The Leakage of Trade Secrets (Customer Data) by the Employees of Contractors

The *Benesse Corporation Customer Data Leakage* Case (Criminal Case)

Tokyo High Court (Mar. 21, 2017) 1180 *Rodo Hanrei* 123

Hirokuni Ikezoe

Facts

This was a criminal case in which the defendant was an employee of a subcontractor, Company K, the end company in a chain of contractors engaged to develop an information system for a project that had been outsourced to Company B by Company A (Benesse Corporation), which were both non-parties to the litigation. The defendant violated the Unfair Competition Prevention Act (UCPA) by downloading around 30 million pieces of customer information—namely, the trade secrets (*eigyō himitsu*) of Company A—and disclosing and selling around 10 million of those pieces to a list broker for the purpose of wrongful gain. The key points at issue were as follows: (i) *himitsu kanri sei*—whether the customer information in question was managed properly as secret, and (ii) whether the defendant was under *eigyō himitsu hoji gimu*—the obligation to maintain confidentiality of the trade secrets.

In the first instance (Tokyo District Court Tachikawa Branch [Mar. 29, 2016] 1180 *Rohan* 133), the court recognized the claims that said customer information was managed as secret and that the defendant was obliged to maintain the confidentiality of the trade secrets, and the defendant was sentenced to three and a half years' penal servitude and a fine of three million yen (approximately US$27,500). Here we will look at the High Court case that was brought by the defendant to appeal said judgment.

Judgment

The High Court reversed the judgment of the District Court and issued its own judgment. The defendant was sentenced to two and a half years' penal servitude and a fine of three million yen (namely, the High Court set a one-year shorter jail term than that set by the District Court).[1]

(1) Customer information and whether it is properly managed as secret

According to the essence of the requirements of UCPA Article 2, Paragraph 6[2] that requires proper management as secret, trade secrets to be protected must be distinct from other information. Without a clear distinction between them, it will be difficult for the people who come into contact with business owners' information to judge whether they are permitted to use said information, thereby potentially hindering the effective use of information. In order for such information to be classed as managed secret, it is not sufficient for the owner to have a subjective will to keep the information secret. It is important that it is sufficiently possible for the people who access said information to recognize that the information is a secret. The owner therefore needs to be taking the reasonable efforts to manage said information, such as placing restrictions upon who can access said information.

In the first instance, the judgment appears to have set the following factors for the information in question to be managed as secret: (i) that it is possible for people who access the information in question to objectively recognize that the information should be kept secret, and (ii) that the reasonable efforts required to protect the secrecy of said information are being taken, such as limiting who has access to the information or other such methods.

However, according to the essence of the UCPA, it is primarily the first of these two points—namely, (i) that the people who access the information objectively recognize it as secret—that is important, and, while the (ii) is a key for determining whether the information is "managed as secret," it is not acceptable to isolate it from (i). In this case, even though the restrictions on access to customer information and other such measures were unsatisfactory, such that the highly-advanced information management measures expected of a major company had not been established or implemented, the requirements for the information to be classed as managed secret were fulfilled on the whole, provided that the people who accessed said information were able to recognize it as a secret.

Company B, the contractor to which the work was directly entrusted, provides information security training for all employees each year. All employees are also required to confirm that they have attended the training by submitting a form, in which it is specified that it is prohibited to wrongfully disclose personal or classified information. They were also expected to submit a consent form in which they commit to maintain the secrecy of personal and secret information. Moreover, it could also be said that, based on the content and purpose of the system, the information within it, and others, it was easy to recognize that the relevant customer information, which was accumulated in the aforementioned database, was important for the sales and marketing strategies utilized in the business activities of Company A, the company that initially ordered the work, and that said information must remain classified. In this case, the requirements for the information to be classed as managed secret had been fulfilled.

(2) The obligation to maintain confidentiality of trade secrets

The defendant had submitted a written pledge to his employer, Company K, in which he pledged not to take classified information out of the company without the company's permission. He was also under the obligation to maintain the confidentiality of the classified information he acquired in the course of his work as prescribed for all employees under the work rules of Company K. Moreover, the outsourcing agreements exchanged between each company also included clauses regarding the confidentiality of classified information. It can therefore be suggested that the classified information that the defendant was handling as part of his work for the primary contractor Company B was also covered under the confidentiality obligations that he held to Company K. However, this does not mean that the defendant was therefore automatically a party to the contract such that he was under obligation to Company B to maintain the confidentiality of the relevant customer information.

At the same time, it must also be noted that in this case the chain of outsourcing consisted of four stages—that is, work was outsourced from Company A to Company B, from Company B to Company O, from Company O to Company Q, and from Company Q to Company K. The outsourcing agreements between Company B and Company O, Company O and Company Q, and Company Q and Company K each fall under what is known as "disguised contracting" (*gisō ukeoi*, where an employer directly supervises and instructs a worker as they would a dispatched worker, while treating them as a subcontractor, in order to avoid administrative responsibility for them). As the defendant was working under direction and orders from Company B, he is recognized as a dispatched worker under Article 2, Item 2, of the Worker Dispatching Act (WDA).[3] Under the application by analogy of Article 40-6, Paragraph 1, Item 1 of the WDA[4] (this clause was not yet in effect when this incident occurred, but its essence can be considered valid even at that time) a direct employment contract is considered to have been formed between the defendant and Company B, and it can be understood that, according to Article 24-4 of the WDA,[5] the defendant was under the obligation not to disclose to other people any classified information handled over the course of his work.

This therefore meant that as the defendant had submitted to Company B a consent form pledging not to wrongfully disclose to persons outside of the company any classified information acquired in his

work for Company B, the consent form is a valid confidentiality agreement with Company B and the defendant was under an obligation to Company B to protect the classified information acquired in the course of his work. Given that the customer information in this case was classed as classified information under Company B's internal regulations, and that people who came into contact with it were easily able to recognize it as classified information, the defendant is deemed to have had an obligation to Company B to maintain the confidentiality of the relevant customer information.

Commentary

(1) Significance and features of the judgment

This is a precedent of a criminal case that garnered public attention because the leakage involved such a massive data of trade secrets in the form of customer information. In this case, the penal provisions under the UCPA (the cumulative imposition of penal servitude and a fine) were also approved by the High Court, and it can be considered a significant precedent for similar cases (this is thought to be the first case in which the High Court recognized the application of criminal penalties under the UCPA). Moreover, it is surely socially significant as it may serve as a deterrent against similar behavior.

The High Court judgment is also distinctive in the way in which it adopted a slightly different approach to determining whether the information was managed as a secret—which is one of the UCPA's requirements prescribed as trade secret[6]—to that which is typically used in judgments.

From the perspective of labor law, this judgment is also significant in the way in which an interpretation and application of the WDA was adopted to present a legal construction to ensure that workers not under direct employment fulfil their contractual obligation to maintain trade secrets.

(2) The requirements for "trade secret": whether it is managed as secret to be confidential

According to the judgment, the important factor in determining whether the information is being managed as secret, is not only the subjective will of the trade secret owner to keep them secret, but also the possibility for the people who come into contact with the trade secrets to objectively recognize them as such. In addition, the high court regards the imposition of access restrictions and other such reasonable efforts for implementing the safeguards as not a requirement, but one of factors in determining whether information can be objectively recognized as secret.

In the conventional scholarly and administrative interpretations, it is understood that for information to be managed as trade secret, it needs to fulfil the two requirements—"the information in question is objectively recognized as being trade secret" and "steps are being taken to restrict access to it."[7] In this case, some part of the judgment in the first instance could have shared this interpretation. However, the high court judgment clearly rejects this understanding. That is the distinctive feature of this judgment.

Moreover, among the precedents up until now,[8] there have been cases in which the protection of trade secrets was denied due to the strict requirements applied in determining whether the information was being treated as secret. Such strict interpretation of managed secret was thought necessary to prevent disputes regarding trade secrets and to clarify the scope of criminal liability responding to the amendments to the UCPA.[9]

However, it has been questioned whether a strict requirements for being managed as secret is in accordance with the purpose of the UCPA, and such requirement could result in excessive burdens, particularly for small and medium-sized companies in practice.[10] There were therefore calls to include the relative standard of whether the people contacting with the trade secrets are able to objectively recognize it as such. Analysis also suggests that, as if in response to this opinion, courts have tended toward a lenient (flexible) judgment of whether information is being managed as secret around the last 12 years.[11] This judgment also appears to have entailed a more flexible framework for determining information being managed as secret. More specifically, in this

judgment, this can be seen from the way in which it explores whether the reasonable efforts were adopted to manage trade secret (the fact that it does not demand advanced and rigid management methods) and, while there are typically two factors—namely, that access to the information was restricted and that the information could be objectively recognized as information to be kept—it currently, emphasizes the latter and makes a judgment of the circumstances "as a whole." This judgment can be seen to have adopted the same mode of thinking as that of judicial precedents and theories in recent years. The current official interpretation is considered to tend toward that of the case described above and other such judicial precedents and theories of scholars.[12]

And yet, it remains controversial whether the kind of approach adopted in this ruling is suitable for the practical application of the law. Indeed, as stated in the judgment, restricting access to information is not so much a factor that can be treated independently, as it is one important factor for determining whether information is managed secret. However, it is not unquestionable that the issue may in practicality be difficult to determine whether information is managed "on the whole," as it was in this judgment. Trade secrets are extremely important information that forms the core of business administration. Therefore, while the possibility for the person who came into contact with the trade secrets to objectively recognize it as such is important in legally determining whether information is being managed as secret, efforts need to be made to understand how the extent to which the information is "on the whole" being managed as secret that depending on the characteristics and the scale (of the eventual disclosure or leak) of said secret information, and the business owner's financial power to whom the trade secrets belong, while also taking note of further judicial precedents in the future.

(3) The legal construction regarding the obligation to protect trade secrets

Under the provisions set out by labor laws, it is understood that the obligation to protect trade secrets is imposed on workers in accordance with the good faith and fair dealing principles that are incidental to the existing contractual relationship.[13] Previous labor lawsuits regarding violation of the obligation to maintain the confidentiality of trade secrets have focused on the company taking measures against the worker, such as requests for the payment of damages, injunctions, disciplinary action, dismissal, or restriction on the payment of retirement allowances.[14] On the other hand, the UCPA notes trade secrets as one of the interests protected by law, and prescribes remedies[15] for victims of infringements upon the confidentiality of their trade secrets and penal provisions[16] to be imposed upon the perpetrator. In violation of trade secrets under the UCPA, the civil remedies do not—unlike the typical concept adopted in labor law—focus on the obligation to maintain confidentiality as set out in the contractual relationship.[17] However, in criminal cases such as this one, in prescribing the penal provisions—the point which caused an issue here—it is necessary for the perpetrator to have been found to have "breached their duties of management."[18] These "duties of management" are interpreted as "the duties to protect confidentiality typically imposed in a contract, and the duties to protect confidentiality individually imposed through confidentiality agreements and other such contracts."[19] Thus, his duty to protect the confidentiality of trade secrets is itself not a concept that originated in the UCPA, but one that has its roots in the contractual relationship. Therefore, in criminal cases such as this, it is necessary to recognize and construct a contractual relationship between the defendant and Company B, which was contracted to conduct the work for Company A, under which the defendant is subject to the obligation to protect trade secrets.

According to the court's fact finding in this case, the multi-layered outsourcing over a chain of companies, and each outsourcing relationship should be deemed a worker dispatching relationship, as these were cases of disguised contracting. Therefore, by applying the provisions of the WDA, it is possible to construct a direct contractual relationship between Company B, the company to which A had initially outsourced the work, and the defendant, an

employee of the end subcontractor in the chain of the contractors to which the work was outsourced. Such a logical construction seems to be the unique feature of this case.

Work that entails handling trade secrets in the form of electronic information is, as in this case, often conducted as part of multi-layered outsourcing among the information and communications industry, rather than within a direct employment relationship. With this in mind, even in labor relations-focused civil cases that address dispatched labor (disguised contracting) and outsourcing relationships, it is possible that the kind of logical construction adopted in this judgment may be applied in order to recognize that the worker who ultimately engages in the work is under the obligation to maintain confidentiality. In this sense, this case alerts us to the existence of issues that stretch beyond the realms of conventional labor law and to the importance of collaboration and cooperation between the labor laws intended to respond to such circumstances and the related study of the law. In a broader perspective, focusing on the judgment in this case, we could learn measures need to be taken against the wrongful disclosure of companies' important trade secrets.[20]

1. The High Court reduced the sentence on the grounds (i) that in the outsourcing relationship referred to in this case confidential information was being managed extremely inappropriately, as indicated by the fact that the subcontractor's employees—namely, people whose backgrounds, etc. are unknown—were permitted access to said customer information (that is, important trade secrets that form a fundamental component of the business) and (ii) that it was partially due to the approach of Company B, the company to which the project was initially outsourced, that the database's alert system was not functioning at all, in turn allowing the defendant's behavior to go unchecked for around one year and the damage to grow.

2. UCPA, Article 2, Paragraph 6: "The term 'Trade Secret' as used in this Act means technical or business information useful for business activities, such as manufacturing or marketing methods, that are kept secret and that are not publicly known."

3. WDA, Article 2, Item 2: " 'Dispatched Worker' means a worker, employed by an employer, who becomes the object of Worker Dispatching."

4. WDA, Article 40-6, Paragraph 1, Item 1: "In the event that the person(s) receiving the provision of Worker Dispatching services undertake one of acts described in the following items, the person(s) receiving said provision of Worker Dispatching services are at that time deemed to have made the Dispatched Worker who engages in the dispatched work the offer of a labor contract with the same labor conditions as the labor conditions pertaining to said Dispatched Worker at that time, with the proviso that this does not apply when the person(s) receiving the provision of Worker Dispatching services are unaware, without negligence, that their behavior falls under any of the acts listed in the following items.

Items 2-4 (omitted)

Item 5: When a person receives the provision of Worker Dispatching services under the title of contracting or other such title other than worker dispatching and without prescribing the provisions set out in the items of Article 26, Paragraph 1 (Author's note: Provisions related to the content of the worker dispatching contract), with the intention of avoiding the application of this act or the provisions of the act applied under the provisions of the following clause."

5. WDA, Article 24-4: "A dispatching business operator, as well as his/her agent, employee or other worker, shall not disclose to another person a secret learned with regard to a matter he/she handled in the course of business, unless there are justifiable grounds. The same shall apply to any person who ceased to be a dispatching business operator or his/her agent, employee or other worker."

6. In addition to the requirement for information to be managed as secret (*himitsu kanri-sei*), the requirements that are to be fulfilled for information to be "trade secrets" are that the information is useful (*yūyō-sei*) and is not publicly known (*hikōchi-sei*). UCPA, *supra* note 2.

7. Yoshiyuki Tamura, "Eigyō himitsu no fusei kōi riyō wo meguru saibanrei no dōkō to hōteki na kadai" [Trends in court decisions and legal issues surrounding improper use of trade secrets], *Patent* 66, no.6 (April 2013): 82; Kazuko Takizawa, "Himitsu kanri sei to eigyo himitsu kanri" [Confidentiality requirements for a trade secret and its management], *Waseda Bulletin of International Management* no.46 (2015): 53.

8. For more on the analysis of judicial precedents, see Emi Tsubata, "Eigyō himitsu ni okeru himitsu kanrisei yōken" [Reasonable efforts to maintain secrecy in Trade Secret Law], *Intellectual property law and policy journal* 14 (2007): 191; Takeshi Kondo, "Himitsu kanrisei yōken ni kansuru saiban rei kenkyu" [Swinging back of court decisions about trade secrets], *Intellectual property law and policy journal* 25 (2009): 159; Wataru Sueyoshi, "Eigyo Himitsu" [Trade Secrets in Japan], *The University of Tokyo Law Review* 9 (Oct. 2014): 157.

9. Kondo, *supra* note 8, 201.

10. Tsubata, *supra* note 8, 213; Kondo, *supra* note 8, 201.

11. Takizawa, *supra* note 7, 53; Sueyoshi, *supra* note 8, 165.

12. "Eigyō himitsu kanri shishin" [Guidelines on the management of trade secrets], Ministry of Economy, Trade and Industry, last modified January 23, 2019, https://www.meti.go.jp/policy/economy/chizai/chiteki/guideline/h31ts.pdf.

13. Takashi Araki, *Rodo ho* [Labor and employment law] 3rd ed. (Tokyo: Yuhikaku, 2016), 279.

14. Araki, *supra* note 13.

15. UCPA Article 3, Paragraph 1 (Right to Claim for an Injunction): "A person whose business interests have been infringed on or are likely to be infringed on due to Unfair Competition may make a claim to suspend or prevent that infringement, against the person that infringed or is likely to

infringe on the business interests."

UCPA Article 4 (Damages): "A person who intentionally or negligently infringes on the business interests of another person through Unfair Competition is held liable to compensate damages resulting therefrom"

16. The penal provisions that were an issue in this case are those set out in Article 21, Paragraph 1, Items 3 and 4.

Article 21, Paragraph 1, main clause: "A person who falls under any of the following items will be punished by imprisonment with required labor for not more than ten years, a fine of not more than twenty million yen, or both."

Item 3: "[A] person to whom the Owner of Trade Secrets has disclosed a Trade Secret, and who, for the purpose of wrongful gain or causing damage to the Owner, obtains a Trade Secret by any of the following means (Author's note: omitted), in breach of the legal duties regarding the management of the Trade Secret"

Item 4: "[A] person to whom the Owner of Trade Secrets has disclosed the Trade Secret and who, for the purpose of wrongful gain or causing damage to the Owner, uses or discloses Trade Secrets obtained through the means set forth in the preceding item (Author's note: omitted), in breach of the legal duty regarding the management of the Trade Secret"

17. Protection, remedy, and sanctions regarding trade secrets that do not fall under the classification of trade secrets under the UCPA are therefore dealt with as a contractual issue. Moreover, as long as the information is classed as a trade secret under the UCPA, even after the worker has left their employment, he or she is prohibited from using or disclosing the trade secrets without forming a special contract with their employer for the purpose of wrongful gain, etc.

18. *See supra* note 16.

19. Hirokazu Aoyama, *Fusei kyoso boshi ho* [Unfair Competition Prevention Law] 5th ed. (Tokyo: Hougakushoin, 2008), 231.

20. This judgment is also covered in a commentary by Keiichiro Hamaguchi in "Gisō ukeoi deatta SE no kokyaku jōhō rōei to fusei kyōsō bōshi hō ihan no umu" [The leakage of customer information by a system engineer hired under a disguised contracting arrangement and whether it constituted a violation of the UCPA] *Jurist*, no. 1528 (2019):119. Hamaguchi explores the judgment from a different perspective from the author.

The *Benesse Corporation Customer Data Leakage* Case (Tokyo High Court, Mar. 21, 2017), 70-1 *judgments* 10. http://www.courts.go.jp/app/files/hanrei_jp/028/087028_hanrei.pdf. See also 1180 *Rodo Hanrei* pp. 123–147.

AUTHOR

Hirokuni Ikezoe Senior Researcher specialized in Labor and Employment Law, The Japan Institute for Labour Policy and Training (JILPT). Research interests: Working time, Work-life balance / conflict, Diversification of labor market, Legal concept of employee, and Labor / employment dispute resolution. Profile: https://www.jil.go.jp/english/profile/ikezoe.html