents include a clause which provides that they must not reveal, disclose, use or share any trade secrets from their past employers.

4. Safeguarding Against Allegations of Trade Secret Misappropriation

4.1 Pre-existing Skills and Expertise

Considering the legal definition of "trade secret" under the FLPIP, trivial information and the

experience and skills gained by employees in the normal course of their work is likely to be 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 and information that is not likely to help obtain or maintain a competitive or economic advantage over third parties in the conduct of economic activities. In addition, there is no relevant Mexican case law or jurisprudence addressing the doctrine of "inevitable disclosure".

4.2 New Employees

Considering that the individual or legal entity that hires an employee, with the purpose of obtaining industrial secrets is considered liable under the FLPIP, it is common for companies to include wording in the employment agreement, or execute a non-disclosure or confidentiality agreement with the employee, that specifically obliges the employee not to disclose or use any trade secrets of their previous employers.

5. Trade Secret Litigation

5.1 Prerequisites to Filing a Lawsuit

Under the Mexican legal framework, and subject to the contractual framework available, a trade secret owner having standing to initiate a trade secret misappropriation administrative infringement action before IMPI, which has jurisdiction over trade secrets disputes, will need to demonstrate the following factors through appropriate supporting evidence:

- ownership and legal control over confidential information, through deploying appropriate measures;
- information which has a commercial or industrial application;
- legal control over the confidential information;
- the existence of confidentiality and the measures taken to preserve it, such as confidentiality policies, non-disclosure agreements and clauses, and mechanisms and training intended to preserve confidentiality;
- competitive advantage obtained or maintained through the confidential information;
- prior notice or notices given to the third party who had access to the trade secret, informing that party of the trade secrets and their confidential nature;
- evidence showing, to a reasonable standard, the likelihood of trade secret misappropriation or unauthorised disclosure; and
- evidence showing the potential damage caused as a result of the misappropriation or unauthorised disclosure.

Formally speaking, it is not necessary to take any prior steps to filing a trade secret infringement action. In the event of potential misappropriation, unauthorised disclosure, or other kinds of detected infringing activity, prior to filing the claim, it is advisable to deliver notice to the infringing party, informing the latter of the alleged infringement, as well as requesting that the party in question attend a meeting to remedy the situation, before engaging in formal litigation.

5.2 Limitations Period

There is no applicable statute of limitations for raising a claim derived from a trade secret misappropriation or unauthorised disclosure. However, IMPI has a five-year limitation on enforcing administrative infringement claims, and the sooner the claim is brought the better, especially when seeking injunctive relief to prevent further disclosure or unauthorised dissemination.

5.3 Initiating a Lawsuit

Pre-litigation

Preparation and protection prior to allowing access to the trade secret is of the utmost importance to have sufficiently strong evidence to bring a successful claim. Generally speaking, vagueness and isolated elements, such as generic non-disclosure agreements or clauses, will be deemed insufficient to reach the reasonable standard requested or sought by IMPI, as it is a fact and evidence-intensive claim. Consequently, the trade secret owner should have as many supporting documents as possible to enhance their chances of success in the event of a potential litigation action. Examples of such documents include:

- detailed and to-the-point non-disclosure agreements or clauses, specifying the trade secret and its confidential nature;
- periodic policies and training for handling, managing, and preserving confidential information, including trade secrets;
- prior notices provided to the authorised users concerning the trade secret protection, its scope, and the necessary training and policies to be followed for protecting and managing the confidential information; and
- supporting documents showing the implemented measures to protect trade secrets, such as training, encryption, passwords, two-step identification authentication and monitoring access logs.

While it is possible to start a claim without these documents, an owner should consider that the claim's chances of success are likely to be directly related to the amount and quality of the documents that the owner can use to provide evidence of preparedness, protective measures taken, and training/education efforts concerning the awareness of the trade secret's users when they were handling the owner's trade secrets and confidential information.

Litigation

As mentioned, the trade secret owner will need to demonstrate the following factors through appropriate supporting evidence, in a written claim to be filed before IMPI:

- the detailed arguments supporting the trade secret misappropriation, misuse, or unauthorised disclosure, including the date and time at which the infringement occurred;
- ownership and legal control over the confidential information, through deployed appropriate measures;
- information which has a commercial or industrial application;
- the existence of confidentiality and the measures taken to preserve it, such as confidentiality policies, non-disclosure agreements and clauses, mechanisms and training intended to preserve confidentiality;
- the competitive advantage granted or obtained through the confidential information;
- prior notice or notices given to the third party who had access to the trade secret, informing them of the trade secrets and its confidential nature;
- evidence showing, to a reasonable standard, the likelihood of trade secret misappropriation or unauthorised disclosure – relevant evidence could include expert appraisals, forensic reviews, log records and prior notice;
- evidence showing the potential damage caused as a result of the misappropriation or unauthorised disclosure – relevant evidence could include expert appraisals, forensic reviews and accounting reports; and
- payment of IMPI's fees, which are around USD150, plus any and all legal and expert fees, which are the parties' burden.

Once the plaintiff files the claim, IMPI will review its contents to determine whether to admit it, to issue an official requirement for clarification purposes or to comply with a formal requirement. If IMPI admits the claim, the agency will order the delivery of service to the defendant. IMPI serves the defendant at the designated address, who in turn will have ten business days to prepare and file its written reply in a brief before IMPI. The defendant has the right to present evidence, including expert witnesses and appraisals, as well as any forensic reviews or other technical evidence as needed to defend its position.

5.4 Jurisdiction of the Courts

The competent authority for hearing trade secret cases, from a purely administrative scope, is IMPI, as trade secret enforcement is seen as an administrative infringement action under the applicable statute, the FLPIP. While it may be theoretically possible to pursue a civil claim before a local civil court, this will be subject to the contractual framework specifying civil enforcement, in addition to the administrative course of action. Such a claim would likely allege violations of contractual obligations related to confidential information's protection, as opposed to trade secret protection, which is the exclusive jurisdiction of IMPI.

At the appellate level, the Federal Administrative Court (*Tribunal Federal de Justicia Administrativa* or TFJA) has a specialised jurisdiction for all intellectual property-related matters, including trade secrets.

5.5 Initial Pleading Standards

Having concrete evidence of misappropriation is recommended before bringing a claim to increase chances of successful enforcement, and lack of evidence may affect the admissibility of a claim. While it is possible to bring a claim based "on information and belief", with the expectation of obtaining the hard evidence through technical evidence, such as an expert appraisal review of the misappropriation obtained during trial, it is necessary to meet a reasonable threshold concerning the evidence of misappropriation. Similarly, it is important to have relevant evidence to demonstrate that the confidential information grants the competitive advantage to its owner to meet the "trade secret" standard, which is assessed by IMPI upon reviewing the claim.

5.6 Seizure Mechanisms

The seizure of accused products or evidence, directly related to the claim, can be requested, granted, and executed by IMPI, as part of injunctive relief, as it is foreseen as part of its prosecution powers. The seizure should be requested before IMPI at the time when the claim is filed and can last throughout the entire proceeding. In considering such requests the IMPI will balance different factors:

- whether the request is bona fide;
- whether it is in the public interest;
- the seriousness of the matter; and
- the request's nature.

The plaintiff must also demonstrate the trade secret's ownership through appropriate evidence, as well as:

- an infringement of the right;
- that the infringement or violation will be imminent;
- the likelihood of suffering an irreparable harm; and
- a well-founded fear that the evidence could be destroyed, hidden, lost or altered.

Further, they must provide the relevant and necessary information to identify the goods, ser-

vices, or physical or digital platforms where the infringement takes place.

Additionally the applicant may need to file a bond or certified deposit to compensate the respondent for any harm suffered during the seizure in the event that it is later determined that it had been wrongly granted. The bond's amount will be set by IMPI after assessing the merits of the case and the request's scope. FLPIP also foresees that defendant may file a counterbond to respond for any potential harm against the plaintiff. The counterbond, subject to IMPI's discretionary decision, may be sufficient lift such measures during the trial.

5.7 Obtaining Information and Evidence

FLPIP grants powers to IMPI to obtain certain evidence from a third party for any type of claim, including a trade secret infringement claim, subject to a written and reasonable request made by a plaintiff. The available mechanisms are:

- an information request from a third party, which is materially linked to the claim; and
- an on-site visit to an establishment to verify compliance with FLPIP.

Generally speaking, while IMPI has reasonably strong powers through these fact-gathering mechanisms, which do not require court assistance, these actions may not be sufficient to support a trade secret claim by themselves. Consequently, these activities should be considered to be ancillary to the evidence showing the infringement, which the plaintiff needs to prepare and have ready before filing the claim.

5.8 Maintaining Secrecy While Litigating

The parties can request measures to preserve confidentiality of the trade secrets at issue through the special structure available under the Federal Administrative Procedural Law (*Ley Federal Procedimiento Administrativo*), through which a party can request IMPI to designate the documents and any other element related to the trade secrets claim as confidential due to its nature. In turn, IMPI's officers will store the specified documents in a private chamber, with access restricted to the involved attorneys.

5.9 Defending Against Allegations of Misappropriation

The following defences are available under FLPIP:

- the information at issue is in the public domain;
- the information is generally known or is easily accessible for individuals within the circles in which the information is regularly used;
- the information must be disclosed due to a statutory mandate or a judicial order;
- the information at issue has been discovered or created independently;
- the information was obtained through the observation, study or disassembly of – or the experiment on – a product or object that has been made available to the general public, or that it is in the lawful possession of the individual who obtains the information, as long as they not been under a confidentiality obligation regarding the trade secret; and
- lawfully acquiring information from a third party, without a confidentiality obligation, or unaware that the information was a trade secret.

5.10 Dispositive Motions

Dispositive motions are not available under Mexican Law.

5.11 Cost of Litigation

The costs will vary depending on the case's complexity, the evidence prepared and filed, as well as the duration. Typically, the cost of a trade secret litigation case in the first instance can vary from USD15,000 to USD25,000 plus expert appraisals, notary public fees, and other fees relating to evidence preparation, which can vary from USD10,000 to USD30,000.

While theoretically it is possible to seek to fund litigation on a contingency basis, including through law firms, in practice this is seldom used, due to a trial's extensive duration, which can be over five years in the administrative phase, as the Mexican damages system is still being developed, especially where it concerns IP rights.

6. Trial

6.1 Bench or Jury Trial

Trade secret trials are decided by IMPI only, which functions akin to a judge, in the first instance. Subsequently, the federal courts will have jurisdiction over the case.

6.2 Trial Process

In Mexico, trade secret litigation cases are decided by the papers filed, including expert appraisals. The plaintiff has the burden of proof to demonstrate the facts of the case, with IMPI issuing a determination in the first instance. Both parties have the right to present evidence and arguments during the trial to defend their positions. Testimonies can be brought to the case, as long as the testimony is presented in writing, as there are no depositions or in-person witness testimony available under the applicable statute. Typically, a trade secret trial can take anywhere from one year to three years, subject to IMPI's workload.

6.3 Use of Expert Witnesses

Expert witness testimony or appraisals are allowed in Mexico and can be regularly used to demonstrate facts and technical issues during the litigation to bolster the chance of success. Each party is entitled to name its expert witness, which should be done at the time of presenting the initial brief, for the plaintiff; or at the time of filing the reply brief, for the defendant. The Federal Rules of Civil Procedure foresee certain limitations regarding expert testimony, such as that it cannot be on a question of law, as this will be the judge's role.

When offering the written testimony, the party presenting the evidence must present a questionnaire and name the expert. Following this, in its reply brief, the defendant will have the right to add questions to the proposed questionnaire, as well as naming its own expert. IMPI will have the right to name a third expert from a list of pre-approved experts. IMPI will then provide the experts with a reasonable term to render their expert appraisals, which will be considered by IMPI in its final resolution. Concerning costs, it is difficult to ascertain potential costs involved in these activities, as they vary widely depending on the field.

7. Remedies

7.1 Preliminary Injunctive Relief

The requirements for obtaining injunctive relief are the same as those for seizing accused products and other evidence (see **5.6 Seizure Mechanisms**).

7.2 Measures of Damages

Damages are calculated starting at 40% of the legitimate value indicator, as presented by the affected owner. An award of damages can be sought through a damages incident with IMPI or

before a civil court, after the administrative procedure, including both rounds of appeal, concludes. IMPI's recent powers to grant a damages award are yet to be constitutionally tested before the Mexican Supreme Court, so until a decision is taken, it is advisable to file the damages incident before a civil court.

To prove damages, it is necessary for the plaintiff seeking such a remedy to prove the following elements, through appropriate documents:

- that an IP infringement occurred, which can be proven through IMPI's resolution declaring an infringement;
- that the infringement resulted in economic damage to the plaintiff's interest, which can be proven through financial appraisals and expert witnesses on accounting; and
- the factual/causal link between the infringement and the economic effect or loss.

To interpret the legitimate value indicator on which to base the 40% damages compensation, the plaintiff will propose that IMPI or the civil court assess it based on the following:

- the infringed product or service value, calculated through market price, or the suggested retail price;
- lost profits of the plaintiff as a result of the infringement;
- gained profits of the defendant as a result of the infringement; and
- the price that the infringer would have paid the legitimate titleholder for granting a licence, considering the commercial value of the infringed right, as well as the granted and existing licences.

As of today, an owner can only seek the described statutory damages, as punitive damages are not expressly foreseen in the FLPIP, and have not been widely accepted in Mexican case law.

7.3 Permanent Injunction

Typically, IMPI has the powers to order a third party to refrain from continuing to violate intellectual property rights after the claim has been definitively resolved. Such orders may include a product recall or destruction of the seized goods, through IMPI, as well as an order to refrain from conducting certain activities. On the other hand, orders restraining individuals from employment opportunities are rare, as the general rule prioritises an individual's right to seek and obtain future employment opportunities. This rule may allow for specific exceptions that can be tied or related to unfair competition practices, but it is unlikely to be enforced in practice, as Mexico tends to prioritise the rights of individuals over those of companies in employment issues.

7.4 Attorneys' Fees

Under the previous statute, IMPI did not have such the authority to award attorney's fees. Although there has not been a change in this situation since the FLPIP's enactment, as the FLPIP foresees a new damages system, it could be possible to claim attorney's fees through a quantification of damages, as is foreseen under the Federal Rules of Civil Procedure. However, this remains merely a theoretical possibility.

7.5 Costs

In administrative litigation, each party bears its own costs for litigation and cannot seek an award for costs.

8. Appeal

8.1 Appellate Procedure

The Mexican legal system has two different appeals before a decision is final: ordinary appeal and constitutional appeal.

Ordinary Appeal

The first appeal level is with the TJFA, which has a Specialised IP Court with federal jurisdiction over IMPI's activities, as the latter is a federal authority and IP rights, including trade secrets are regulated at the federal level.

Once IMPI issues a final decision, the affected party will have a non-extendable term of 30 business days to prepare and file an appeal. IMPI and the winning party will have the right to file a reply brief with the appellate court. At this instance, only the affected party has the right to appeal an unfavourable decision. The appeal's arguments should challenge all the issues raised in the decision, including formal prosecution mistakes or errors that have affected the losing party's position. Generally speaking, it is not possible to challenge non-final judgments and orders.

Typically, an ordinary appeal lasts from 10–18 months.

Constitutional Appeal

The constitutional appeal is prosecuted before the Federal Circuit Courts (*Tribunales Colegiados de Circuito en Materia Administrativa*), part of the Federal Judiciary Power in Mexico. These courts regularly hear administrative litigation cases, including intellectual property disputes, but lack a specialised IP court.

The affected party has a non-extendable 15-business-day term after service of the TFJA's adverse resolution to challenge it through an amparo, or a constitutional appeal, which will review the constitutional and legal grounds of the ruling, without any admission of new evidence. Contrary to the ordinary appeal rules, the prevailing party has the right to present a recourse against a favourable ruling in the parts that are adverse to its interests, or to present additional, stronger arguments to prevail in the new ruling.

Typically, a constitutional appeal lasts from 10–12 months.

8.2 Factual or Legal Review

Generally speaking, both appellate courts can only review legal issues, as any and all evidence related to the merits of the case should have been presented and rendered during the trial phase, for the trial authority (IMPI) to hear, analyse, and assess the evidence. Under the applicable statute and case law, the appeal court cannot receive any additional evidence which should have been presented to try the case. It is possible to present evidence intended to challenge what is claimed to be IMPI's erroneous interpretation or appreciation in the resolution, but not evidence which was meant to demonstrate the facts of the case.

The appellate phase is mostly a written proceeding. Parties can present oral arguments before the court, but this is not a formally recognised hearing in the procedure, so it is an informal practice.

9. Criminal Offences

9.1 Prosecution Process, Penalties and Defences

Like its predecessor statute, the FLPIP recognises criminal offences of trade secret theft, misappropriation, unauthorised disclosure,

and unauthorised use – requiring the presence of an additional element: that the illicit activity took place with ill-intent, which must be proven beyond any reasonable doubt. This evidentiary burden makes it more difficult to sustain criminal charges against trade secret defendants in practice. Additionally, the success of any criminal action depends on the prosecutor's expertise and skill set to prepare the case; unfortunately for victims of trade secret violation, federal prosecutors tend to prioritise prosecuting other kinds of criminal complaints having a larger impact on society. Consequently, criminal enforcement is rarely used in practice.

It is likely that these same defences and arguments available in civil trade secret actions may apply in practice to criminal claims. From an evidence preparation perspective, the National Code of Criminal Procedure foresees a broad array of investigation techniques that can be devised and implemented through the federal prosecutor, with and without court orders, to investigate trade secret misappropriation or economic espionage offences. However, for more sophisticated and invasive techniques – such as wiretapping and data extraction from platforms, servers and devices, electronic apparatus, computers and storage devices – it is necessary to obtain a court order, which will be very limited in scope and time.

Finally, for criminal trade secret violations, the FLPIP imposes penalties, from two to six years; as well as economic penalties, from the equivalent of USD5,460 to USD1.638 million, in addition to compensatory damages.

10. Alternative Dispute Resolution (ADR)

10.1 Dispute Resolution Mechanisms

To date, while the possibility of encouraging the use of ADR mechanisms through contractual clauses is anticipated in Mexico, this option is seldom used for intellectual property cases, as it was not expressly authorised under the former statute. However, this changed recently due to the FLPIP's enactment, which now foresees the parties' right to open a conciliation procedure, before IMPI, to explore the possibility of reaching a settlement in infringement cases. This right is available to both parties until IMPI reaches a decision in the first instance.

FLPIP also contemplates a conciliation procedure in which IMPI will be conciliator, holding the infringement proceeding in abeyance while the conciliation is ongoing. The party requesting the conciliation must present a written proposal to settle the claim. The other party will have the right to accept it, present a written counterproposal, or reject it. If a counterproposal exists, an IMPI officer will summon the parties to in-person meetings at IMPI's premises to discuss potential settlements. Due to statutory restrictions, the conciliation procedure is limited to two meetings. If the parties do not reach a settlement, IMPI will resume the infringement proceeding.

NORWAY

Trends and Developments

Contributed by:
Ulrikke Asbøll and Ann-Cathrin Hoel
Onsagers AS

Onsagers AS is the largest full-service specialised IP firm in Norway, acting globally with its team of around 50 IP experts, with offices in Norway, Sweden, Germany and the UK. Onsagers' dedicated experts work in industry teams, where attorneys-at-law and European patent attorneys with extensive international and technical experience work in close collaboration. The firm offers specialist assistance in all key areas of IP law. It is known for always being on top of each client's business and business areas to ensure the best strategic and commercial advice is provided. Its team of experts has comprehensive experience in trade mark and patent prosecution, enforcement and litigation, including customs seizures, passing-off and unfair competition cases, as well as trade mark and patent infringement and validity cases. The firm's team members have extensive knowledge from the Norwegian Industrial Property Office, the Appeal Board, and from representing Norway in WIPO and the EPO.

Authors

Ulrikke Asbøll is a senior partner/head of IP management consulting at Onsagers. She has more than 16 years of domestic and international experience, offering legal and strategic IP advice to global corporations, as well as services to IP in-house counsels. Her extensive IP experience covers a broad range of services, including identifying and managing IP assets, building and managing large IP-portfolios, IP due diligence and M&A, IP preparations for IPOs, oppositions in EPO, cross-border litigation, IP strategy and freedom to operate, and contributing to the sale of Norway's first unicorn. Ulrikke's work involves complex interdisciplinary co-operation and co-ordination, and she always endeavours to find the most advantageous solution for the client.

Ann-Cathrin Hoel is a senior partner/head of business development at Onsagers. She has worked in IP for more than 30 years, and has extensive experience as an in-house lawyer, IP consultant and legal counsel. She brings invaluable, client-side industry experience, having worked in-house as head of the IP department at Nycomed Amersham for seven years and as founder and head of the IP department of Telenor for four years. Ann-Cathrin has comprehensive knowledge in handling IP portfolios, agreements and licensing of technology, IP due diligence, innovation capture and IP strategy. She has worked as head of the legal department at Onsagers for 17 years.

Contributed by: Ulrikke Asbøll and Ann-Cathrin Hoel, **Onsagers AS**

Onsagers AS

Munkedamsveien 35
0123 Oslo
Norway

Tel: +47 24 00 37 00
Email: uas@onsagers.no
Web: onsagers.com

Trade Secrets, Opportunities and Trends From a Business Perspective

Introduction

Challenging times give rise to new opportunities. There are currently significant and turbulent changes and challenges in the global economy, political alliances and with respect to the environment. Such changes impact and concern us all. In a maritime conference in Norway earlier this year, one of the questions to the US chargé d'affaires (diplomat) was about how the US is dealing with risks related to these uncertain times. The reply was, in part, to take steps to identify and protect intellectual property.

It is expected that AI will continue to move into our daily lives during 2024. The rapid proliferation of AI along with AI-driven innovation creates new business models, changes our lives in unexpected ways and illustrates that legislators did not have AI in mind when the legislation was created, although in relation to legal protection for inventions, most countries have concluded that AI cannot be the inventor.

In addition to AI, the UN's ESG reporting will also have a great impact on our lives. A consequence of ESG is the creation of new untraditional co-operations between companies to develop new solutions to fulfil ESG requirements. Yara, a well-known global company developing and offering fertiliser, now owns Yara Birkeland, the world's first fully electric and autonomous container vessel with zero emissions. With this container vessel set on water in 2023, Yara will reduce diesel-powered truck haulage by 40,000 journeys a year.

Furthermore, according to statistical research at Statistics Norway, in 2022 the number of patent filings in Norway decreased by 11% since 2021, and slightly lower in 2023. Independent of the reasons for this decrease, the trends in patent filing should be taken into account when considering the increasing focus on trade secrets.

All of this has an impact on the role of trade secrets in IP strategies, aiming for a robust IP protection for companies' competitive edge. In the US, trade secret litigation has increased, whilst this has not been the case in Norway after the Trade Secret Act 2020 came into force (nor before), as there have been just a handful of court cases relating to trade secrets for Norwegian courts. However, Norwegian companies and IP practitioners have an increased focus on identifying and protecting trade secrets alongside other forms of confidential information, with this being a particular focus for companies with current or potential foreign investors.

The key question within an IP policy has often been if an invention should be patented or kept as a trade secret, or alternatively if there should be a publication of the invention. However, a more nuanced question is how to combine patents and trade secrets to create an even stronger barrier around the invention, which will make it even more difficult for others to enter the market.

What is the difference between trade secrets and patents?

To acknowledge the interplay between trade secrets and patents, we need to understand what trade secrets are and the difference between trade secrets and patents.

What is the subject for patents and trade secrets?

A granted patent gives the inventor legal ownership of the invention (technical solution) – the product itself (product patent), how a product is made (process patent) and how it works.

Trade secrets are not limited to inventions with a technical solution, but embrace most kinds of information. In particular, information such as:

- know-how – a deep understanding of how to perform specific tasks, in-house processes for making the right business decision, methods to utilise and maintain machines, technologies and data, processes for management of people, and knowledge of failure/what does not work;
- technical information – drawings, production processes, software, recipes, and chemical compounds; and
- commercial information – client lists, supplier lists, prices and costs market studies, market intelligence, and launching date.

Legal requirements

For an invention to be patentable it must be new; ie, the invention cannot be published before the filing date of the patent application, and it must have an inventive step (ie, not be obvious to someone in that field), and have an industrial use.

For information to qualify as a trade secret, it needs to be of "commercial advantage" and it is required to take "reasonable steps" to keep the secrecy. If a competitor uses another company's trade secrets and this damages the company's competitive edge, it is regarded to be of "commercial advantage". "Reasonable steps" to keep the secrecy involves digital and/or physical access restrictions, internal guidelines on how to handle trade secrets, and a contractual duty of confidentiality, both for employers and third parties. In Norway there may also be an implied duty of confidentiality in certain circumstances.

Establishing patents and trade secrets

In order to achieve a patent, it is needed to draft, file and prosecute the patent application in the relevant jurisdictions, whilst a trade secret needs to be identified by the company and handled in accordance with the company's guidelines/policies on how to keep the secrecy. It is not possible to register a trade secret in Norway.

Publication

The patent application is published (18 months after the priority filing), and after the patent has expired, anyone, including competitors, can, in principle, legally produce a similar product. Publication is the trade-off by getting the exclusive right for 20 years, so others can use the invention for further innovation.

If the trade secret is disclosed without no duty of confidentiality, it will no longer be considered as a trade secret. To maintain legal protection of the trade secret, it must be kept secret.

Costs

Prosecution of a patent application may take many years and can involve significant costs, in addition to the annual renewal fees, especially if it is required to obtain patents in multiple international jurisdictions.

At first glance, the initial cost of a trade secret seems to be minimal compared with the costs of a patent. However, trade secrets need a system and a strategy to ensure that they are identified and correctly handled. This may include internal polices giving guidelines on how to handle them from a legal and technical point of view, educational awareness programmes for employers and employees, and confidentiality agreements. The cost for protection via trade secrets should still be significantly lower than filing a patent family and securing granted patent rights in multiple countries.

Lifetime

A patent typically expires after a maximum of 20 years, whilst trade secrets have no time limit as they can persist forever if they are not disclosed to the public or others, without an obligation of confidentiality. Trade secret protection will last as long as they stay secret.

Licence

Licences are an essential tool for technology transfer and exploitation of intellectual property rights. Both patents and trade secrets can be subject to a licence. Since patents protect technical solutions and trade secrets can protect know-how, licences combining trade secrets and patents can result in robust protection. Licence terms should be carefully drafted in order to control the handling of information that is protected as a trade secret, such as by restricting access to a specific set of employees of a licensee company and/or by setting minimum security requirements for IT systems.

Legal basis for litigation

Patents provide the owner with a right to exclude others from making, using, selling, offering to sell, or importing the invention. The patent owner can use the patent as a legal basis for claiming infringement of the owner's patent rights.

Trade secrets can be the basis for preventing others from misappropriating (ie, stealing) the trade secret. In other words, the ownership to a trade secret is not violated by someone who independently invented or reverse engineered the same technology.

The right to a trade secret can also be asserted against someone who illegally obtained or disclosed the trade secrets. Typically, breach of a contractual duty of confidentiality can result in trade secret infringement.

Trade secret or patent?

When deciding on filing a patent application or keeping a trade secret, it is important to take into account the commercial goals and context of the company.

A relevant factor to take into consideration before filing a patent application, is how easy it is for others to reverse engineer the invention once it is placed on sale. If reverse engineering is easy, it may be wise to file the patent application to avoid others having a free ride on your innovation, and, in the worst-case scenario, filing a patent application which may cause problems for your freedom to operate.

It may also be important to consider the ability to identify an infringement. For example, innovative products/services implemented using AI are often operated at least partly in the cloud, or otherwise remotely located from the user. In that case there are difficulties for reverse engineering and it may not be possible to detect if a third party is using a patented invention, since the relevant technical details are often not available for inspection.

For products that have a longer lifespan and cannot be reverse engineered, and/or for situations where an inability to detect infringement could reduce the benefit of patent protection, a well-guarded trade secret can provide protection without competition even after 20 years and at minimal cost.

If a new innovation is not regarded as inventive then it may not be worth drafting and filing a patent application, but rather consideration should be given to keeping it as a trade secret instead.

However, trade secrets protection requires that employees or third parties to whom the information is disclosed, can be trusted to understand and fulfil the duty of confidentiality. In principle, breach of confidentiality can be more difficult to prove than patent infringement as the initial source of the breach may be unclear. For this reason it is highly important to have a strong set of internal policies supported by suitably worded contracts/agreements.

Publication

An alternative and opposite option to trade secrets is publication of the information to prevent competitors gaining an exclusive patent right or trade secret. In this way a company can try to ensure freedom to operate, whilst avoiding any significant expense. The published information will be available for competitors to use freely on the market, but the publication blocks later filed patent applications that may bar others from the market. However, there is a risk that a Patent Examiner could overlook the publication or that a competitor may develop the initial innovation in a way that is unexpected, but gives them a commercial advantage.

Publishing can be achieved in several ways and through specific databases and online companies that Patent Examiners search through. Details of an invention on a public database that registers the time and date of publication can be used as an independent source of evidence against patent applications.

If a patent application is filed then the application can be withdrawn before the publication and the invention kept as a trade secret or abandoned to save costs. Or it may be allowed to publish since once published this will be a hindrance for other similar inventions submitted at a later date.

How can trade secrets and patents supplement each other?

In the early stages of R&D, before a patent application is filed and published, invention disclosure forms and all related know-how, including test results, and blind alleys, should be strictly confidential and are subjects for trade secret protection until it is decided to file a patent application, to keep it as a trade secret, or to use a defensive publication.

A relevant question is how much information should be disclosed in a patent application? The rule of thumb when it comes to disclosing trade secrets internally or externally, under the obligation of confidentiality, is to only disclose to a limited number of persons and only on a

need-to-know basis. The same applies for patent applications.

To achieve a granted patent, it is required to disclose a claimed invention in sufficient detail so that the person skilled in the art can carry out that claimed invention. However, it is not necessary to provide additional information about test results that are not necessary with regard to the sufficiency requirement. When drafting a patent application, it should be carefully considered if parts of the information can be kept as a trade secret or if it is necessary to include the information in the patent application, for example, to fulfil the requirement for sufficiency.

If it is necessary to disclose trade secrets to third parties, such as investors, risks should be considered before disclosure, and a non-disclosure agreement should be signed. The right to a patent can be lost by disclosing too much information before the application is filed. Trade secrets can be totally devoid if they are improperly (or accidentally) made public, including in discussions with investors. A suitable confidentiality agreement is therefore needed, taking account of relevant legal systems (eg, being drafted specifically for use under Norwegian law if Norwegian trade secrets are involved). It can also be important to consider other forms of protection in some cases, such as allowing third parties to inspect confidential material only on a restricted basis and limiting the ability to make or send copies.

Not all types of invention are capable of patenting, and so for some inventions, a trade secret will be the only option. Business methods, computer games and software implemented innovations (using AI or otherwise) that do not create technical effect, may be difficult to patent whilst also creating challenges for detecting infringements.

Trade secrets in the digital age

The digital age has made it possible to digitally store unlimited amounts of information within systems with shared, controlled and limited access to specific persons, passwords and surveillance, and details of when the information is accessed. Innovations such as blockchain, artificial intelligence and quantum cryptography contribute to enhanced trade secret security. However, cloud computing, remote work and the home office environment, and interconnected systems across borders create new practical, legislative and technological challenges in securing trade secrets against cyber-attacks, industrial espionage, and inadvertent leaks.

Open innovation with traditional and untraditional collaborations, licensed technology, IoT, big data, and machine learning enables rapidly developed and complex technology, requiring a comprehensive and multidisciplinary approach on how to protect trade secrets.

There are, in particular, two topics in which there is an increased focus when it comes to digital innovation and trade secrets.

IoT and sensor technology enables big data, which has revolutionised machine learning and related AI-based products/services. Selection of such input and output data can be patentable if it is related to solving a problem, and cloud-based solutions and quantum-computing-based solutions may be patentable. What can be decisive is if the patent applications can adequately describe the inner workings of the technology for which protection is being sought.

However, the input and output data may be better suited for trade secret protection instead, in particular if they are not protected by the database protection or similar legislation.

The digital wave of technology is still flushing over us, and trade secret protection needs to be dynamic with a proactive and adaptable approach in the light of patents, contracts, legal, technical and organisational measures.

Trade secrets from a company perspective

On- and off-boarding

When joining a new company, HR plays an important role in communicating values and priorities within the company and regarding the new job/position to new employees, and often plays the central role in the onboarding process.

At this stage, general awareness regarding the importance of IP and trade secrets and the role they play in the company should be communicated to new employees.

Also, the company policy on how to handle trade secrets and confidential information should be presented and communicated as part of the onboarding process.

Working from home represents a security risk and specific details regarding information data security when working from home should be a part of the onboarding programme. This could also represent a potential threat to preserving trade secrets and confidential information.

In this connection it should also be noted that junior employees generally have higher job mobility and therefore the company policy and associated training should make sure to properly define where to draw the line regarding information that belongs to the company, and, as such, that it should not be shared with others after the employee leaves, as well as specifying information the employee is free to share when moving on. Defining the boundaries and identifying the company's confidential information should be a general part of the off-boarding programme.

An explicitly defined duty of confidentiality along with non-compete clauses and other restrictive covenants must be a part of employment contracts to reduce the risk that confidential information and/or trade secrets could be spilled.

When an employee is leaving, it is important to check their computer/s for any stored data.

IP and trade secrets awareness training

It is important to work with IT on how to secure trade secrets and to prepare a restriction policy that limits access to all types of confidential and privileged information including trade secrets. In limiting the accessibility, the IT department plays a vital role.

IP awareness training should be conducted at regular intervals throughout the different parts of the organisation as it is essential that all employees understand the importance of handling trade secrets and other forms of IP in accordance with company guidelines. The IP awareness programme should be specifically designed for the different parts of the organisation.

It is especially important to understand which parts of the organisation have a role when it comes to IP, innovation and the handling of trade secrets – the "IP Triggers" in the organisation.

Product developments are generally potential IP Triggers and could also trigger the creation of trade secrets. Accordingly, it is particularly important that the parts of the organisation

where product development is occurring have a general IP and trade secrets awareness training programme.

The same is the case where it comes to adaptations, optimisations of production processes, or other product developments. Quite often these adjustments or optimisations could be protected as trade secrets.

Also, when working with third parties and entering into co-operation agreements, the chance of spilling a trade secret could be high. It is therefore important that descriptions of trade secrets are very precise and that descriptions and definitions in agreements are similarly narrow so that no unnecessary information is shared.

Many companies find that C-level (chief level) and senior level are more demanding to train and here it is important to stress that a signed NDA (non-disclosure agreement) does not mean that all information can be disclosed.

When it comes to an IP awareness programme for scientists, it is important to know that scientists need to know why the relevant IP policies are important. Emphasis should therefore be put on explaining the relevance of trade secrets to the business. In this connection it is also necessary to explain that extra diligence should be exerted when working with the trade secrets of third parties.

Also important is the handling of negative know-how which is information on what did not work. That can be very relevant information to a competing company.

Additionally, risk of contamination is imperative to consider. Contamination is when a third party shares information that has not been requested by the receiving party. Such information could prevent the possibilities of validly obtaining a patent or retaining a trade secret.

With regard to awareness training of the IP department and legal department, the extent of protection that can be obtained from an NDA or confidentiality agreement should be clarified.

A basic point is also that any innovation that is going into a patent application as a general rule is a trade secret and should be handled as such even though it may be published later during the patenting process.

When it comes to IP awareness training of the department of procurement, it is important to realise that this department often has extensive knowledge of the parts, designs and requirements of the innovative parts of the organisation. Ordering specially designed parts, fittings and other items to the production line or otherwise could result in the sharing of trade secrets and IP with third parties.

Procurement often also negotiates supply and delivery agreements with third parties and in this connection may be involved in indemnification clauses. Therefore, it is very important that procurement understands the concept of IP and trade secrets and what is required in order to protect and secure them and also what to expect in terms of indemnities and liabilities when receiving products that are produced under a licence from a third party.

Remuneration programme

Many innovative companies have remuneration programmes to stimulate employee innovation. Such stimulus generally drives innovation by offering compensation or bonus programmes

and is thereby designed to drive innovation in accordance with company goals.

Many such employee reward/recognition programmes focus on innovation resulting in patent applications, but as more companies learn more about trade secrets and understand the value and benefit of protecting innovation with trade secrets, it seems to be worth considering linking the remuneration programme to the innovation itself and not to whether it results in a patent application or not.

A trade secret can be a very valuable company asset if kept strictly confidential and has the very clear benefit that, contrary to patent applications which have to be published, a trade secret must be kept secret to keep its status as a trade secret. This means that other companies cannot base their innovation on the information in the trade secret. Arguably, a combination of trade secrets and patent applications, managed according to a strong IP strategy, can create a stronger protection of innovation than patent applications alone.

Therefore, a remuneration programme that focuses on the innovation itself, and not on whether it results in a patent application, trade secret, design protection or any other IP protection, is better designed to suit trends in business today.

Conclusion

The authors' experience shows that companies need practical and straightforward advice on how to handle trade secrets, along with regular awareness training.

Disclaimer: *This article is based on the authors' experience from various in-house IP functions and current roles as IP advisers, and it does not constitute legal advice.*

PHILIPPINES

Law and Practice

Contributed by:
Editha R. Hechanova, Chrissie Ann L. Barredo
and Yazmine A. Bajamundi-Pura
Hechanova Bugay Vilchez & Andaya-Racadio

Contents

Hechanova Bugay Vilchez & Andaya-Racadio is part of Hechanova Group with Hechanova & Co, Inc (HCI). It was established in 2005 and currently employs 58 professionals, including 15 lawyers, 30 engineers/technical professionals and 13 support staff. Its main office is located in Makati City. HCI is an intellectual property (IP) consulting firm, handling patents and trade marks prosecution, maintenance, search services, food and drug product registration, plant variety protection, copyright registration, IP valuation and IP consulting. HBVAR is a full-service law firm and deals with contentious IP, including enforcement, litigation, border-control measures, licensing and alternative dispute resolution. For the period 2017–2021, the IP-OPHL cited HCI as a top agent filer for invention patents and industrial design. The Group services Alpargatas SA, Mercedes Benz Group AG, Gilead SA, Mattel Inc, Panasonic Corporation, Hangzhou Dac Biotech Co, Ltd, and the Technology Application and Promotion Institute (DOST-TAPI), among others.

Authors

Editha R. Hechanova leads the intellectual property (IP) law practice of the Hechanova Group, comprising Hechanova & Co, Inc (where she is President/CEO, handling non-contentious IP) and the law firm Hechanova Bugay Vilchez & Andaya-Racadio (where she is managing partner, specialising in contentious IP). Editha graduated from the University of the East with a business degree and a major in accounting, magna cum laude. She is a certified public accountant. She obtained her law degree from the Ateneo de Manila University. She was cited by the Asia Business Law Journal as one of the Top 100 Lawyers in the Philippines for 2018–2023.

Chrissie Ann L. Barredo is a junior partner at the law firm Hechanova Bugay Vilchez & Andaya-Racadio. She has practised law since 2006, and has extensive experience and knowledge in intellectual property law, particularly trade marks and patent prosecution and litigation. She is a certified patent agent (since 2007), and is currently the Treasurer of the Association of PAQE Professionals, Inc (APP), an organisation consisting of those who have passed the Patent Agent Qualifying Examination (PAQE). She earned her bachelor's of science degree in Management Information Systems from the Ateneo de Manila University, and obtained her law degree from the University of the Philippines.

Contributed by: Editha R. Hechanova, Chrissie Ann L. Barredo and Yazmine A. Bajamundi-Pura,
Hechanova Bugay Vilchez & Andaya-Racadio

Yazmine A. Bajamundi-Pura is an associate lawyer of Hechanova Bugay Vilchez and Andaya-Racadio. She is licensed both as a lawyer and as a medical doctor. She earned her bachelor's of science degree in Psychology from the University of the Philippines. She then gained her doctor of medicine degree from San Beda College of Medicine. Thereafter, she attained her juris doctor degree from the Philippine Christian University. She has also graduated from several training programmes, such as the WIPO Summer School and the IPOPHL's Intellectual Property (IP) Masterclass. Besides IP law, she loves teaching and is currently a law instructor in certain law schools.

Hechanova Bugay Vilchez & Andaya-Racadio

GF Salustiana D Ty Tower
104 Paseo De Roxas Ave
Makati City 1229
Philippines

Tel: +632-8888-4293
Fax: +632-8888-4290
Email: mail@hechanova.com.ph
Web: www.hechanova.com.ph

Contributed by: Editha R. Hechanova, Chrissie Ann L. Barredo and Yazmine A. Bajamundi-Pura,
Hechanova Bugay Vilchez & Andaya-Racadio

1. Legal Framework

1.1 Sources of Legal Protection for Trade Secrets

There is no specific law protecting trade secrets (also known as undisclosed information) in the Philippines, though there are different Philippine statutes that apply to the protection of trade secrets and that penalise the revelation of such trade secrets.

Article 4(g) of the Republic Act 8293 as well as the Intellectual Property Code of the Philippines includes "protection of undisclosed information" or trade secrets under the term "intellectual property rights".

Article 40(f) of the Republic Act 7394 as well as the Consumer Act of the Philippines prohibit "the using by any person to his own advantage, or revealing, other than to the Department or to the courts when relevant in any judicial proceeding under this Act, any information concerning any method or process which as a trade secret is entitled to protection".

Article 292 of the Revised Penal Code penalises the revelation of industrial secrets, as follows: "The penalty of *prision correccional* in its minimum and medium periods and a fine not exceeding 500 pesos shall be imposed upon the person in charge, employee or workman of any manufacturing or industrial establishment who, to the prejudice of the owner thereof, shall reveal the secrets of the industry of the latter."

Under Rule 27 of the Rules of Court, a court, upon motion, may order the production or inspection of documents or things *which are not privileged*, and which constitute evidence material to any matter involved in the action.

In the case of Air Philippines Corp v Pennswell (GR No 172835, 13 December 2007), the Supreme Court had occasion to define what a trade secret is: a plan or process, tool, mechanism or compound known only to its owner and those of their employees with whom it is necessary to confide.

The definition also extends to a secret formula or process not patented but known only to certain individuals using it in compounding some article of trade having a commercial value. A trade secret may consist of any formula, pattern, device or compilation of information that:

- is used in one's business; and
- gives the employer an opportunity to obtain an advantage over competitors who do not possess the information.

Generally, a trade secret is a process or device intended for continuous use in the operation of the business – for example, a machine or formula – but can be a price list or catalogue, or a specialised customer list.

In another case, the Supreme Court upheld the validity of the policy of a pharmaceuticals company prohibiting its employees from marrying employees of any competitor company, on the rationalisation that the company had a right to guard its trade secrets, manufacturing formulas, marketing strategies and other confidential programmes and information from competitors (Duncan Association of Detailman-PTGWO v Glaxo Wellcome Philippines, Inc, GR No 162994, 17 September 2004).

1.2 What Is Protectable as a Trade Secret

Based on existing Philippine laws and jurisprudence, any information that can fall within the

definition of a trade secret can be protected. In Air Philippines v Pennswell, the Supreme Court adopted the following factors to determine whether information is a trade secret:

- the extent to which the information is known outside the employer's business;
- the extent to which the information is known by employees and others involved in the business;
- the extent of measures taken by the employer and competitors;
- the value of the information to the employer and competitors;
- the amount of effort or money expended by the company in developing the information; and
- the extent to which the information could be easily or readily obtained through an independent source.

1.3 Examples of Trade Secrets

There is very little case law in the Philippines involving trade secrets. The following are some examples, including applicable statutes.

Air Philippines v Pennswell (GR No 172835, 13 December 2007): in this case, the composition, formulation and ingredients of the subject lubricant were declared by the Supreme Court as a trade secret and therefore as privileged against compulsory disclosure.

Universal Food Corporation (UFC) v Court of Appeals, Magdalo Victoriano Francisco Sr (GR L-29155, 13 May 1970): in this case, the Supreme Court ordered UFC to return and restore to the plaintiff (Magdalo Victoriano Francisco, Sr) the right to the use of his Mafran sauce trade mark and formula. UFC and all its assignees and successors were permanently enjoined, effective immediately, from using in any manner said Mafran sauce trade mark and formula.

Tiu v Platinum Plans Phils (GR No 163512, 28 February 2007). The petitioner Tiu was re-hired by the respondent Platinum (which was engaged in the pre-need business) as senior assistant vice-president. The employment contract carried a non-involvement clause which prevented her from being employed or engaged in the pre-need business, whether directly or indirectly, for a period of two years from separation of employment, and breaching this rendered the employee liable for PHP100,000 (about USD1,800).

In 1995, Tiu stopped reporting for work, and it turned out that she had become vice-president of a corporation that was also in the pre-need industry. Platinum sued Tiu for damages for violating the non-involvement clause. Tiu countered that the non-involvement clause was unenforceable as being against public order or public policy. Platinum argued that the inclusion of the two-year non-involvement clause in the contract of employment was reasonable and necessary since her job gave her access to the company's confidential marketing strategies.

The Supreme Court held that a non-involvement clause is not necessarily void for being in restraint of trade, as long as there are reasonable limitations as to time, trade and place. In this case, the non-involvement clause had a time limit (two years from the time employment ended) and was also limiting as to trade since it only prohibited the petitioner from engaging in any pre-need business similar to Platinum.

More significantly, since Tiu was the senior asstistant vice-president and territorial operations head in charge of Platinum's Hong Kong and ASEAN operations, she had been privy to con-

fidential and highly sensitive marketing strategies of the respondent's business. To allow her to engage in a rival business soon after she left would make Platinum's trade secrets vulnerable, especially in a highly competitive marketing environment. In summary, the authors find the non-involvement clause to be not contrary to public welfare and not greater than affordably necessary.

As mentioned previously, in Duncan Association of Detailman-PTGWO v Glaxo Wellcome Philippines, Inc, GR No 162994, 17 September 2004, the Supreme Court upheld the validity of the policy of a pharmaceuticals company prohibiting its employees from marrying employees of any competitor company, on the rationalisation that the company had a right to guard its trade secrets, manufacturing formulas, marketing strategies and other confidential programmes and information from competitors.

Section 12 of the Republic Act No 6969 and the Toxic Substances and Hazardous and Nuclear Waste Control Act of 1990 provide for the following as confidential subject matter: "production or sales figures or methods, production or processes unique to such manufacturer, processor or distributor, or [that] would otherwise tend to adversely affect the competitive position of such manufacturer, processor or distributor."

The Securities Regulations Code Rule 66.3.2 – Amended Implementing Rules and Regulations states that confidential information includes:

- trade secrets;
- commercial or financial information prepared by analysts within or outside a company for strategic purposes; and
- similar information that raises concerns regarding business confidentiality.

1.4 Elements of Trade Secret Protection

See **1.2 What Is Protectable as a Trade Secret**.

1.5 Reasonable Measures

As stated previously, in Duncan v Glaxo (GR No 162994, 17 September 2004), the Supreme Court upheld the validity of the policy of a pharmaceuticals company prohibiting its employees from marrying employees of any competitor company, on the rationalisation that the company had a right to guard its trade secrets, manufacturing formulas, marketing strategies and other confidential programmes and information from competitors. In its decision, the Court held the following:

"The prohibition against personal or marital relationships with employees of competitor companies upon Glaxo's employees is reasonable under the circumstances because relationships of that nature might compromise the interests of the company. In laying down the assailed company policy, Glaxo only aims to protect its interests against the possibility that a competitor company will gain access to its secrets and procedures. That Glaxo possesses the right to protect its economic interests cannot be denied. No less than the Constitution recognises the right of enterprises to adopt and enforce such a policy to protect its right to reasonable returns on investments and to expansion and growth. Indeed, while our laws endeavour to give life to the constitutional policy on social justice and the protection of labour, it does not mean that every labour dispute will be decided in favour of the workers. The law also recognises that management has rights which are also entitled to respect and enforcement in the interest of fair play."

1.6 Disclosure to Employees

The availability of protection for trade secrets is not affected if the information was disclosed to

the employee in the course of their employment, and if the employee was made aware that it was a trade secret and needed to be protected. Article 292 of the Revised Penal Code penalises the revelation of the employee to other persons of the secrets of their employer.

1.7 Independent Discovery

In Cocoland v National Labour Relations Commission (GR No 98458, 17 July 1996), the Supreme Court disregarded the claim of the employer Cocoland that its technology was a trade secret. Here, it was actually the dismissed employee who established in the course of the proceedings that the purported secret propagation technique was no longer a secret, as it had attained wide currency via government publications and leaflets. As such, the Court declared that the employee's termination on the grounds of unauthorised disclosure of trade secrets was unfounded and without valid cause.

1.8 Computer Software and Technology

No specific law in the Philippines provides protection for trade secrets unique to computer software and/or technology. However, offences against the confidentiality, integrity and availability of computer data and systems may be penalised under the Republic Act 10175 or the Cybercrime Prevention Act of 2012.

1.9 Duration of Protection for Trade Secrets

Trade secrets may be protected through non-disclosure agreements (NDAs) or confidentiality agreements. These are basically contractual in nature, and as such, the period of validity or protection will depend on the period stated in the NDA. Such NDA may also indicate that the confidentiality be maintained even after the termination of an employee.

1.10 Licensing

In the Philippines, trade secrets do not require registration or licensing. An owner that granted a licence to use such trade secret may utilise an NDA or a confidentiality agreement to maintain or protect its trade secret.

1.11 What Differentiates Trade Secrets From Other IP Rights

Certain types of intellectual property (IP) rights, such as patents and trade marks, may be protected through registration with the Intellectual Property Office of the Philippines (IPOPHL). However, trade secrets cannot be registered.

Complaints concerning violation of IP rights may be filed either with the IPOPHL or the regional trial court. Conversely, breach of an NDA covering trade secrets may result in claims for damages, monetary claims, termination from employment or even criminal complaints, which should be filed with the regular courts.

1.12 Overlapping IP Rights

It is possible for a plaintiff to assert their rights over trade secrets along with other IP rights – for example, regarding patent or copyright infringement.

1.13 Other Legal Theories

A claim for damages for breach of fiduciary duty or tortious interference may be filed against the obligor if such acts resulted in pecuniary loss to the obligee (Article 2199 of the Civil Code). If there is no proof of pecuniary loss, a claim for other types of damages such as moral (Article 2217 of the Civil Code) or nominal (Article 2221 of the Civil Code) damages may be filed against the obligor.

1.14 Criminal Liability

Revelation of industrial secrets is penalised under Article 292 of the Revised Penal Code, which states as follows:

"The penalty of *prision correccional* (six months and one day to six years) in its minimum and medium periods and a fine not exceeding 500 pesos shall be imposed upon the person in charge, employee or workman of any manufacturing or industrial establishment who, to the prejudice of the owner thereof, shall reveal the secrets of the industry of the latter."

Since every person criminally liable for a felony is also civilly liable (Article 100, Revised Penal Code), a trade secret owner may pursue both civil and criminal claims.

Violation of Article 40(f) of the Consumer Act (revelation of trade secrets) is penalised as follows:

"Any person who violates any of the provisions of Article 40 hereof shall, upon conviction, be subject to imprisonment of not less than one year but not more than five years, or a fine of not less than five thousand pesos but not more than ten thousand pesos, or both such imprisonment and fine, in the discretion of the court."

1.15 Extraterritoriality

If the trade secret owner can prove pecuniary loss due to misappropriation that happened in another country, they can still file a claim for damages here as long as they can prove that they have a juridical personality for filing a case in the Philippines (eg, a natural person – a Filipino citizen, or a corporation with Philippine nationality).

2. Misappropriation of Trade Secrets

2.1 The Definition of Misappropriation

Although there is no available jurisprudence or statutes which cover trade secret misappropriation in the Philippines, the required elements can be based on the elements of claims for damages and the crime of revelation of industrial secrets.

The elements for a claim of actual damages are:

- the fact of the injury or loss; and
- the actual amount of loss, with a reasonable degree of certainty premised on competent proof and the best evidence available.

The elements of Article 292 on revelation of industrial secrets include that:

- the offender is an employee or officer in charge of the industrial establishment;
- the industrial establishment has a secret which the offender has learned;
- the offender reveals the secret; and
- prejudice was caused to the owner.

It is important to prove that there was loss, injury or prejudice caused to the owner of the trade secret.

2.2 Employee Relationships

If the trade secret misappropriation involves an employee of the owner, provisions of the Labour Code may also apply, such as regards:

- termination of an employee on the grounds of serious misconduct;
- wilful disobedience with the lawful orders of the employer (Article 297(a)); or
- fraud or wilful breach by the employee of the trust reposed in them by the employer (Article 297(c)).

There is no particular obligation owed by the employee to the employer in such case, aside from the damages that may be caused to the employer/trade secret owner.

2.3 Joint Ventures

A joint venture was defined by the Supreme Court (see Valdes v La Colina Development, GR No 208140, 12 July 2021) as akin to a partnership – the essential elements of which are as follows:

- an agreement to contribute money, property or industry to a common fund; and
- an intention to divide the profits among the contracting parties.

Thus, the laws on partnerships will apply to joint ventures. Although there is no specific reference to trade secrets in laws governing partnerships or joint ventures, or in jurisprudence, it can be assumed that laws governing obligations and property involving joint ventures/partnerships will also govern obligations between joint venturers with respect to trade secrets.

2.4 Industrial Espionage

There is no specific statue that covers industrial espionage involving trade secrets in the Philippines. Thus, any damages incurred from such espionage may be filed under claims for damages or criminal complaints such as theft, and may be filed with the regular courts.

3. Preventing Trade Secret Misappropriation

3.1 Best Practices for Safeguarding Trade Secrets

There are currently no recognised best practices in the Philippines for safeguarding trade secrets.

3.2 Exit Interviews

Employees usually sign a non-compete or confidentiality agreement during the onboarding process. It is not common for them to sign such confidentiality agreement during an exit process. Many employers would also enquire as to the nature of the new position that the departing employee will undertake.

4. Safeguarding Against Allegations of Trade Secret Misappropriation

4.1 Pre-existing Skills and Expertise

Courts may or may not recognise the doctrine of "inevitable disclosure" (more commonly known as the "non-compete clause" in the Philippines) in employment contracts, depending on the reasonableness of such clause. This issue was discussed by the Supreme Court in Rivera v Solidbank (GR No 163269, 19 April 2006), where the Court explained that, in determining whether the contract is reasonable or not, the trial court should consider the following factors:

- whether the covenant protects a legitimate business interest of the employer;
- whether the covenant creates an undue burden on the employee;
- whether the covenant is injurious to the public welfare;
- whether the time and territorial limitations contained in the covenant are reasonable; and
- whether the restraint is reasonable from the standpoint of public policy.

4.2 New Employees

In the Philippines, there is currently no recognised best practice for onboarding programmes that involve minimising trade secret misappro-

priation. An approach taken by some employers is to ask the potential employee whether they have signed any NDA, and if so whether it is still in force.

5. Trade Secret Litigation

5.1 Prerequisites to Filing a Lawsuit

Since theft is a crime in the Philippines, civil liability arising from such crime is deemed as instituted with the criminal action for the theft (Rule 111, Rules of Court). As such, to initiate a criminal/civil action for theft of trade secrets, a formal complaint with the police is necessary. The blotter issued by the police, along with other pieces of evidence related to the theft, must be gathered and preserved.

A complaint should thereafter be filed with the prosecutor's office which has jurisdiction over the area where the theft took place. The prosecutor will then conduct a preliminary investigation. If the prosecutor finds sufficient merits, it shall then issue a resolution and file information with the proper court.

5.2 Limitations Period

If the trade secret claim is based on claims of damages, the prescription period for filing a claim for damages is four years (Article 1146, Civil Code).

5.3 Initiating a Lawsuit

The owner should gather all their evidence and prepare a complaint with the assistance of a counsel. The complaint for damages should then be filed with the special commercial court (if available) within the territory of the owner, or with the proper courts, depending on the amount being claimed by the owner.

5.4 Jurisdiction of the Courts

Some regional trial courts exist that are designated as special commercial courts, and which are empowered to hear and decide on IP rights violations.

5.5 Initial Pleading Standards

Trade secrets claims are not common in the Philippines. Like any other claim, there must be concrete evidence of the loss or injury caused to the owner by the misappropriation of the trade secret before such a claim may be filed.

5.6 Seizure Mechanisms

Special commercial courts in Quezon City, Maila, Makati and Pasig have the authority to act on applications for the issuance of writs of search and seizure in civil actions regarding violations of the IP Code, which will be enforceable nationwide (Rule 2, Section 2, AM No 10-3-10-SC, Rules of Procedure for Intellectual Property Rights Cases).

5.7 Obtaining Information and Evidence

Modes of discovery – such as interrogatories, requests for admission, and production or inspection of documents or things – may be availed of not later than 30 days from the joinder of the issues of the case (Rule 5, AM No 10-3-10-SC, Rules of Procedure for Intellectual Property Rights Cases).

5.8 Maintaining Secrecy While Litigating

Requests for closed-door hearings in cases involving trade secrets or undisclosed information may be set forth by the parties in their pretrial brief (Rule 6, Section 1, AM No 10-3-10-SC, Rules of Procedure for Intellectual Property Rights Cases).

5.9 Defending Against Allegations of Misappropriation

Although there are no specific defences for trade secret litigation, in one case the Supreme Court held that the widespread knowledge of a supposedly secret technology rendered the claim of the petitioner without basis. See **1.7 Independent Discovery**.

5.10 Dispositive Motions

Dispositive motion is not available in the Philippines. However, parties will need to undergo mediation proceedings prior to the trial. If the parties come to an amicable settlement during mediation, they do not need to go through with the trial.

5.11 Cost of Litigation

Contingent fee arrangement are valid in the Philippines (see Taganas v National Labour Relations Commission, GR No 118746, 7 September 1995). Aside from the professional fees of lawyers, the filing fee for the complaint will also need to be paid by the complainant. Such filing fees vary depending on the amount of damages being claimed.

6. Trial

6.1 Bench or Jury Trial

All actions filed before Philippine courts are decided by a judge. Administrative actions filed before administrative agencies performing quasi-judicial functions (such as the IPOPHL for instance) are decided by an adjudication or hearing officer at the first level.

6.2 Trial Process

Civil Cases Before the Special Commercial Courts

The Rules of Procedure for Intellectual Property Rights Cases are observed by the regional trial courts designated by the Supreme Court as special commercial courts. Said courts have jurisdiction over commercial cases, including IP violation cases, such as unfair competition.

Actions are initiated by the filing of a verified complaint, which must contain a concise statement of the ultimate facts constituting the complainant's cause or causes of action, and must specify the relief(s) sought. Judicial affidavits submitted with the complaint should state only facts of direct personal knowledge of the affiants which are admissible in evidence, and should also show the competence of the affiants to testify to the matters stated therein.

The defendant must file their answer to the complaint within 15 days from service of summons.

A party can avail of any of the modes of discovery not later than 30 days from the joinder of issues. Any mode of discovery may be objected to *on the ground that the matter requested is undisclosed information or privileged information*, among other grounds provided by the law.

The case will then be set for pretrial and the parties will be directed to submit their respective pretrial briefs. In their pretrial briefs, the parties may set forth *requests for closed-door hearings in cases involving trade secrets, undisclosed information and patents*, among other matters.

Upon the parties' appearance at the pretrial, the court shall order them to appear before the Philippine Mediation Center in accordance with mediation rules of the Supreme Court. If the parties fail to settle the case after mediation, the pairing court shall conduct judicial dispute resolution (JDR) conferences upon request of the court handling the case. If either mediation or JDR fails, the case will be returned to the court for the pretrial.

Where the case is submitted for decision immediately after pretrial, the court shall render judgment within 45 days.

If the court deems it necessary to hold trial, the court shall include in the pretrial order the schedule of hearings to be conducted expeditiously and completed not later than 60 days from the date of the initial trial. The judicial affidavits shall serve as the direct testimonies of the witnesses during trial, subject to cross-examination by the adverse party.

Immediately after an oral ruling on the last offer of evidence, the court shall order the parties to simultaneously submit their respective draft decisions within 30 days.

Within 60 days after receipt of the draft decision of the parties, the court shall render judgment.

Unless restrained by a higher court, the judgment of the court shall be executory, even pending appeal, under such terms and conditions as the court may prescribe.

Administrative Actions Before the IPOPHL's Bureau of Legal Affairs (BLA)

Administrative actions for unfair competition before the BLA follow a similar trial procedure. However, since IP violation actions before the BLA are administrative in nature, they are not strictly governed by technical rules of procedure and evidence.

6.3 Use of Expert Witnesses

Any party may present the testimony of an expert witness. According to the Revised Rules on Evidence, as amended by AM No 19-08-15 SC, the opinion of a witness may be received in evidence when on a matter requiring special knowledge, skill, experience, training or education, which they are shown to possess.

The testimony of an expert witness is presented by the submission of said witness's judicial affidavit as forming part of the verified complaint or the defendant's verified answer. The affidavit must be in a question-and-answer format numbered consecutively, and must show the competence of the witness to testify to the matters stated therein. The judicial affidavit shall serve as the direct testimony of the expert witness during trial, subject to cross-examination by the adverse party.

According to Rule 133, Section 5 of AM No 19-08-15 SC, in any case where the opinion of an expert witness is received in evidence, the court has a wide discretion in determining the weight to be given to such opinion, and for that purpose may consider the following:

- whether the opinion is based upon sufficient facts or data;
- whether it is the product of reliable principles and methods;
- whether the witness has applied the principles and methods reliably to the facts of the case; and
- such other factors as the court may deem helpful for making the determination.

7. Remedies

7.1 Preliminary Injunctive Relief

A preliminary injunction may be granted by the courts and the BLA of the IPOPHL at any stage of an action or proceeding, prior to the judgment or final order, requiring a party, court, agency or person to refrain from a particular act or acts. It may also require the performance of a particular act or acts, in which case it shall be known as a preliminary mandatory injunction. It persists until it is dissolved or until the termination of the action without the court issuing a final injunction.

A preliminary injunction may be granted when it is established that:

- the applicant is entitled to the relief demanded, and the whole or part of such relief consists in restraining the commission or continuance of the act or acts complained of, or in requiring the performance of an act or acts, either for a limited period or perpetually;
- the commission, continuance or non-performance of the act or acts complained of during the litigation would probably work injustice to the applicant; or
- a party or any person is doing or threatening, is attempting to do, or is procuring or suffering to be done some act or acts probably in violation of the rights of the applicant respecting the subject of the action or proceeding, and tending to render the judgment ineffectual.

Unless exempted by the court, a preliminary injunction or temporary restraining order may be granted only when the applicant files with the court (where the action or proceeding is pending) a bond executed to the party or person enjoined, in an amount to be fixed by the court, to the effect that the applicant will pay to such party or person all damages which they may sustain by reason of the injunction or temporary restraining order if the court should finally decide that the applicant was not entitled thereto. Upon approval of the requisite bond, a writ of preliminary injunction shall be issued.

See Rule 58, 2019 Amendments to the 1997 Rules of Civil Procedure; Rule 5, IPOPHL Rules and Regulations on Administrative Complaints for Violation of Laws Involving Intellectual Property Rights.

7.2 Measures of Damages

Although the IP Code includes the protection of undisclosed information as an IP right, it does not provide for a relief or remedy in the case of infringement of a trade secret or undisclosed information. In the IP Code, civil actions for infringement are available to:

- patentees;
- anyone possessing any right, title or interest in and to the patented invention; and
- owners of a registered trade mark.

However, the unlawful use of trade secrets or undisclosed information may fall within *unfair competition*, which the IP Code defines as being committed by any person who employs deception or any other means contrary to good faith by which they pass off the goods manufactured by them or in which they deal, or their business or services, for those of the one having established such goodwill, or who commits any acts calculated to produce said result.

Since trade secrets are commonly protected by contract, a party whose trade secrets have been unlawfully disclosed in violation of contractual stipulations may file a civil action for breach of contract and damages. Damages may be:

- actual or compensatory;
- moral;
- nominal;
- temperate or moderate;
- liquidated; or
- exemplary or corrective.

Since *actual damages* are awarded to compensate for a pecuniary loss, the injured party is required to prove two things:

- the fact of the injury or loss; and

- the actual amount of loss with a reasonable degree of certainty premised upon competent proof and on the best evidence available (see Yamauchi v Suñiga, GR No 199513, 18 April 2018).

Nominal damages are recoverable where a legal right is technically violated, and must be vindicated against an invasion that has produced no actual present loss of any kind or where there has been a breach of contract and no substantial injury or actual damages whatsoever have been or can be shown. See Seven Brothers Shipping Corporation v DMC-Constructions Resources, Inc, GR No 193914, 26 November 2014.

Temperate or moderate damages, which are more than nominal but less than compensatory damages, may be recovered when the court finds that some pecuniary loss has been suffered but its amount cannot, from the nature of the case, be provided with certainty. Temperate damages must be reasonable under the circumstances.

Liquidated damages are those agreed upon by the parties to a contract, to be paid in the case of breach thereof. When the breach of the contract committed by the defendant is not the one contemplated by the parties when agreeing upon the liquidated damages, the law shall determine the measure of damages, and not the stipulation.

Moral damages are recoverable for breach of contract where the breach was wanton, reckless, malicious or in bad faith, oppressive or abusive. However, moral damages are improperly awarded in the absence of a specific finding and pronouncement from the trial court that a party acted in such manner. See FAJ Construction and Development Corp v Saulog, GR No 200759, 25 March 2015.

Exemplary or corrective damages are imposed by way of example or correction for the public good, in addition to the moral, temperate, liquidated or compensatory damages. In contracts and quasi-contracts, the court may award exemplary damages if the defendant acted in a wanton, fraudulent, reckless, oppressive or malevolent manner.

7.3 Permanent Injunction

A successful trade secret claimant may be granted an injunction.

The Supreme Court has held that the inventor, discoverer or possessor of a trade secret or similar innovation has rights therein which may be treated as property, and *ordinarily an injunction will be granted to prevent the disclosure of the trade secret* by one who obtained the information "in confidence" or through a "confidential relationship". See Air Philippines Corporation v Pennswell, Inc, GR No 172835, 13 December 2007.

To be entitled to the injunctive writ, the petitioner must show that:

- there exists a clear and unmistakable right to be protected;
- this right is directly threatened by the act sought to be enjoined;
- the invasion of the right is material and substantial; and
- there is an urgent and paramount necessity for the writ to prevent serious and irreparable damage.

See AMA Land, Inc v Wack Wack Residents' Association, Inc, GR No 202342, 19 July 2017.

7.4 Attorneys' Fees

As a general rule, the parties may stipulate the recovery of attorneys' fees. In the absence on

such stipulation, Article 2208 enumerates the instances when attorneys' fees and litigation expenses (other than judicial costs) may be recovered – ie:

- when exemplary damages are awarded;
- when the defendant's act or omission has compelled the plaintiff to litigate with third persons or to incur expenses to protect their interest;
- in criminal cases of malicious prosecution against the plaintiff;
- in the case of a clearly unfounded civil action or proceeding against the plaintiff;
- where the defendant acted in gross and evident bad faith in refusing to satisfy the plaintiff's plainly valid, just and demandable claim;
- in actions for legal support;
- in actions for the recovery of wages of household helpers, labourers and skilled workers;
- in actions for indemnity under workmen's compensation and employer's liability laws;
- in a separate civil action to recover civil liability arising from a crime;
- when at least double judicial costs are awarded; and
- in any other case where the court deems it just and equitable that attorneys' fees and litigation expenses should be recovered.

In all cases, the attorneys' fees and litigation expenses must be reasonable.

The Supreme Court has held that an award of attorneys' fees demands factual, legal and equitable justification to avoid speculation and conjecture surrounding the granting thereof. Owing to the special nature of the awarding of attorneys' fees, a rigid standard is imposed on the courts before these fees can be granted. As such, it is imperative that the court's decisions clearly and distinctly set forth the basis for the awarding thereof, and it is not enough that they merely state the amount of the grant in the dispositive portion of their decisions.

Since the award of attorneys' fees is an exception rather than the general rule, there must be compelling legal reasons for bringing the case within the exceptions provided under Article 2208 of the Civil Code to justify the award. See Philippine National Construction Corporation v APAC Marketing Corporation, GR No 190957, 5 June 2013.

7.5 Costs

As described in **7.4 Attorneys' Fees** and similar thereto, in the absence of stipulation, *litigation expenses* cannot be recovered except under the circumstances enumerated in Section 2208 of the Civil Code. In all cases, litigation expenses must be reasonable.

8. Appeal

8.1 Appellate Procedure

Any party may appeal a judgment or final order of the courts and of the BLA.

Actions With the BLA

Decisions or final orders rendered by the Director of the BLA may be appealed to the Director General, and this is effected by filing an appeal memorandum within 30 days from notice of an appealed decision or final order. The appeal shall be perfected by:

- filing the appeal memorandum in the ODG;
- proof of service of a copy on the appellee and the BLA's Director; and
- proof of payment of the appeal fee and other applicable fees.

Interlocutory orders shall not be appealable to the Director General.

The Director General's decision or order shall be final and executory 15 days after receipt of a copy thereof by the parties, unless appealed to the Court of Appeals in the case of appeals of BLA decisions or final orders. No motion for consideration of the decision or order of the Director General shall be allowed.

Actions With the Special Commercial Court

All decisions and final orders rendered by the special commercial court shall be appealable to the Court of Appeals through a petition for review under Rule 43 of the Rules of Court. The petition for review shall be taken within 15 calendar days from notice of the decision or final order of the regional trial court designated by the Supreme Court as a special commercial court.

Upon proper motion and the payment of the full amount of the legal fees prescribed, and before the expiry of the reglementary period, the Court of Appeals may grant an additional period of 15 calendar days within which to file the petition for review. No further extension shall be granted except for the most compelling reasons, and shall in no case exceed 15 calendar days.

No appeal may be taken from an interlocutory order. In such an instance, the aggrieved party may file an appropriate special civil action under Rule 65 (certiorari, prohibition and mandamus). For example, when any tribunal, board or officer exercising judicial or quasi-judicial functions has acted without or in excess of their jurisdiction, or with grave abuse of discretion amounting to lack or excess of jurisdiction, and when there is no appeal or any plain, speedy and adequate remedy in the ordinary course of law, a person aggrieved thereby may file a verified *petition for certiorari* (under Rule 65) in the proper court.

The petition should be filed not later than 60 days from notice of the judgment, order or resolution. If a motion for reconsideration or new trial is filed timely, whether such motion is required or not, the petition should be filed not later than 60 days counting from the notice of denial of the motion.

Appealing a Judgment, Final Order or Resolution of the Court of Appeals

A party desiring to appeal a judgment, final order or resolution of the Court of Appeals, the regional trial court or other courts, may file a verified *petition for review on certiorari under Rule 45* with the Supreme Court. The petition may include an application for a writ of preliminary injunction or other provisional remedies, and *should raise only questions of law*, which must be distinctly set forth.

The petition should be filed within 15 days from notice of the appealed judgment, final order or resolution, or of the denial of the petitioner's motion for new trial or reconsideration filed in due time after notice of the judgment. Following a motion duly filed and served, with full payment of the docket and other lawful fees and the deposit for costs before the expiry of the reglementary period, the Supreme Court may, for justifiable reasons, grant an extension of 30 days only within which to file the petition.

8.2 Factual or Legal Review

Court of Appeals

The Court of Appeals has the power to try cases and conduct hearings, receive evidence and perform any and all acts necessary to resolve factual issues raised in cases falling within its *original and appellate jurisdiction*, including the power to grant and conduct new trials or further proceedings.

The Court of Appeals, acting as an appellate court, is still a trier of facts. Parties can raise

questions of fact before the Court of Appeals, and it will have jurisdiction to rule on these matters. Otherwise, if only questions of law are raised, the appeal should be filed directly before the Supreme Court. This is not to say that the trial court's findings of fact are of little weight. It is a time-honoured rule that the trial court's findings of fact are given much weight because of the trial court judges' first-hand knowledge and familiarity with the disposition of the witnesses who testified before them, and this is important in certain cases. However, this doctrine does not diminish the Court of Appeals' jurisdiction in reviewing the factual findings of the trial court. See Pascual v Burgos et al, GR No 171722, 11 January 2016.

Supreme Court

Appeal by certiorari

In all cases *where only questions of law are raised or involved*, the appeal shall be to the Supreme Court by *petition for review on certiorari* in accordance with Rule 45.

Certiorari, prohibition and mandamus under Rule 65

See **8.1 Appellate Procedure**.

9. Criminal Offences

9.1 Prosecution Process, Penalties and Defences

The law does not provide for criminal prosecution of trade secret theft. However, the following provisions in the Revised Penal Code (RPC) and National Internal Revenue Code provide protection to trade secrets.

Revised Penal Code

Revealing secrets with abuse of office – Article 291 of the RPC imposes the penalty of *arresto mayor* and a fine not exceeding PHP500 on any manager, employee or servant who, in such capacity, learns the secrets of their principal or master and reveals such secrets.

Revelation of industrial secrets – Article 292 of the RPC imposes the penalty of *prision correccional* in its minimum and medium periods and a fine not exceeding PHP500 on the person in charge, employee or workman of any manufacturing or industrial establishment who, to the prejudice of the owner thereof, reveals the secrets of the industry of the latter.

National Internal Revenue Code (NIRC)

Section 278 of the NIRC imposes the penalty of imprisonment of not less than six months and not more than five years, or a fine of not more than PHP2,000, or both, on any person who causes or procures an officer or employee of the Bureau of Internal Revenue to divulge any confidential information regarding the business, income or inheritance of any taxpayer, knowledge of which was acquired by them in the discharging of their official duties and which it is unlawful for them to reveal. The penalty also applies to any person who publishes or prints, in any manner whatsoever not provided by law, any income, profit, loss or expenditure appearing in any income tax return.

10. Alternative Dispute Resolution (ADR)

10.1 Dispute Resolution Mechanisms

Mediation as a mode of alternative dispute resolution (ADR) is mandatory at the IPOPHL and at the regular trial courts, including the special commercial courts.

While there are no considerations that are unique to the use of ADR for trade secrets, the Alternative Dispute Resolution Act of 2004 (RA No 9285) protects the confidentiality of information obtained through mediation proceedings by setting forth the following guidelines, subject to certain exceptions.

- Information obtained through mediation shall be privileged and confidential.
- A party, mediator or non-party participant may refuse to disclose and may prevent any other person from disclosing a mediation communication.
- Confidential information shall not be subject to discovery and shall be inadmissible in any adversarial proceeding, whether judicial or quasi-judicial. However, evidence or information that is otherwise admissible or subject to discovery does not become inadmissible or protected from discovery solely by reason of its use in a mediation.
- In such an adversarial proceeding, the following persons involved or previously involved in a mediation may not be compelled to disclose confidential information obtained during the mediation:
  (a) the parties to the dispute;
  (b) the mediator or mediators;
  (c) the counsel for the parties;
  (d) the non-party participants;
  (e) any persons hired or engaged in connection with the mediation as secretary, stenographer, clerk or assistant; and
  (f) any other person who obtains or possesses confidential information by reason of their profession.
- The protections of this Act shall continue to apply even if a mediator is found to have failed to act impartially.
- A mediator may not be called to testify to provide information gathered in mediation. A mediator who is wrongfully subpoenaed shall be reimbursed the full cost of their attorney's fees and related expenses.

Administrative Actions With the IPOPHL

All administrative complaints for violation of IP rights and/or unfair competition undergo mandatory mediation, which is carried out by the Alternative Dispute Resolution Services (ADRS) under the BLA. A case filed with the BLA is submitted to the BLA-ADRS for mediation immediately after filing of the answer.

Each party must pay a non-refundable fee of PHP4,000, which entitles the parties to four sessions at a maximum of one hour per session. Additional sessions may be held subject to payment of an extension fee of PHP2,000 for each party, which entitles the parties to two one-hour sessions. These fees cover the mediator's compensation, administrative costs and other related expenses.

The failure or refusal of the party who initiated the case to participate in the mediation and/or to pay the fees shall be grounds for the dismissal of the case. However, if the respondent fails or refuses to participate and/or to pay the fees, the respondent shall be declared in default.

If parties are unable to settle their dispute within 60 days from submission of the case to mediation, the mediation shall terminate the proceedings and issue a Notice of Non-settlement of Dispute. This period may be extended for another 30 days upon joint written request of the parties. If mediation fails and/or is terminated, the BLA-ADRS will again inform the parties of their option to submit the dispute to arbitration in accordance with the existing IPOPHL arbitration rules and guidelines. Otherwise, the BLA-ADRS shall furnish the BLA with a copy of the Notice of

Non-settlement of Dispute, and the adjudication proceedings will immediately resume.

If the mediation is successful, the BLA-ADRS shall, within five days from the parties' submission of their compromise agreement, refer the agreement to the BLA, which shall, within three days from receipt of the draft decision based on the compromise agreement, approve the agreement – unless the terms or parts thereof are contrary to law, public policy, morals or good customs, in which case the agreement shall be sent back to the parties, through the ADRS, for revision or modification.

Upon the parties' revision or amendment of the agreement, it shall again be returned to the BLA. An approved compromise agreement shall have the effect of a decision or judgment on the merits, and shall be immediately executory and enforced in accordance with the pertinent rules of the IPOPHL and the Rules of Court.

Civil Actions Filed With the Special Commercial Courts

As previously described, on the day of termination of the pretrial, the court shall refer the parties for mandatory court-annexed mediation, which shall not exceed 30 calendar days and is non-extendible.

If the court-annexed mediation fails, and if the judge is convinced that settlement is possible, the case may be referred to another court for judicial dispute resolution (JDR). JDR shall be conducted within a non-extendible period of 15 calendar days.

If JDR fails, the trial before the original court shall proceed on the dates agreed upon.

All proceedings during the court-annexed mediation and the JDR shall be confidential.

Alternative Dispute Resolution Act of 2004 (RA No 9285)

An agreement to submit a dispute to mediation by an institution must include an agreement to be bound by the internal mediation and administrative policies of such institution. Further, an agreement to submit a dispute to mediation under institutional mediation rules shall be deemed to include an agreement to have such rules govern the mediation of the dispute, and for the mediator, the parties, their respective counsel and non-party participants to abide by such rules. In the case of conflict between the institutional mediation rules and the provisions of the Alternative Dispute Resolution Act, the latter shall prevail.

The parties may agree to refer one or more (or all) issues arising in a dispute or during its pendency to other forms of ADR, such as (but not limited to):

- the evaluation of a third person;
- a mini-trial;
- mediation-arbitration; or
- a combination thereof.

SOUTH KOREA

Law and Practice

Contributed by:
Dong Ju Kwon, Changkwon Kim, Sejung Lee and Yoon Sun Kim
Yoon & Yang LLC

Contents

Yoon & Yang LLC is a full-service law firm with more than 520 attorneys and other professionals based in Seoul, South Korea, and in overseas offices in Tashkent, Uzbekistan and Ho Chi Minh City and Hanoi, Vietnam. The firm's trade secrets practice team has over 25 attorneys and other professionals, including intellectual property, antitrust, criminal defence and labour attorneys, who demonstrate world-class professionalism and expertise for providing top-notch legal services based on clients' needs. The trade secrets practice team has accumulated considerable litigation expertise, with Korean companies having been increasingly initiated or 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. In particular, the intellectual property group advised in cases of trade secret infringement litigation regarding Medytox's botulinum strains.

Authors

Dong Ju Kwon is a partner of Yoon & Yang LLC and head of the intellectual property group. His main practice areas are intellectual property rights and specialised fields such as healthcare. Mr Kwon was admitted to the Bar in 1994 and handled cases for more than 20 years as a chief judge and presiding judge. With such experience, he has considerable strength in developing logical arguments and submitting relevant evidence with consideration for the perspectives of judges. His representative matters include working for clients such as SK Innovation Co, Ltd, SK Chemicals and Hanmi Pharma.

Changkwon Kim is a partner of Yoon & Yang LLC. He has considerable strength in matters related to intellectual property, product liability, bankruptcy, corporate rehabilitation and healthcare disputes. Starting his career in the public sector, he held various positions before retiring from public office as a presiding judge at the Seoul Bankruptcy Court. He has actively participated in publications related to trade secrets, intellectual property rights and copyright.

Sejung Lee is a partner of Yoon & Yang LLC. She specialises in counselling and litigation on intellectual property and antitrust matters. She has successfully represented major Korean and overseas companies in several trade secrets, trade marks, copyright and patent cases. Moreover, 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, and is widely published.

Yoon Sun Kim is a partner/senior foreign attorney at Yoon & Yang LLC. Her main practice areas are intellectual property and corporate/M&A, and she has handled various trade secrets, trade marks, copyright and other intellectual property matters for major domestic and multinational corporations. She earned her JD at University of Pennsylvania Law School, and her BA (with Distinction and Phi Beta Kappa) and MA at Stanford University. She is a member of the New York Bar.

Yoon & Yang LLC

6th, 17th, 18th, 19th, 22nd, 23rd, 27th, 34th Floors,
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

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 on 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 Co-operation Between Large Enterprises and SMEs; and
- the Act on the Investigation of Unfair International Trade Practices and Remedy Against Injury to Industry.

The UCPA does not distinguish between national and local levels for regulation.

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 acquiring it from the information owner as the information is not widely known to many unspecified persons – which would be the case if, for example, the information had been published.

Information has independent economic value if the information owner can gain a competitive advantage over 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 the 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, in 2019 the UCPA amended the "maintain secrecy by reasonable efforts" clause to "manage the information as secret", to lower the bar for the secrecy requirement for trade secrets. 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 trade secret misappropriation. The entity engaged in independent discovery or reverse engineering actually bears the burden of presenting 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 (see Supreme Court Decision No 2018Ma7100), 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 by independent development or reverse engineering;
- the time taken for the owner to acquire 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.

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.

However, in the case of controlled disclosure of a trade secret, it remains protectable as a trade secret as long it meets the requirements of a trade secret, and this has no impact on the protection period.

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 should require that the third party maintain or manage the information as a trade secret by imposing a non-disclosure or confidentiality obligation (or similar).

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 infringer's intention 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.

That said, trade secrets do not involve a registration process requiring the disclosure of information. A disadvantage of this is that, to receive protection, 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.

However, an advantage is that a wide range of information that meets the trade secret protection requirements are protectable, and smaller costs are incurred for maintaining and protecting 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) is 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 this 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 with the corporate employee's occupational breach of trust may be recognised as having committed a breach of trust. Further, the third party may be subject to tortious 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 imprisonment 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:
  - (a) acquiring or using trade secrets, or leaking them to any third party;
  - (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.
- Acquiring or using trade secrets while knowing that an act set forth in the preceding points 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, 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 a company or person), the trade secret owner can bring a civil claim in Korea based on misappropriation that happened overseas.

Moreover, if a Korean commits the crime of trade secret misappropriation overseas, they may be subject to criminal proceedings in Korea.

In addition, if a foreigner commits such a 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 secrets 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 preceding point 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; and
- 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 in which 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 in Article 2(iii) of the UCPA (see the final three points 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 this to be unreasonably long given 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 by 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 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 is advisable to develop and implement security procedures that would reduce the risk of improper disclosure of trade secrets, and to 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;
- keeping 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 to 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 a trade secret misappropriation lawsuit. When the original electronic document including trade secrets is registered, and once 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 in recognising that the relevant information has been managed as a secret when a legal dispute occurred; and
- may be used to prove prior use rights or prior invention with respect to another person's patent rights.

3.2 Exit Interviews

During exit interviews, an employer reminds departing employees of 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 such agreement could harm general consumer welfare by directly restricting the employee's freedom of job selection and restraining free competition, especially by being directly linked to the employee's livelihood. Thus, courts basically view the non-compete agreement as unacceptable.

However, a court may accept the employer's claim prohibiting an employee's transfer to another employer in the exceptional case where the content and term of the non-compete agreement is found to be 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 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 or 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 of 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, under the Civil Act, 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 occurs (Article 766).

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 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 were filed in order to infringe on the counterparty's rights or interests or to inflict harm on the counterparty without reasonable cause, and where 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 collection 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, as well as 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 only submit documents under court order in any of the following cases (Article 344):

- 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.

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 may, at a party's request, order the other party, its legal counsel or any other entity that has acquired the trade secrets due to such lawsuit to not 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 may, at the party's request, 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 this 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 that 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 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 before 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 that the court render such judgment.

5.11 Cost of Litigation

It is difficult to provide a general estimate of the costs for trade secret litigation, as such costs are dependent on various factors, including the content, type and complexity of alleged information and relevant technology, and on the complexity of the relevant case at hand.

Most 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 to dispose of 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 the suit or claim and states whether it accepts each of the claims provided in the complaint. The plaintiff may respond regarding 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 subsequent hearing for pleadings and examination of evidence.

Examination of Evidence

Under the CPA, at the hearings for the examination of evidence, a witness should attend the hearing, swear an oath and make testimonies (Article 303). Further, the court may hold an explanatory session at the hearing, which normally lasts for one to two hours, for understanding the case, including as regards alleged trade secrets and relevant technical information.

As such, the court holds several hearings where it reviews and examines information/evidence to render judgment; when it considers that it has sufficiently examined these, hearings are closed and the court schedules the date when it will announce its judgment. The first-instance proceedings usually last from around eight months to a couple of years depending on the complexity of the case (among other factors). Based on 2022 statistics, the average time for the issuance of a first-instance judgment in civil cases was 14 months.

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 where the expert witness examination is based on the witness examination procedure (Article 340).

In principle, an expert witness should provide oral testimony, and thus cannot testify by documents, unless permitted by the court. In other words, in principle, the expert witness 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 for 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 a preliminary injunction (aside from in a civil trade secret lawsuit) for

establishing a temporary position on the disputed rights in order to avoid potential material damage to the rights, to 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 that 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 is usually equivalent to between 10% and 20% of the amount or value of the subject matter in the litigation.

7.2 Measures of Damages

Under the UCPA, a misappropriator that damages the trade secret owner's business interests through wilfulness, intention or negligence is liable to compensate for such damages; if the misappropriation is found to be wilful, the court may award up to treble damages (Articles 11 and 14-2).

Actual Damages From the Misappropriation

As it is difficult for the claimant (owner) to prove a causal relationship between the misappropriation and actual damages, as well as the amount of actual damages, the UCPA provides damage calibration rules based on the following legal presumptions.

Calculation of damages

As a formula for damages, the amount of damages may be calculated by the sum of the following.

- The amount calculated by multiplying the volume of the goods transferred by the misappropriator (the "Volume Transferred") with the claimant's presumed profit per unit of the goods that the claimant could have sold had there been no misappropriation. The volume of the goods that the claimant could not have sold even in the absence of such misappropriation (the "Unsaleable Volume") should be deducted from the Volume Transferred. The Volume Transferred should not exceed any volume resulting from deducting the volume of the goods actually sold by the claimant from the volume of the goods that the claimant had the capacity to produce (the excess volume shall be referred to as "Volume Exceeding Presumed Inventory").
- The amount that the claimant could reasonably have received had there been no such misappropriation from the Volume Exceed-

ing Presumed Inventory or the Unsaleable Volume.

Misappropriator's profits gained by the misappropriation

The profits gained by the misappropriator may be presumed to be the amount of damages suffered by the claimant.

Reasonable royalty

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.

Calculation of Damages at Court's Discretion

Further, under the UCPA, 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, it 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 (Article 14-2):

- whether the misappropriator has a superior bargaining position;
- the degree of the misappropriator's wilfulness or the degree of the misappropriator's knowledge about the risk of damages;
- the scale of damages suffered by the owner owing 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.

Submission of Materials

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

Under the UCPA, the trade secret owner (claimant) is entitled to claim for injunction against or prevention of misappropriation by the entity that misappropriated or that is intending to misappropriate trade secrets, as well as for 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).

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 per-

manent 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. Under the CPA, attorneys' fees should be the costs 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 attorneys' 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 was served, and such period is invariable (Articles 390 and 396).

Although the appeal period differs by case based on the complexity of the 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 a repetition of 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 this is 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 is determined as regards 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 that the conduct at issue constitutes trade secret misappropriation, and could also submit written opinions to this effect.

10. Alternative Dispute Resolution (ADR)

10.1 Dispute Resolution Mechanisms

Alternative dispute resolution (ADR) mechanisms include settlement, mediation and arbitration procedures.

Settlement

Settlement procedures include court-led settlements and out-of-court settlements. In an out-of-court settlement, parties sign a settlement agreement to make mutual concessions and to end the dispute. The content and method of settlement agreement follows the principles of contractual freedom and is not subject to any limits. However, a 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, for settlement. Once the mediation is established and the mediation protocol is prepared, this would carry the same effect as a court-led settlement.

Arbitration

Arbitration refers to the process whereby the appointed arbitrator resolves the dispute by an arbitral award, based on the parties' agreement. 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 the 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 (Article 18):

- to maintain or restore the status quo pending determination of the dispute;
- to take action that would prevent current or imminent harm or prejudice to the arbitral proceeding, or to prohibit action that may cause such harm or prejudice;
- to provide a means of preserving assets subject to the execution of an arbitral award; or
- to preserve evidence that may be relevant and material to the dispute resolution.

SWITZERLAND

Trends and Developments

Contributed by:
Dr Oliver M Brupbacher and Dr Claudia Götz Staehelin
Bär & Karrer AG

Bär & Karrer AG is a leading Swiss law firm with more than 200 lawyers in Zurich, Geneva, Lugano, Zug, Basel and St Moritz. The firm's core business is advising clients on innovative and complex transactions, and representing them in litigation, arbitration and regulatory proceedings. Clients range from multinational corporations to private individuals in Switzerland and around the world.

Authors

Dr Oliver M Brupbacher is a dispute resolution and investigation partner at Bär & Karrer with extensive experience in the life sciences and healthcare sectors, including in complex commercial and cross-border litigation, investigations and arbitration, as well as in regulatory, corporate and compliance counselling and risk management. Oliver's practice focuses on representing national and multinational clients in heavily regulated industries and at various stages of dispute resolution and investigations, including pre-dispute advice, crisis management and information governance. As a former senior litigation counsel, global product lawyer and head of global discovery at Novartis, Oliver combines deep expertise in his areas of practice with an intimate understanding of industry and clients' needs at all organisational levels.

Dr Claudia Götz Staehelin is a dispute resolution and investigation partner at Bär & Karrer with extensive experience in the life sciences and healthcare sectors. Based on her experience as former Head of Litigation at Novartis, Claudia's practice focuses on complex investigation and litigation matters at the intersection of civil, criminal and regulatory proceedings. Claudia leads large-scale internal investigations, supports her clients in crisis management and advises them on all aspects of their compliance framework. She represents and advises clients on domestic and cross-border litigations, international judicial and administrative assistance matters, internal and regulatory investigations led by Swiss and foreign authorities, and pharma regulatory and compliance in the healthcare and life sciences industries.

Contributed by: Dr Oliver M Brupbacher and Dr Claudia Götz Staehelin, **Bär & Karrer AG**

Bär & Karrer AG

Lange Gasse 47
4052 Basel
Switzerland

Tel: +41 58 261 50 50
Email: basel@baerkarrer.ch
Web: baerkarrer.ch

The Protection of Trade Secrets in Domestic and Cross-Border Proceedings, Investigations and Employee Relationships in Switzerland

The protection of trade secrets plays an important role in the success of individual business enterprises and for a functioning economy as a whole. Swiss law recognises the importance of protecting confidential business information and provides robust legal remedies for the misappropriation of trade secrets.

In Switzerland, there is no legal act or framework that specifically governs the protection of trade secrets and the duties and liabilities of the parties involved. Pertinent provisions are found in:

- the Code of Obligations (CO);
- the Criminal Code (SCC);
- the Unfair Competition Act (UCA); and
- the Civil Procedure Code (CPC).

The SCC and the UCA stipulate certain misconduct regarding trade secrets as criminal offences and as unfair competition, respectively.

The CO protects trade secrets particularly in the context of employment relationships.

The CPC grants the owner of trade secrets access to interim measures, while providing civil courts with the authority to take appropriate measures to ensure that evidentiary proceedings do not violate the legitimate confidentiality interests of the parties or third persons.

As Switzerland is not a member of the European Union (EU), the EU Trade Secrets Directive (Directive (EU) 2016/943) neither applies directly nor has Switzerland implemented its contents into Swiss national law.

The following overview focuses on two areas of application of trade secrets protection that have become increasingly important in Switzerland in recent years. The first part highlights practical considerations and recent legal trends in connection with the protection of trade secrets in domestic and cross-border proceedings and investigations. The second part looks at the options available to companies to protect their trade secrets against unlawful disclosure and exploitation by current or former employees. Finally, an update is provided on the introduction (by 2025) in the CPC of a new in-house counsel privilege, and on its potential use for the protection of trade secrets.

Protecting Trade Secrets in Domestic and Cross-Border Proceedings and Investigations

Handling trade secret protections in court proceedings means treading a fine line between the

trade secret owner's protection against unauthorised use or misappropriation on the one hand, and safeguarding the right to a fair trial on the other. In Switzerland, as a general rule, all evidence must be disclosed to the opposing party without restriction and in the same manner as it is presented to the court. If, however, the interest of the trade secret owner so requires, civil courts must take appropriate measures to safeguard trade secrets (Article 156 CPC).

In a recent decision, the Swiss Federal Supreme Court (FSC) had the opportunity to revisit the practice of anonymising published court judgments (BGer 1C_642/2020). The case concerned a ruling of the Federal Administrative Court on the inclusion of medicinal products on the Federal Office of Public Health's specialties list. While the FSC recognised that the general interest in public justice and the individual interest in confidentiality must be weighed against each other, it held that the Federal Administrative Court's anonymisation of its judgment limits the comprehensibility of – and may restrict access to – justice. In particular, where the anonymised information was publicly available elsewhere, the FSC held that its re-publication could not represent a competitive disadvantage.

The FSC has also held that, as a procedural protective measure under Article 156 CPC – provided this proves to be the mildest means – it is also possible to order a duty of confidentiality subject to criminal sanctions, whereby such a duty can only be ordered for the duration of the proceedings (BGE 148 III 84). In addition to the evidence and the motions for evidence, procedural protective measures can only extend to information in the legal documents in exceptional cases.

In another decision, the Federal Patent Court laid out the general definition of a trade secret as knowledge that is not readily available, has a commercial value and is intended to be kept secret by its owner (O2020_014). While it is not required that the information cannot be obtained legally, it should at least require a significant effort to do so. The prevailing view is that relative obscurity of information and subjective desire for confidentiality alone are not enough to establish a secret; a legitimate interest in confidentiality is also required. Thereby, financial harm alone does not establish a worthy interest in confidentiality; the protection of confidentiality must be necessary for the proper functioning of the competition in the market. The Federal Patent Court then went on to state that whether an interest is worthy of protection ultimately depends on the result of a balance-of-interest test between individual confidentiality interests (and the constitutional right to a fair hearing) and the procedural interest in discovering the truth.

In cross-border proceedings and investigations, any disclosure of a trade secret to a foreign counterparty, court or authority may constitute a criminal offence under Article 162 and/or Article 273 SCC.

Any person who betrays a manufacturing or trade secret that they are under a statutory or contractual duty to not reveal, and any person who exploits for themselves or another such a betrayal, is criminally liable on complaint to a custodial sentence not exceeding three years or to a monetary penalty (Article 162 SCC). Thereby, it must be determined in each individual case whether a piece of information constitutes a trade secret. Generally, a fact or piece of information is qualified as a trade secret if it is neither generally known nor generally accessible. The owner of the fact or information must further have an objective, legitimate secrecy interest as well as the subjective will to maintain secrecy.

It is noteworthy that Article 162 SCC does not require any specific result of the secrecy violation, such as damages, to establish criminal liability. In recent years, there have been around six convictions under Article 162 SCC per year.

If there is a sufficient connection to Switzerland, the disclosure of a trade secret may equally constitute the criminal offence of industrial espionage (Article 273 SCC). Thereby, any person who seeks to obtain a manufacturing or trade secret in order to make it available to an external official agency, a foreign organisation, a private enterprise or the agents of any of these, or any person who makes a manufacturing or trade secret so available, shall be liable to a custodial sentence not exceeding three years or to a monetary penalty, or in serious cases to a custodial sentence of not less than one year. Notably, this provision covers violations of a trade secret in Switzerland as well as abroad (Article 4 paragraph 1 SCC; BGE 141 IV 155). In the recent past, on average there has been around one conviction under Article 273 SCC per year.

In any case, the criminal liability under Articles 162 and 273 SCC does not go further than the scope of the trade secret under civil law. Accordingly, there is no violation if:

- there is a contractual arrangement with the owner of the trade secret that permits disclosure to foreign parties;
- the owner of the trade secret has granted a waiver in the individual case; or
- the foreign parties already had prior full knowledge of the disclosed information.

There is also no criminal liability if the trade secrets are completely redacted before the disclosure of respective documents or information.

Regardless of the criminal liability, it is to be noted that the violation of a trade secret usually also constitutes a violation of the confidentiality obligations that are normally contained in commercial contracts. This may also lead to a violation of the personality and data protection rights of the owner of the trade secret.

Protecting Trade Secrets in Employee Relationships

For companies' trade secrets, employees play a major role as they often have insight into confidential information and practices of their employer. From the perspective of companies and employers, the question thus arises as to how to deal with the unlawful disclosure and exploitation of trade secrets by current or former employees.

Measures under civil law

The main possibility an employer has under civil law is to file an employment action against an employee. Under Swiss employment law, as part of their duty of loyalty and care, employees are prohibited from disclosing facts that are meant to be kept secret and that were obtained while in the employer's service, such as manufacturing and business secrets (Article 321a CO). A secret may be violated not only by communicating it to unauthorised third parties but also by exploiting it – ie, by using it for one's own advantage. To the extent necessary to safeguard the employer's interests, this protection my extend beyond the end of an employment relationship.

In the case of an existing employment relationship, the employer can terminate the employment relationship and may do so with immediate effect if a serious violation occurs (Article 337 CO). The employer may also claim damages incurred as a result of the violation of the trade secret (Article 321e paragraph 1 CO). It should

be noted, however, that such claims must be made without delay in order to minimise the risk of the court considering the damages as waived by the employer. The FSC assumes that any known, unclaimed damages at the end of an employment relationship are waived. Unknown damages can be claimed at a later point in time if and when they come to light.

In two leading decisions, the FSC decided on the disclosure of trade secrets by a current employee (BGer 6B_364/2021; BGer 6B_438/2021). In its legal assessment, the FSC held that information constitutes a trade secret if:

- it is neither generally known nor generally accessible;
- it is intended by the owner of the information to be known only to a limited group of people; and
- there is a legitimate interest in keeping it secret.

Furthermore, the FSC ruled that employees act intentionally if they are able to foresee the risk for the employer and are nevertheless willing to consciously take such risk, irrespective of whether they intended to harm their employer and whether they act in a refined, planned or calculated manner.

Measures under criminal law

In addition to triggering potential criminal liability under Article 162 and/or Article 273 SCC, the violation of a trade secret may also amount to the punishable offence of disloyal management of a business (Article 158 SCC). This provision generally provides for sanctions against any person who by law, an official order, a legal act or authorisation granted to them has been entrusted with the management of the property of another person or with the supervision of such management, and who in the course of and in breach of their duties causes or permits that other person to sustain a financial loss.

The exploitation of an entrusted work product, as well as the exploitation or disclosure of an unlawfully obtained manufacturing or trade secret, may further violate unfair competition law (Articles 5 and 6 UCA). Thereby, the term "work product" encompasses products of an intellectual and material effort and expenditure and, contrary to trade secrets, does not require a legitimate interest in maintaining secrecy. It therefore potentially has a broader scope of application than the term "trade secret".

The general time limit for filing a criminal complaint is three months, beginning on the day on which the complainant discovers the identity of the suspect (Article 31 SCC). The prosecution of a criminal complaint by the authorities requires that the complaint be well founded and that the alleged events have actually taken place with a certain degree of probability. In particular, all coercive measures, such as a house search, require sufficient suspicion of a crime and level of urgency. Any supplementary civil measures (see below) will have to be co-ordinated with the criminal measures.

Interim measures

For trade secrets, interim measures such as a court injunction may be suitable – for instance, to prevent further dissemination or even the initial disclosure of a trade secret at an early stage.

Swiss civil procedure law provides for interim measures in situations in which applicants credibly demonstrate that their rights have been violated or that a violation of their rights is anticipated, and that the violation threatens to cause not easily reparable harm to the applicant (Article

261 CPC). Applicants must also credibly demonstrate the urgency of the requested measure. In particularly urgent cases, the court may even order ex parte interim measures immediately and without hearing the opposing party (Article 265 CPC). The civil courts enjoy broad discretion as to the type of interim measure they consider appropriate in an individual case. Interim measures are also available under unfair competition law (Article 9 UCA).

New In-House Counsel Privilege

Under current Swiss law, only Swiss and EU/EFTA attorneys (but not in-house counsels) are subject to professional secrecy and therefore have a special right to refuse to co-operate in legal proceedings by invoking an attorney-client privilege. This situation has been criticised in Switzerland for years as Swiss companies may suffer procedural disadvantages in foreign court proceedings due to the lack of in-house counsel privilege. In particular, Swiss companies may be required to disclose correspondence with their Swiss in-house counsel in US proceedings, while at the same time the correspondence of US companies and their in-house counsel is protected by the US attorney-client privilege.

Against this backdrop, a parliamentary initiative was submitted in 2015 to introduce a right of non-cooperation for in-house counsels, at least in civil proceedings. On 17 March 2023, the Swiss Parliament passed a new Article 167a CPC providing for a right of non-cooperation in civil proceedings as regards activities in an in-house legal department. The new law will enter into force on 1 January 2025.

Accordingly, to the extent that trade secrets can be qualified as information that is profession-specific for attorneys, and that in particular does not relate to accessory activities of attorneys such as asset management, board of directors' activities or business consulting, there will be a right to refuse the disclosure of such information. Note, however, that the wording of Article 167a CPC limits such right to refuse disclosure to civil proceedings, and that many questions in connection with the application of the new law remain open to date.

Conclusion

Trade secret owners, such as litigants and employers, can rely on strong protections of their trade secrets under Swiss law. In practice, however, the effective protection of trade secrets is a demanding exercise that requires speed and practical expertise in navigating the complex legal landscape, and also requires strategic experience in choosing the appropriate tools to achieve the desired goal. In particular, it may be difficult in the individual instance to clearly distinguish between the trade secrets of a company on the one hand and the professional experience and knowledge of its employees on the other. Also, in order to prove that the disclosure or use of a trade secret is a criminal offence, it must be shown that an individual has acted intentionally.

Furthermore, the protection of trade secrets in domestic proceedings is within the broad discretion of the courts. This adds a degree of uncertainty to the fate of trade secrets in such proceedings. In cross-border contexts, special care must be taken to adequately protect trade secrets from prohibited disclosure to foreign counterparties, courts and authorities. Accordingly, the production of documents and information in cross-border proceedings and investigations regularly requires a careful strategic consideration of the available options, as well as tactical and operational legal advice in preparing the information for production.

UK

Law and Practice

Contributed by:
Nicola Dagg, Steven Baldwin, Gabriella Bornstein and Ashley Grant
Kirkland & Ellis International LLP

Contents

Contributed by: Nicola Dagg, Steven Baldwin, Gabriella Bornstein and Ashley Grant,
Kirkland & Ellis International LLP

Kirkland & Ellis International LLP is an international law firm with approximately 3,500 attorneys across the USA, 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 depth of Kirkland's intellectual property, commercial litigation and other practices to provide an approach tailored to 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 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' IP. The practice's success is grounded in extensive jury and bench trial experience, and a sophisticated appellate practice to protect clients' successes at the trial level.

Authors

Nicola Dagg is a partner and leader of Kirkland's IP litigation practice in London. She has over 25 years of experience at the forefront of IP litigation, particularly in relation to trade secrets and patents. Her broad 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.

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. Focusing on former employee trade secrets cases and complex cross-border life sciences and telecommunications patent disputes, Steven's trade secrets experience includes high-value disputes in the life sciences and financial industries. He is routinely instructed on "bet-the-farm" cases and has a strategic approach to litigation, 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, biological and chemical product development and screening platforms, next-generation cancer treatments and e-cigarette/vaping technologies.

Contributed by: Nicola Dagg, Steven Baldwin, Gabriella Bornstein and Ashley Grant,
Kirkland & Ellis International LLP

Gabriella Bornstein is an IP partner in Kirkland & Ellis, London. She has extensive trial and appellate experience across the IP spectrum with a focus on hi-tech, software, pharmaceutical and biotechnology patents, trade marks and copyright. She works on high value, cross-border disputes dealing with complex technical, patent and jurisdictional issues. She also has specific experience with the interplay between trade secrets and patent disputes and in assisting organisations develop their trade secrets policies from a practical and legal perspective. She has experience 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.

Ashley Grant is an associate in the Kirkland's IP litigation team in London. Ashley has broad trial and appellate experience in complex cross-border IP litigation in the technology, telecommunications (including SEP/ FRAND) and life sciences sectors. Her clients cover a broad range of industries, including telecommunications, software, medical devices, and manufacturing. Ashley also has experience in large scale commercial disputes, international arbitrations and high-profile investigations. She is dual qualified in England and Wales, and New York, giving her particular insight into cross-border litigation.

Kirkland & Ellis International LLP

30 St Mary Axe
London
EC3A 8AF
UK

Tel: +44 20 7469 2000
Fax: +44 20 7469 2001
Email: Nicola.dagg@kirkland.com
Web: www.kirkland.com

KIRKLAND & ELLIS

Contributed by: Nicola Dagg, Steven Baldwin, Gabriella Bornstein and Ashley Grant,
Kirkland & Ellis International LLP

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. This is acknowledged in, for example, Mulsanne Insurance Company Ltd v Marshmallow Financial Services Ltd and another [2022] EWHC 276 (Ch).

Following the UK's exit from the European Union and the expiry of the Brexit transition period on 31 December 2020, CJEU case law continues to apply to lower courts in the UK as a result of the application of the European Union (Withdrawal) Act 2018. However, future CJEU decisions, including in relation to the Directive, will not apply. 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, for example, 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 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

The first UK cases under the Directive/Regulation were in 2020. 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);
- 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); and
- design of the projects to be carried out under the contract and the manner of performance of the contract in the tender process (Antea Polska S.A. v Państwowe Gospodarstwo Wodne Wody Polskie (ECJ Case C-54/21)).

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 of the information to the detriment of the person communicating it. 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 Regulation 2, "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 (Regulation 3):

- 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. However, 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.

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). The facts in the Celgard case were as follows: 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" confiden-

tial 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 and/or 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). In Kieran Corrigan & Co Ltd v OneE Group Ltd [2023] EWHC 649 (Ch) at [312] the court concluded that this limitation period only applies to claims for the application of measures, procedures and remedies provided for under the Regulation. 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) and Kieran Corrigan & Co Ltd v OneE Group Ltd [2023] EWHC 649 (Ch) at [315] – [333].

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 covers the specialist civil courts of the Kings Bench Division, and all of the lists of the Chancery Division. Which specific list or Court (eg, Commercial Court or Intellectual Property List etc), 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. The statement of truth acknowledges that proceedings for contempt of court may be brought against anyone who makes, or causes to be made, a false statement in a document verified by a statement of truth. 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.

This point was re-emphasised in Mulsanne Insurance Company Ltd v Marshmallow Financial Services Ltd and another [2022] EWHC 276 (Ch) where the court noted (citing Shenzhen Senior Technology Material Co Ltd v Celgard LLC [2020 EWCA Civ 1293 at [32]) that "[i]t is well established that, in a claim for misuse of trade secrets, it is important for the claimant properly to particularise the information which is alleged to be a trade secret and to have been misused" and (citing Ocular Sciences Ltd v Aspect Vision Care Ltd [1997] RPC 289 at 359) that "[t]he courts are therefore careful to ensure that the plaintiff gives full and proper particulars of all the confidential information on which he intends to rely in the proceedings. If the plaintiff fails to do this, the court may infer that the purpose of the litigation is harassment rather than the protection of the plaintiff's rights and may strike out the action as an abuse of process."

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 ran a disclosure pilot scheme, which became permanent in October 2022. The guidelines for disclosure under the scheme are now set out at Practice Direction 57AD.

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; at the other end, 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". Parties may also apply under CPR 5.4(c)(4) for an order to keep statements of case confidential and out of the public domain.

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.

See also **7.5 Costs**.

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 applicant'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 available in an action for breach of confidence remain available to claimants where they provide wider protection to the trade secret holder than provided under the Regulation. 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 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)).

As noted above, Regulation 3 of the Regulation provides that common law remedies available in an action for breach of confidence remain available to claimants. The claimant can apply for relief both under common law remedies and the remedies under the Regulation.

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 six to 12 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 (ADR)

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 (and settlement) at the outset and generally throughout the litigation timetable. Further, the Court of Appeal recently held that courts have the power to order parties to engage in non-court based dispute resolution – eg, mediation (James Churchill v Merthyr Tydfil County Borough Council (the Council) [2023] EWCA Civ 1416).

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.

USA

Law and Practice

Contributed by:
Claudia Ray, Joseph Loy, Miriam Kontoh and Andrew (Keum Yong) Lee
Kirkland & Ellis LLP

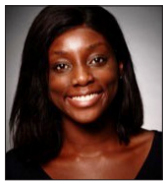
Contents

Kirkland & Ellis LLP is an international law firm with approximately 3,500 attorneys across the USA, Europe and Asia. Kirkland's trade secrets litigation practice includes approximately 85 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 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' IP. The practice's success is grounded in extensive jury and bench trial experience, and a sophisticated appellate practice to protect clients' successes at the trial level.

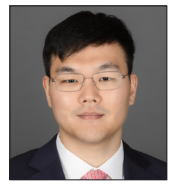
Authors

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 contract/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 Bulletins Committee 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 autonomous vehicles, biotechnology, computer hardware and software, cruise ships, digital photography, exercise equipment, mattresses, medical devices, oil drilling, petrochemicals, pharmaceuticals, robotics, smartphones and wireless communications. He is a frequent commentator on trade secret issues before intellectual property Bar associations and law school communities.



Miriam Kontoh is an associate in the New York office of Kirkland. Miriam's practice focuses on litigation and counselling in the fields of copyright, trade mark, internet/social media, right of publicity, art, trade secret and advertising law. She represents and advises clients in a range of industries, including entertainment, social media, film, and technology.



Andrew (Keum Yong) Lee is an associate in Kirkland's intellectual property practice group, whose practice focuses on patent litigation.

Kirkland & Ellis LLP

601 Lexington Avenue
New York
NY 10022
USA

Tel: +1 212 446 4800
Fax: +1 212 446 4900
Email: claudia.ray@kirkland.com
Web: www.kirkland.com

KIRKLAND & ELLIS

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 law, the Defend Trade Secrets Act (DTSA);
- individual state laws modelled after the Uniform Trade Secrets Act (UTSA); and
- common law protection in New York, which is the only state that has not yet adopted a version of the UTSA.

Prior to adopting some variation of the UTSA, most states had relied on common law trade secret protection, which was summarised in the Restatement of Torts Section 757. In 1979, the UTSA was promulgated by the Uniform Law Commission (ULC) as a model act that each state could use as a template for enacting its own trade secret legislation. In 1985, the UTSA was significantly amended to resolve issues with the 1979 version and better align it with the variations adopted by the states. In 2016, the DTSA was passed to enhance federal protection of trade secrets.

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.

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 (S.D. Ohio 2000));
- source code (Wellogix, Inc v Accenture, LLP, 716 F 3d 867, 875 (5th Cir. 2013));

- internal design and software architecture documents (TouchPoint Solutions, Inc v Eastman Kodak Co, 345 F Supp 2d 23, 28 (D. Mass. 2004)); 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 and UTSA

To prevail on a claim of trade secret misappropriation under the DTSA and state trade secret laws, a claimant must prove the following three elements:

- that the claimant owns a trade secret (see discussion below on ownership of trade secrets);
- that the trade secret was misappropriated by the defendant; and
- that the claimant was damaged by the defendant's misappropriation.

With respect to the first element, 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 v LG Electronics Inc, 343 F Supp 3d 868, 877 (N.D. Cal. 2018).

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 common law factors in determining whether a trade secret exists, despite having adopted a variation of the UTSA.

In order to prevail on a claim for trade secret misappropriation in New York, a claimant must prove that (i) they own a trade secret, and (ii) 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, 177–78 (3d Cir. 2020).

Ownership

Who can "own" a trade secret

In order to bring a trade secret action, one must be an "owner" of the trade secret. The DTSA defines a trade secret owner as "the person or entity in whom or in which rightful legal or equitable title to, or license in, the trade secret is reposed". 18 U.S.C. § 1839(4). Various states that have adopted the UTSA similarly define trade secret owners. Such a definition may enable both the creator of a trade secret and any assignees or licensees that have rightful possession of the trade secret to bring trade secret misappropriation claims. See – eg, BladeRoom Group Ltd v Facebook, Inc. 219 F. Supp. 3d 984, 990-91 (N.D. Cal. 2017).

Ownership issues may arise in the context of employer-employee relationships where a trade secret was developed by the employee. Many employment contracts provide for the assignment of such trade secrets to the employer under the "work for hire" doctrine. However, states vary in the presumption of assignability of trade secrets developed by employees, and the "work for hire doctrine" may be limited to cover only those trade secrets that were developed through work performed (i) by the employee for the employer or (ii) using the employer's information or equipment.

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, unlike patent infringement, is not a "strict liability" offence. 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, such as 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 warranted. 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. See Turret Labs USA, Inc v CargoSprint, LLC, 2022 WL 701161, at *2–3 (2d Cir. Mar. 9, 2022). 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 (S.D.N.Y. 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 United States 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.

That said, many state trade secret laws preempt common law and statutory claims to the extent they are based on the same facts and/or underlying conduct as the trade secret claims.

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 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 mis-

appropriation 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 USA 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 USA or an organisation that is organised under the laws of the USA or one of its 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 USA. Courts are just beginning to grapple with the contours of extraterritorial application of the DTSA, so the precise parameters are not entirely clear. So far they have been willing to apply the DTSA to misappropriation occurring overseas based on "acts in furtherance" that occurred in the USA, including marketing of products embodying the stolen trade secrets at trade shows within the USA and travel to the USA for the purpose of hiring a competitor's engineers. See Motorola Solutions Inc v Hytera Communications Corp, 436 F Supp 3d 1150, 1157–66 (N.D. Ill. 2020); Micron Technology Inc v United Microelectronics Corp, 2019 WL 1959487, at *3–4 (N.D. Cal. May 2, 2019).

On the other hand, loss of domestic revenues from entirely extraterritorial activity may not be alone sufficient to bring alleged misappropriation within the reach of the DTSA. See Luminati Networks Ltd v BIScience Inc, 2019 WL 2084426, at *9–10 (E.D. Tex. May 13, 2019). The ability of domestic trade secret owners to redress theft by foreign companies and those in their employ will therefore 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 (Restatement (Third) of Unfair Competition Section 42, Comment b (1995)).

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;
  (c) multi-factor authentication;
  (d) access and security audits;
  (e) penetration testing;
  (f) spam and phishing email filters; and
  (g) 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 their new position, such as any responsibilities, the name of the new employer, and the new employer's address (although the employee does not have to provide such information);
- 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 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 they only rely on such general knowledge and skill, and do 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 recognises 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 discovered or should reasonably have been discovered. The particular facts that can put a trade secret owner on notice of a trade secret mis-

appropriation 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. See Syntel Sterling Best Shores Mauritius Ltd v TriZetto Grp, Inc, 2021 WL 1553926 (S.D.N.Y. Apr. 20, 2021). 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: (i) unconsented use, (ii) acquisition, or (iii) 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 United States International Trade Commission (ITC) if products embodying a misappropriated trade secret are imported into the USA. 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 corporation 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 expressly governed by the notice pleading requirements of the Federal Rules of Civil Procedure. Under those pleading requirements, 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.

An increasing number of state and federal courts have imposed a heightened pleading standard, which requires that the plaintiff identify the asserted trade secret with reasonable particularity before proceeding to discovery. See Torsh, Inc v Audio Enhancement, Inc, 2023 WL 7688583 (E.D. La. 2023). While only California and Massachusetts impose statutory reasonable particularity requirements, the growing consensus among courts towards demanding greater detail in pre-discovery pleadings may expose a plaintiff to unique strategic challenges in terms of articulating the trade secrets that it believes have been misappropriated.

In the growing number of jurisdictions 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, 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 courts that follow the reasonable particularity standard 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 fact-dependent, and 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 the 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 (18 USC Section 1836(b)(2)). 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. Moreover, as companies embrace distributed workforces and increasingly rely on novel tools for managing and distributing information, parties seeking discovery should think creatively about information repositories where proof of misappropriation might exist. For example, discovery requests may need to go beyond traditional email and documents and consider cloud storage services, "chat" or other synchronous communication tools such as Slack, collaboration tools or "wikis" such as Confluence or Trello, issue and project tracking tools such as Jira, source code management tools such as GitHub, and virtual meeting recordings such as those generated in WebEx or Zoom.

5.8 Maintaining Secrecy While Litigating

Plaintiffs will need to strike a careful balance between under-disclosure 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 high in trade secret cases. For example, a 2021 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 USD2.75 million. For trade secret cases with over USD25 million at risk, median litigation costs rise to USD4.5 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 run 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. In certain jurisdictions, however, measures of damages such as unjust enrichment may not be triable to a jury and will instead by submitted for adjudication by the court.

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 good will, 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. Courts are increasingly moving towards requiring sufficient precision in the identification of the trade secret such that defendants receive fair and precise notice of what the injunction actually prohibits. See Carl Zeiss Meditec, Inc v Topcon Medical Sys., Inc, 2022 WL 1530491 (Fed. Cir. May 16, 2022).

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. However, some state trade secret laws do not require putting a trade secret to commercial use before royalty damages may be obtained. See AirFacts, Inc v Amezaga, 30 F.4th 359, 369 (4th Cir. 2022).

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 defendant'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 misappropriation by the defendant or a bad-faith claim of misappropriation by the plaintiff.

The Circuit Split on Damages Under a Theory of Unjust Enrichment

Currently, circuit courts are split over whether avoided costs can be awarded as unjust enrichment damages in a trade secret case where those costs bear no relationship to the plaintiff's harm or the defendant's gain. In, for example, the Third and Seventh Circuits, damages for avoided costs can be awarded under a theory for unjust enrichment. See Epic Sys. Corp. v Tata Consultancy Servs., No 22-2420 (7th Cir. 2023); PPG Indus. v Jiangsu Tie Mao Glass Co, 47 F.4th 156, 164 (3d Cir. 2022). However, other circuits, such as the Second Circuit, have explicitly rejected the idea that avoided costs can be awarded as unjust enrichment damages. See Syntel Sterling Best Shores Mauritius Ltd v The Trizetto Grp., 68 F.4th 792 (2d Cir. 2023). The Supreme Court declined a petition for a writ of certiorari for a case that would have resolved the circuit split, and thus the circuit split on this issue remains. See Tata Consultancy Servs. Ltd v Epic Sys. Corp., 144 S. Ct. 425, 217 L. Ed. 2d 237 (2023). Therefore, practitioners should consider whether avoided costs under a theory of unjust enrichment are available in their jurisdiction when filing suit.

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 US 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 thousand 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 not raised in the district court 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, espe-

cially 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 (ADR)

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.

Trends and Developments

Contributed by:
Robert Milligan and Dawn Mertineit
Seyfarth Shaw LLP

Seyfarth Shaw LLP has a trade secrets, computer fraud, and non-compete practice dedicated to safeguarding intellectual capital, trade secrets, and confidential information. With 18 offices domestically and abroad, the firm has a team of over 60 trade secret/restrictive covenant attorneys in major US cities. The experienced team emphasises proactive measures to prevent and address intellectual property theft and aggressively protect clients' legitimate business interests. Its approach includes advising on trade secret protection policies, audits of existing secrets, non-compete agreements, electronic information protection systems, and training. Seyfarth also assists clients in protecting and recovering assets, as well as defending clients from such claims. It pursues injunctions, collaborates with law enforcement, works with private investigators and other experts, and represents clients at trial and arbitration. Recent success stories include injunction victories in high-stakes technology matters, obtaining large jury trial verdicts, and complete defence decisions in respect of company trials and arbitrations.

Authors

Robert Milligan has practiced commercial litigation and employment law, specialising in business disputes, trade secret misappropriation, restrictive covenants, and intellectual property theft for over 20 years. He is the co-chair of Seyfarth's national trade secrets, computer fraud, and non-competes practice, and holds leadership roles in several legal organisations focusing on intellectual property protection. Robert serves as an editor/author of several prominent trade secret treatises and is editor-in-chief of the Trading Secrets blog. His practice encompasses domestic and international litigation and transactional work involving trade secrets and restrictive covenants, including trade secret audits, and his extensive experience and results in trials, arbitrations, and appellate proceedings solidify his reputation as a leading authority.

Dawn Mertineit has been a litigator for over 15 years and specialises in complex commercial litigation, with a notable focus on non-compete and trade secrets litigation, where she adeptly guides clients through intricate legal landscapes. Dawn's cross-state knowledge is crucial as restrictive covenant laws evolve, and as an editor of Seyfarth's award-winning Trading Secrets blog, she remains a thought leader, offering insights into legislative changes affecting businesses. Her practical advice and creative solutions, often quoted in legal publications, showcase her impactful approach. Dawn has litigated and arbitrated disputes throughout the United States, both prosecuting and defending trade secrets and restrictive covenant disputes.

Seyfarth Shaw LLP

South Wacker Drive
Suite 8000
Chicago
IL 60606-6448
USA

Tel: +1 312 460 5000
Fax: +1 312 460 7000
Web: www.seyfarth.com

In 2023, restrictive covenants were subject to more scrutiny than ever, with multiple governmental agencies and state legislatures setting their sights on the enforceability of such contracts. Indeed, the Federal Trade Commission (FTC) just announced a rule banning most non-competes (although as discussed below, it remains to be seen whether the ban will go into effect). We anticipate additional scrutiny and legislation in 2024, requiring employers to stay apprised of the latest developments – particularly as more states impose stiff financial penalties for failure to comply with the applicable laws. As a result, trade secrets have become even more important than ever, as companies may only be left with trade secret protections, if their restrictive covenants are no longer applicable. In addition, the lasting impact of remote and hybrid work and the increasing ease of data transfer has made it even more critical for employers to stay abreast of state-specific requirements and ensure effective protection of company trade secrets, particularly when onboarding and off-boarding employees. In light of this challenging framework, employers should be more motivated than ever going into 2024 to identify and protect their valuable trade secrets and conduct trade secret audits to shore up their protections.

Federal Attempts to Curb Non-Competes

2023 saw several attempts by federal agencies to crack down on non-compete agreements (and potentially other restrictive covenants). Most notably, in January 2023, the FTC issued a proposed rule seeking to ban virtually all non-competes. On 23 April 2024, the FTC announced its final rule after having received over 26,000 comments on the proposed rule. The final rule prohibits non-competes for all workers, both new and pre-existing, with limited exceptions (namely, existing agreements for senior executives in policy-making positions earning more than USD151,164 annually are still permitted, as are non-competes entered into in a bona fide sale of a business). It also requires employers to provide individualised notice to workers subject to a prohibited non-compete that the non-compete cannot be enforced. The rule has already been challenged in multiple lawsuits based on the question of the FTC's authority to legislate on this topic, with an eventual showdown at the Supreme Court likely. More information on the rule is available here and here.

Additionally, the General Counsel of the National Labor Relations Board (NLRB) issued a memorandum in May 2023 advising that non-com-

petes in employment agreements and severance agreements violate the National Labor Relations Act (NLRA) except in rare circumstances. Specifically, the memorandum claims that such covenants interfere with workers' rights under the NLRA, which protects employees' rights to self-organise, join labour organisations, bargain collectively, and "engage in other concerted activities for collective bargaining or other mutual aid or protection". The exceptions to this blanket rule (as outlined in the memorandum) are, like the FTC's rule, extremely limited – namely, the memorandum only notes restrictions on an individual's "managerial or ownership interests" in a competing business, and "true independent-contractor relationships", as being reasonable (although it concedes that there may be other circumstances in which a narrowly tailored covenant is "justified by special circumstances", but notably declines to give examples of such circumstances). The memorandum's stated reasoning for this position is dubious at best, and its impact is unclear; it is not binding or precedential. However, it certainly signals a priority from yet another federal agency to target the use of what the government sees as overly broad covenants and the NLRB has already filed a consolidated complaint alleging that certain restrictive covenants contained in offer letters and policies in an employee handbook violated the NLRA.

In sum, federal agencies are seeking to undertake enforcement responsibilities aimed at curtailing the use of non-compete agreements that are perceived to limit workforce mobility and wage enhancement.

State Initiatives

Unsurprisingly, state legislatures have also continued to crack down on restrictive covenants, maintaining a trend that we have seen over the past several years.

Most notably, California (already the vanguard of state legislation prohibiting restrictive covenants except in exceedingly rare cases) recently passed two laws that tighten the screws for employers even more, starting on 1 January 2024. First, in September 2023, Governor Newsom signed a law that provides that any contract that is void under California law (eg, non-compete) is unenforceable regardless of where and when the employee signed the contract. Accordingly, employers can anticipate more disputes with former employees who flee to California at the behest of their new employer to avoid enforcement of their covenants by former employers. Under the new California law, an employee, former employee, or prospective employee may bring a private action to enforce the law for injunctive relief or the recovery of actual damages, or both, and they are entitled to attorneys' fees and costs if successful. Expect more "races to the courthouse" as former employers try to secure a more favourable venue to enforce non-competes and similar agreements. We also anticipate potential constitutional challenges to this new law.

Next, Governor Newsom also signed a law that required employers, by 14 February 2024, to notify in writing current employees, and former employees who were employed after 1 January 2022, whose contracts include a non-compete clause or who were required to enter a non-compete agreement that does not satisfy an exception to California law, that the non-compete clause or agreement is void. The law makes a violation of these provisions an act of unfair competition pursuant to California's unfair competition law. Needless to say, employers will need to consult with their counsel to carefully consider the best approach to avoid liability.

Minnesota also joined the list of states banning non-competes in 2023, with the sole exceptions being non-competes entered in connection with the sale of a business, or in anticipation of dissolution of a business. The new law also prohibits out-of-state choice of law and forum provisions in employment agreements containing non-compete provisions, a trend that we expect to continue in other states in 2024 and beyond.

New York's legislature tried to follow suit, passing a wholesale non-compete ban that was ambiguous as to its scope (for example, it was not clear whether it applied to non-solicits or even to "sale of a business" agreements). However, Governor Hochul opted not to sign, while indicating support for a pared-down version that would potentially include wage thresholds. We expect that a bill will be passed in 2024 that limits the availability of employers to use such covenants.

Wisconsin and Maine's legislatures have also proposed non-compete bans (Wisconsin's proposed ban failed to advance, and Maine's proposed ban was ultimately vetoed by the governor). Employers can expect more legislation in 2024 in a variety of jurisdictions, underscoring the need to remain up to speed with the latest changes in this area of the law. Several states have implemented wage thresholds for the use of restrictive covenants, which increase at regular intervals. Employers need to be aware of such thresholds, which continue to rise. At least one class action was filed in 2023 based on an employer's alleged improper use of non-competes for employees who did not earn the statutory minimum in Washington.

Finally, state legislatures and federal agencies are not the only places where non-competes are being scrutinised. In Nevada, the Supreme Court recently held that Nevada courts are not required to blue pencil overly broad non-competes, despite a statute that seemingly mandates it, and only requires them to do so "when possible". In Delaware, long a preferred venue of employers and businesses, the courts are taking a dim view of overly expansive non-competes – even in the context of a sale of a business. Many of these cases even struck down the contractual choice-of-law provision designating Delaware law as controlling. And even when applying Delaware law (which permits a court to reform an overly broad covenant), several decisions refused to enforce agreements deemed overly expansive at all. We predict that courts out of Delaware – and elsewhere in the country – will continue to clamp down on agreements that arguably go beyond protecting an employer's legitimate business interests. Finally, we have seen increased scrutiny of allegedly overbroad confidentiality provisions by courts, underscoring the need to narrowly tailor such clauses, which often are overlooked and misunderstood as being automatically enforceable; several court decisions have revealed that this is not the case.

In light of the ever-changing landscape of restrictive covenant enforcement, employers (particularly those with employees in different states) will need to carefully craft their restrictive covenant agreements to be mindful of what might be deemed an overbroad scope, as well as fee-shifting provisions (and other financial and potential criminal penalties) and choice-of-law/forum selection requirements. The use of boilerplate and one-size-fits-all agreements will not cut it in this highly regulated environment.

Identifying and Protecting Trade Secrets Remains Paramount

Although companies employ restrictive covenants and conventional intellectual property safeguards such as patents, trade marks, and copyrights to protect specific assets, there

remains a wealth of crucial company information that could be classified as trade secrets. The heightened governmental and media focus on trade secret theft by competitors and overseas entities underscores the substantial risks associated with breaches and emphasises the necessity of safeguarding trade secrets. Moreover, remote and hybrid work has made it even more challenging to ensure the effective protection of company trade secrets. The surge in trade secret theft, amplified by the rise of remote work, technological advancements, and intense global competition, imposes significant financial burdens on American companies, totalling hundreds of billions of dollars annually. Even the most prominent and sophisticated companies fall prey to these breaches. Especially given the increased hostility to restrictive covenants noted above, companies need to take robust measures to protect their trade secrets, from understanding and identifying what constitutes a trade secret (and how, specifically, it provides value to the business by its secrecy) to deploying tools and strategies to protect them, including pursuing litigation and injunctions to protect such assets.

Indeed, eye-popping damages awards in cases involving misappropriation of trade secrets highlight the pivotal role these assets play within an industry and their critical importance to companies; several decisions in the last few years have resulted in awards of tens of millions (or even hundreds of millions) for plaintiffs who have proven their misappropriation claims. Moreover, emerging court opinions acknowledge the broader spectrum of costs incurred by businesses in cases involving the theft of trade secrets, encompassing the benefits gained by an unlawful actor in reducing development expenses and expediting market entry by illicitly acquiring and deploying trade secrets.

However, gargantuan damages awards are not a given; key decisions this past year have highlighted the need for trade secrets plaintiffs to establish damages with concrete proof and without resorting to speculative theories. For example, a Second Circuit case found unjust enrichment damages inappropriate where the party alleging trade secret misappropriation had been made whole through other compensatory damages, especially where the trade secret had increased in value. This decision, however, sets up a circuit split that (at least as of now) the Supreme Court does not seem keen to weigh in on.

In another case, a jury verdict of over USD100 million was invalidated via a motion for judgment as a matter of law, in which the trial court rejected challenges to the jury's liability findings, but determined that the plaintiff had failed to establish any damages based on misappropriation, leaving the plaintiff with a pyrrhic victory. In yet another case, an appeal to the Seventh Circuit resulted in an order mandating the trial court to reduce punitive damages (although the reduced amount was still in the hundreds of millions). Other key decisions revealed courts' willingness to second guess jury verdicts, carefully scrutinising damages calculations and in some cases finding them unreasonably speculative. Additionally, a ruling from the Seventh Circuit is expected this year on an appeal from a trial court's order disgorging all of the defendant's worldwide profits from sales of products using misappropriated information; the appellate court will determine whether the disgorgement of profits should be limited to profits from US-based sales under the DTSA.

Other recent decisions have revealed certain pitfalls that may be easy for litigants to fall into in trade secret misappropriation. For example,

multiple cases have stressed the need for plaintiffs to prove that their stated trade secret derives its value from its secrecy. In other words, it is insufficient to merely show that information is valuable; it must be valuable due to its secrecy. Other cases have stressed the need to carefully describe alleged trade secrets, as well as reasonable measures taken to maintain the secrecy of such information. We anticipate even more increased scrutiny of a trade secret holder's reasonable secrecy measures in an environment in which more and more businesses are collaborating and, necessarily, sharing information.

While these decisions provide appropriate caution for those seeking to prove misappropriation, several cases suggested a bright side for would-be plaintiffs. For example, at least one court confirmed that misappropriation claims can be brought "on information and belief", noting that concrete information supporting such a claim is often solely in the hands of the defendant (although of course litigants should be mindful of their obligation to assert such allegations in good faith). Additionally, the Fourth Circuit affirmed the imposition of a preliminary injunction that was challenged by the defendant, who argued that a provision of the DTSA covering extraterritorial conduct if an "act in furtherance" occurred in the US was inapplicable; the appellate court, however, determined that the "act in furtherance" requirement is a "relatively low bar", and that the defendant's access to information through servers located in the US and likely use or disclosure of the same within the US was sufficient. Separately, the First Circuit confirmed that compilations of publicly available information can meet the definition of a trade secret.

In other developments this past year, President Biden signed into law the Protecting American Intellectual Property Act, which requires that the president submit periodic reports to Congress identifying foreign actors who have engaged in significant trade secret theft against individuals or entities in the US. The law also permits the president to impose sanctions on such malicious actors. As of the beginning of 2024, no reports had been issued (although the first report was due on 4 July 2023), and it remains to be seen if any reports in the future will spur retaliatory accusations from foreign administrations.

As a result of all the foregoing, increasingly commonplace considerations for sophisticated businesses and their legal representatives include the identification of unlawfully acquired or utilised trade secrets, the expenses associated with their development, and the competitive advantages obtained by the wrongdoer. Particularly given the evolving landscape regarding non-compete agreements and similar restrictive covenants, this trend is expected to lead to a greater reliance on safeguarding trade secrets and pursuing claims of misappropriation through litigation. Consequently, companies must establish robust trade secret protection strategies to navigate these developments effectively. Proving that the property sought to be protected derives its value from its secrecy will continue to be critical, as will drafting confidentiality agreements that are robust enough to adequately protect trade secrets and demonstrate a business's reasonable measures to maintain their secrecy, while not being so broad as to be struck down, and effective onboarding and offboarding policies/strategies for employees from/to competitors will be increasingly significant. In sum, trade secrets will be increasingly important to companies for their competitive advantage as state legislatures and federal and state agencies crack down on restrictive covenants in 2024.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Katie.Burrington@chambers.com