弁護士法人 中央総合法律事務所
CHUO SOGO LAW OFFICE, P. C.

Protection of Trade Secrets in Japan

March 9, 2023
Sumire Eto, Attorney
E-mail: eto_s@clo.gr.jp

I. To Begin With

What examples of "company property" would you give if a friend or a colleague asked you to do so?

Typically, the term "company property" brings to mind assets such as real property (like a building or plants owned by a company), movables (like machinery, materials and products) and human capital (such as employees' skills and experience). Indeed, these are important parts of properties a company owns. But there is another type of asset that should not be overlooked: "information." Information relating to a company's business operations or technologies plays a significant role in making company competitive in the marketplace and differentiating it from other companies. This "information" normally refers to confidential information, and typically contains the company's most valuable asset – trade secrets.

Some reported cases making headlines recently, involving unauthorized leakage of confidential information, demonstrate how valuable trade secrets can be. For example, it has been reported that an ex-employee of Softbank unlawfully took the company's trade secrets concerning high-speed telecommunications technology (5G) and gave them to his new employer Rakuten Mobile, and was consequently sentenced to two years of imprisonment with a four-year suspended sentence plus a fine of one million yen for misappropriating trade secrets in violation of the Unfair Competition Prevention Act ("**UCPA**"). Reportedly, Softbank has filed a lawsuit against both this person and Rakuten Mobile seeking damages of one billion yen, alleging that the company suffered damages of a hundred billion yen.

In another case, a former president of a company operating a well-known sushi restaurant franchise Kappa Sushi, as well as the company itself and some other related entities, are now being charged with unlawfully obtaining trade secrets of another sushi franchise Hama Sushi in violation of the UCPA (or, with "infringing trade secrets," as described below). During the trial, the former president admitted his guilt, while the company and other related entities have recently claimed total innocence of the charges levied against them, demonstrating that they are set on putting a full-scale fight.

In light of the foregoing, it is particularly important for companies to understand how to protect their trade secrets, especially by using the available legal tools and mechanisms. To facilitate such understanding, this article comments on the definition of trade secrets under the applicable law and several types of measures that may be available in cases of unauthorized leakage of trade secrets, based on the *Guidelines on Management of Trade Secrets* (last revised on January 30, 2003) issued by the Ministry of Economy, Trade and Industry (METI).[1]

II. Trade Secrets Subject to UCPA

The UCPA defines "trade secrets" as "technical or business information useful for commercial activities such as manufacturing or marketing methods that is kept secret and that is not publicly known." (UCPA, Article 2(6)) Accordingly, to qualify as a "trade secret," the information must (A) be kept as confidential ("**Requirement A**"), (B) be useful ("**Requirement B**"), and (C) not be publicly known ("**Requirement C**").

Once information qualifies as a "trade secret," various legal proceedings, both civil (most typically a court injunction pursuant to the provisions of the UCPA) and criminal, become available in connection with such information, provided that, in order to bring such legal proceedings, not only the above-mentioned three requirements but also some additional requirements specified in the UCPA in respect of each action, for example, requirements pertaining to "unfair competition" and/or "Crimes of Infringement of Trade Secrets," must be met.

The UCPA does not protect information that does not rise to the level of trade secrets. Nevertheless, it may still be possible to seek remedial measures with respect to such information, including an injunction, by contractually stipulating in a private agreement how such information should be handled. It is generally considered that it is possible to pursue the legal actions referred to above regardless of whether or not the information in question falls within the category of trade secrets under the UCPA.

III. Regarding Requirement A

1. Purpose

The reason why company's information must be "kept as confidential" in order to receive legal protection as trade secrets under the UCPA is to ensure that such information can clearly be recognized as trade secrets by employees (or, in some cases, business partners) of the company who might otherwise want to obtain, use or disclose it (collectively, "**Employees**"). Without

[1] https://www.meti.go.jp/policy/economy/chizai/chiteki/guideline/h31ts.pdf

such a requirement, and with the intangible nature of information that allows for various ways of possession and control, and also trade secrets' confidential nature that, unlike patent or other similar rights, prevents them from being known to public, it might not always be clear to Employees whether such information is legally protected as a trade secret. By specifying Requirement A, the UCPA prevents Employees from accidentally being suspected of any wrongdoing or facing unexpected consequences as a result of handling potentially-confidential information. In other words, the UCPA intends to ensure that Employees can foresee such consequences, and that, ultimately, business activities involving trade secrets can be conducted in a consistent and reliable manner.

2. Required Degree of Protective Measures

(1) General

To fulfill Requirement A, a company's intention to manage certain information as confidential ("**Intention to Safeguard**") must clearly be indicated to its employees in a commercially reasonable way under given circumstances ("**Protective Measures**"). It is also required that the Protective Measures render such Intention to Safeguard easily recognizable by the employees ("**Noticeability**"). This applies almost equally to cases where a company indicates its Intention to Safeguard to its business partners.

Protective Measures consist of two major parts: (a) a reasonable separation of the information concerned (trade secrets) from other general information (non-trade secrets); and (b) clarification of the nature of the information concerned as a trade secret.

(2) Subjects

Protective Measures are intended to apply to Employees who are authorized to access the information that constitutes trade secrets (the "**Information**"). Such Employees (**"Subject Employees"**) include not only employees who are specifically authorized to access the Information as part of their duties (which should be typical in most cases), but also employees who are allowed to handle the Information not as part of their regular duties (e.g., employees whose duty is to deliver information between departments, or employees who are not members of the relevant department but working in a so-called "open plan office" and are authorized to open unlocked common-use bookshelves placed in the office).

(3) Details of Protective Measures

(a) Reasonable Separation

The "reasonable separation" requirement of Protective Measures refers to keeping trade

secrets reasonably separate from other general information in order to give clear notice to Subject Employees of the company's Intention to Safeguard in accordance with, for example, the nature of such secrets, the media being utilized, the degree of confidentiality or the amount of information.

It is generally accepted that such separation may be considered "reasonable" as long as the company's employees can recognize whether the medium in question contains information to be treated as trade secrets or whether it is comprised solely of general information, by considering how such medium is usually being controlled in that specific company, which may vary depending on, for example, the company's size and the type of its business.

(b) Clarification of the Nature of Information as Trade Secrets

The major forms that the above-mentioned "clarification of the nature of the information concerned as a trade secret" may take include selection of and/or placing notice on the media used, limiting personnel who have access to the media, listing the types and/or categories of the Information and specifying confidentiality obligations in writing (e.g., in non-disclosure agreements or written pledges). The basic point is that such clarification should be taken in the manner and to the degree that makes the Subject Employees aware of that the information in question is confidential and therefore should not be treated in the same way as general information.

The specific manner and degree of Protective Measures naturally vary depending on the number of employees who are authorized to access trade secrets, the individual employees' duties, how the business is operated, the specific nature of the Information, the conditions of the office room and other surrounding circumstances. For example, if only a small number of employees are legally and practically allowed to access certain trade secrets, although depending on circumstances, even an exchange of a simple, oral confirmation (for example, that "this information is confidential") among those employees could be considered as adequate measures to be taken.

(4) Practical Examples of Protective Measures

Below are some practical examples of Protective Measures categorized in accordance with various media in which the Information is contained.[2]

(a) In Case of Paper Media

- ✓ Reasonably separate the Information from general information (e.g., by filing), and indicate the confidential nature of the document (e.g., by indicating "CONFIDENTIAL"), whenever possible.
- ✓ As a possible alternative to marking each individual document or file as confidential, store the intended documents in secure storage (e.g., a lockable cabinet or a safe).

(b) In Case of Electronic Media

- ✓ Label storage media as confidential, name computer files or folders with the indication of "confidential," and/or add the indication of "confidential" to the electronic data contained in the electronic files that should be handled as trade secrets, so that such indication appears on the screen when they are opened.
- ✓ If it is not possible to mark storage media themselves as confidential, put a label of "confidential" on cases or boxes in which such storage media are stored.

(c) In Case of Trade Secrets Embodied in Tangible Assets (e.g., manufacturing machinery or molds, high-performance microorganisms and prototypes of new products)

- ✓ Display a notice stating "PERSONNEL CONCERNED ONLY" on the door.
- ✓ Limit visitors' access to the plant by, for example, posting security guards and/or installing a gate that requires ID cards to go through.
- ✓ Display a notice stating "NO PHOTOS."
- ✓ Compile a list that specifies all assets to be treated as trade secrets, and have it scanned and shared internally among employees who are likely to handle such assets.

(d) In Case of Intangible Trade Secrets

Intangible trade secrets, such as know-how concerning skills or design or customer information that are acquired or memorized by employees during the course of their duties,

[2] In cases where multiple types of media are used to control the same trade secret (e.g., when the same information is managed by using both paper and electronic media), it is generally considered that Protective Measures should be implemented in relation to each medium. If, however, there is a possibility that Employees might access more than one media that contain the same Information, safeguarding such Information will normally be considered to be adequate as long as the Employee can recognize the Intention to Safeguard with respect to such Information through Protective Measures implemented in respect of any of such media.

should be reduced to writing whenever possible, for example, by listing the trade secrets with applicable categories.[3]

(5) What to Consider When Sharing Trade Secrets Inside/ Outside Company

Following is a summary of adequate Protective Measures that could be taken when a company shares trade secrets internally (e.g., among its branches and/or offices) or externally (e.g., with its subsidiaries, affiliates, business partners, service providers and/or franchisees).

(a) Internal Sharing Involving Multiple Divisions

According to the prevailing approach, adequacy of Protective Measures should not be assessed on the entire company basis. Rather, the relevant inquiry should be whether the Noticeability of the company's Intention to Safeguard is ensured in respect of each individual section of the company which is deemed to be a unit and which handles trade secrets with a certain degree of independence (a "**Unit of Control**"), typical examples of which is a branch and business division. Whether company sections are adequately independent to make up a Unit of Control is to be determined by considering whether they have autonomous authority to make decisions concerning (i) whether and how Protective Measures should be taken, and (ii) the supervision of the status of compliance (including matters concerning disciplinary actions to be taken in cases of non-compliance), as well as the surrounding circumstances, such as their respective scale, physical environment and business operations.

Consequently, as a basic rule, one branch's adequacy/ inadequacy of Protective Measures does not affect that of other branches, as long as those other branches duly maintain Protective Measures of their own. That said, in a hypothetical scenario of an exceptional case, for example, where Branch A's long-lasting, unconcealed failure to take Protective Measures has made it completely normal for other employees of the company to handle a certain category of information as non-trade secrets, and, as a result of such a lack of Noticeability, a leakage of information involving an employee of Branch B takes place, one branch's (in this case, Branch B's) implementation of Protective Measures could still be affected by other branches, and consequently be considered to have been inadequate.

(b) External Sharing Involving Multiple Companies

The above-described basic rule also applies to cases where information is shared externally among multiple entities. This means that, in such cases, (a) adequacy of

[3] Such reduction to writing is especially important so as not to hinder or discourage employees from changing employment due to the uncertainty of what information they are allowed or not allowed to take with them when moving to other employers.

Protective Measures should be determined on an individual entity (i.e., a Unit of Control) level and (b) the adequacy/ inadequacy of Protective Measures of one company does not affect that of other companies that share the same information.

A potential question that could arise in cases of external sharing is whether the company disclosing its trade secrets (the "**Disclosing Company**") may seek an injunction to restrain unauthorized use of its trade secrets against the entity with whom the Disclosing Company shared the information (the "**Receiving Company**"), for example, its subsidiary. In such a case, in order for the Disclosing Company to seek an injunction against the Receiving Company, the Disclosing Company must show that it has communicated its Intention to Safeguard to the Receiving Party (or, more specifically, the Receiving Party's employee(s) who has/have actually received the trade secrets in question) in the same manner as the Disclosing Company does it to its own employees. While, on the one hand, the effective way to communicate such Intention to Safeguard to the Receiving Company is likely to depend on particular circumstances, on the other hand, in most cases, a sure-fire way of achieving such communication could be by entering into a non-disclosure agreement that specifies information to be treated as trade secrets. In cases where entering into such agreement is not practically feasible due to, for example, lack of sufficient leverage vis-a-vis the intended business partner, possible alternatives to communicate the Disclosing Company's Intention to Safeguard might be to orally state that the information in question is handled as trade secrets in the Disclosing Company, or to mark the documents to be disclosed as confidential.

IV. Regarding Requirement B

1. Purpose

The primary purpose of Requirement B (requiring trade secrets to be "useful") is to protect only information that, in a broad sense, has commercial value by excluding information lacking legitimate interest to be legally protected, such as information that is against public policy (e.g., information associated with tax evasion or dumping of hazardous substances, which is considered to have an anti-social nature) from the scope of trade secrets. Therefore, normally, information that meets Requirements A and C also fulfills Requirement B.

2. Practical Examples

As the above-described purpose suggests, it is not essential for the information to be actually used or utilized in specific business activities to meet Requirement B. In other words, in addition to information that is directly being used in business, any information that has indirect or potential value in connection with business operations, including so-called "negative

information," such as data of failed studies (if such data can be utilized to save research and development costs in the future) and information associated with defective products (which may be useful for a company that plans to develop an AI-based software to detect defective products), might also be considered as "useful" in terms of Requirement B. Furthermore, it is widely accepted that usefulness of trade secrets in terms of Requirement B does not cease to exist even in cases where such secrets can be effortlessly replicated (i.e., by piecing it together from publicly-known information) by entities operating in the same industry.

V. Regarding Requirement C

1. Outline

Information that fulfills Requirement C (requiring trade secrets not to be publicly known) is information that is not known or readily available to the public. It is considered that, if certain information is only available under the control of its owner (e.g., when such information is not published through journals that are reasonably available, or when it is not easy to analyze and/or infer such information from publicly available information or products that are generally available), such information should fulfill Requirement C.

If most trade secrets are a combination of various pieces of knowledge, then it may be possible to replicate some trade secrets by stitching together fragments of such knowledge published separately in various publications. However, the quality of being replicable is not necessarily conclusive evidence that such potentially-replicable information is in fact "publicly known" in terms of Requirement C. This is because, as described above, the major test behind Requirement C is to ascertain whether or not the information in question is generally available outside the control of its owner. Consequently, even when certain information is potentially replicable by collecting available fragments of certain knowledge, whether it fulfills Requirement C or not will be determined by considering its general availability, based on the surrounding circumstances, such as the ease and the cost of combining available fragments of the relevant knowledge, including time and funds required to obtain the component fragments of information.

2. Precedents

In one judicial ruling made in a case in which some information resembling the plaintiff company's specific technical trade secrets was obtained through reverse engineering,[4] the court concluded that the company's technical trade secrets continued to fulfill Requirement C

[4] Referring to a method of research of how a given product is manufactured and/or how it operates, as well as its specifications, design or source codes, by studying the structure of that product by, for example, disassembling machines incorporating the product, observing the operation of the product or analyzing the operation of software.

considering that the reverse engineering in question required a long-term, costly analysis by experts (Osaka Dist. Ct., Feb. 27, 2003, 54 *Intellectual Property Management*, no.1, page 69).

In contrast, in another case in which some research was conducted to discover the types and composition (including ratio) of an alloy used for a product that was available in the market, the court concluded that such types and composition did not qualify as information that fulfilled Requirement C, after finding that the method used in the research was a generally-available technique that could be utilized at a reasonable cost (Osaka Dist. Ct., Jul. 21, 2016, *Intellectual Property Law and Policy Journal* no. 52, page 279).

VI. Measures Against Unauthorized Leakage

1. Overview

Unauthorized divulging of trade secrets can be redressed through either civil or criminal proceedings.

2. Civil Proceedings

The remedies available under civil proceedings against leakage of trade secrets ("**Leakage**") include:

(1) Injunctions (UCPA, Article 3)

If a company's trade secrets have been leaked, in order to prevent leaked trade secrets from being used, or, if already being used, to prohibit any further use thereof at the earliest possible time after becoming aware of the leakage, such company may seek a court injunction predicated upon encroachment or threatened encroachment upon its business interests caused or likely to be caused by the leakage or other unlawful acts committed in connection with trade secrets. The injunction may be in the form of either (a) an injunction to suspend the ongoing encroachment against the person(s) who is/are encroaching upon its business interest, or (b) an injunction to prevent the threatened encroachment from being acted upon against the person(s) who is/are likely to encroach upon its business interest, together with a court order to, for example, have the leaked trade secrets destroyed or discarded, if necessary.

In addition, if the situation is so imminent that, for example, a company's business interests have already been harmed by any act that falls under the category of "unfair competition" defined in the UCPA, and it is likely that the company will further sustain substantial harm unless such harmful act is immediately discontinued, the company may also seek a provisional disposition (*kari shobun*) to enjoin the act.

(2) Claim for Damages (UCPA, Articles 4 and 5)

If a company has suffered loss or damage as a result of an infringement of its rights in trade secrets, such company may, through civil proceedings, seek damages it has incurred against the person(s) who leaked the trade secrets and/or any entity that unlawfully acquired the leaked trade secrets.

Unlike tort claim proceedings pursuant to the provisions of the Civil Code, which require the claimant to establish the amount of incurred loss or damage, proceedings to seek damages under the UCPA can be pursued without having to establish the amount of loss or damage caused by the Leakage, because, in applicable cases, damages under the UCPA are presumed to have been incurred. In this way, the claimant's burden of proving lost profits, which is often not easy to meet, is lessened under the UCPA. As a result, the UCPA is making it easier for companies to seek damages, compared to claims for damages pursuant to the Civil Code.

(3) Restoration of Business Reputation (UCPA, Article 14)

In addition to the above-described two types of remedies, if a company's business reputation is harmed as a result of the Leakage, the company may seek a court order to have the person or entity that leaked the trade secrets take necessary measures to restore the company's reputation by, for example, publishing a formal apology.

3. Criminal Charges (UCPA, Articles from 21(1)(i) to (ix))

(1) Nine Types of Criminal Offences

The UCPA specifies nine types of acts as Crimes of Infringement of Trade Secrets (collectively, the "**CITS**"), making them subject to criminal sanctions. To protect trade secrets, the UCPA specifies potential offenders to include not only those who obtained them directly, or used or disclosed trade secrets by unlawful means, but also those who have obtained them knowingly, and then used or disclosed such unlawfully-obtained trade secrets.

The nine CITS are as follows:

(i) Unlawful Acquisition (UCPA, Article 21(1)(i))

The act of acquiring trade secrets by deceiving, assaulting or intimidating a person ("**Offensive Means**"), or by stealing property, breaking into a facility, gaining unauthorized access to or in any other way interfering with a person's control over such person's trade secrets ("**Violation of Control**") for the purpose of obtaining unjust benefit

or inflicting harm on a person who owns the trade secrets ("**Unjust Purposes**").

(ii) Unauthorized Use or Disclosure after Unlawful Acquisition (UCPA, Article 21(1)(ii))

The act of using or disclosing trade secrets acquired through Offensive Means or Violation of Control for Unjust Purposes.

(iii) Misappropriation (UCPA, Article 21(1)(iii))

Misappropriation of trade secrets for Unjust Purposes by a person to whom the owner of trade secrets has disclosed them if such misappropriation was carried out by means of any of the following acts in violation of such person's duty with respect to the management or custody of such trade secrets:

- ✓ Misappropriation of a document, drawing, or a recording medium containing or storing trade secrets ("**Recording Media**") or any object that embodies trade secrets;
- ✓ Reproducing information contained or stored in Recording Media, or any object that embodies trade secrets; or
- ✓ Failure to delete information contained or stored in Recording Media that should have been deleted, and disguising such failure by pretending to have deleted such information.

(iv) Unauthorized Use or Disclosure after Misappropriation (UCPA, Article 21(1)(iv))

Using or disclosing trade secrets for Unjust Purposes in violation of the duty to manage or keep custody of such trade secrets, by a person who acquired such trade secrets by way of misappropriation listed above in item (iii).

(v) Unauthorized Use or Disclosure by Employees (UCPA, Article 21(1)(v))

Using or disclosing trade secrets by an incumbent officer or employee (but excluding persons to whom the offence under item (iv) above is applicable) to whom such trade secrets have been disclosed by their owner (collectively, "**Personnel Concerned**"), if such disclosure or use was carried out for Unjust Purposes and in violation of such officer's or employee's duties pertaining to the management or custody of those trade secrets.

(vi) Unauthorized Use or Disclosure by Former Employees (UCPA, Article 21(1)(vi))

Using or disclosing trade secrets by a former member of Personnel Concerned for Unjust Purposes after the termination of such member's employment if such member makes, during the time of employment and for Unjust Purposes, any offer to disclose the trade

secrets to any person, or receives from any person a request to disclose the trade secrets or to make them available to such person, in violation of the duties of Personnel Concerned pertaining to the management or custody of those trade secrets.

(vii) Unauthorized Use or Disclosure by Secondary Recipients (UCPA, Article 21(1)(vii))
Using or disclosing trade secrets for Unjust Purposes by a person who has acquired such trade secrets by way of unauthorized disclosure under any of item (ii), (iv), (v) or (vi) above.

(viii) Unauthorized Use or Disclosure by Tertiary Recipients (UCPA, Article 21(1)(viii))
Using or disclosing trade secrets for Unjust Purposes by a person who has acquired such trade secrets knowingly through unauthorized disclosure under item (ii), (iv), (v), (vi) or (vii) above.

(ix) Transfer of Goods Infringing on Trade Secrets (UCPA, Article 21(1)(ix))
(a) Knowingly assigning or delivering any goods for Unjust Purposes, or (b) knowingly exhibiting, exporting, importing or through telecommunications lines or networks distributing such goods for the purpose of assigning or delivering such goods for Unjust Purposes, by any person who has obtained such goods in the knowledge that they were produced by way of using technical secrets and such use of secrets constitutes any of the offences enumerated under item (ii), (iv), (v), (vi) (vii) or (viii) above.

(2) Penalties

The offences stipulated in the UCPA, including the CITS, may be punishable, for example, by imprisonment for not more than five years and/or a fine of not more than 5 million yen (UCPA, Article 21(2)), or imprisonment for not more than ten years and/or a fine of not more than 30 million yen (UCPA, Article 21(3)), as the case may be. Furthermore, under the UCPA, if the offences are committed in connection with the perpetrator's business entity, the business entity may be subject to a fine of not more than 500 million yen (or, in the event of crimes stipulated in Article 21(3), not more than 1 billion yen).

VII. In Closing

Readers who wish to learn more about the recommended measures for the prevention of a Leakage may want to refer to the *Handbook for Protection of Confidential Information – Improving Corporate Value (May 2022)*[5] published by the IP Policy Office, METI, which addresses those

[5] https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/1706blueppt.pdf

measures in a more detailed and comprehensive manner.