WHITE PAPER:
WEBINAR SERIES

Trade Secrets
Protecting Trade Secrets In Taiwan
2019

LIN & PARTNERS
TAIPEI, TAIWAN
WWW.LINANDPARTNERS.COM.TW

Lin & Partners
Offices: Taipei, Taiwan
Tel: +886 2 2771 5929 Fax: +886 2 2731 2896
Email: attorneys@linandpartners.com.tw

Dr. George Lin
Managing Partner
attorneys@linandpartners.com.

AMER ASIA LAW
BEIJING AMERASIA CHINA IT CONSULTING CO. LTD.

Protecting Trade Secrets In Taiwan

by Dr. George Lin, Managing Partner - Lin & Partners

LIN & PARTNERS
恆業法律事務所

Companies in Taiwan - one of the world's most important locations for the design and manufacture of computers, mobile devices, semiconductors, and other technological products - including both local companies and multinational companies operating in Taiwan, are often victims of trade secret theft by departing employees and/or competitors. This has led to the development of sophisticated domestic laws and judicial precedents which enable owners of trade secrets to enhance the protection of their proprietary properties. Typically, victims of trade secret theft will seek redress in the civil courts while simultaneously providing evidence to the public prosecutor to investigate potential criminal offences.

1. Relevant Legislation

1.1 Legislation Concerning Trade Secret In Civil Actions

Taiwan's Trade Secrets Act ("**TSA**"), as last amended on 30 January 2013, is the primary law establishing the general rules relating to trade secrets protection. Generally, certain information becomes a trade secret if (i) it is not generally known to the public, (ii) has economic value due to its secretive nature, and (iii) the owner has taken reasonable measures to maintain its secrecy. However, Taiwan's Civil Code and Fair Trade Act ("**FTA**") also provide for other civil measures and remedies in relation to the violation of trade secrets.

Given the wide array of measures and remedies provided by these laws, victims of trade secret theft must pursue diversified civil litigation strategies. For example, to force the offender to remove stolen trade secrets from their computer systems and prevent the use of such information, the TSA allows victims to seek court orders for the removal and destruction of the materials and files, while the Civil Code offers injunctive relief against the theft. If a former employee has joined another entity that makes use of the stolen trade secret, the FTA allows the victim to demand that the entity cease the use of the stolen trade secret and remove it from its systems.

In addition, the FTA provides ground for victims to seek remedies via Taiwan's Fair Trade Commission ("**FTC**") against a competitor that makes use of stolen trade secrets. A petition may be filed with the FTC to order the competitor to cease the use of such stolen trade secrets, impose administrative fines between NT$50,000 and NT$25 million (approximately US$1,600 to US$820,000 respectively), and impose additional fines between NT$100,000 and NT$50 million (approximately US$3,300 to US$1,640,000 respectively) until the competitor complies with the FTC order. However, the claim under FTC's administrative process relating to trade secret theft is relatively untested, as the court system tends to offer speedier remedies.

Regarding damages, under the TSA the individual offender who steals the information is liable for actual damages and lost profits. Where it can be proved that the offender's actions are intentional, treble damages are possible. The FTA provides for damages to be paid for by the entity that employs the individual who has stolen the trade secrets, and the Civil Code's provisions against unjust enrichment are also applicable to judicial remedies.

1.2 Legislation concerning trade secrets in criminal enforcement actions

The TSA provides for criminal penalties against both individuals and competitor's entity that use the stolen trade secrets. The individual who engages in the unauthorized reproduction and usage of the trade secrets can be sentenced to up to five years imprisonment and a fine between NT$1 million and NT$10 million (approximately US$33,000 to US$330,000 respectively). An individual who steals trade secrets in Taiwan, with the intent to use the information in a foreign jurisdiction (namely, China, Hong Kong and Macau) can be sentenced to imprisonment between 1 and 10 years and a fine between NT$3 million and NT$50 million (approximately US$98,000 to US$1,640,000 respectively); and, if the proceeds from the criminal activity exceed the range of the statutory fines, a fine of two to ten times of the proceeds may be imposed. If the individual uses or discloses the trade secrets while in the employ of a competitor, such competitor – whether a natural person or corporation – may be subject to monetary fine as well. However, the competitor may reduce or eliminate its liability if it can demonstrate that it has implemented measures for the prevention of the use of such trade secrets.

The FTA provides for criminal penalties of up to two years imprisonment and a maximum fine of NT$50 million (approximately US$1,640,000).

The Criminal Code imposes a penalty of up to one year imprisonment and minimal fines for the taking (such as downloading) of commercial and industrial secrets without authorization and disclosing the same to a competitor, though the definition of "secret" in the Criminal Code may be construed more narrowly than in the provisions of the TSA, making the TSA a more effective tool for pressing criminal charges. The Criminal Code also penalizes the individual or third person (such as a competitor) that obtains an "illegal benefit" with up to five years imprisonment and a fine of up to NT$500,000 (approximately US$16,400).

1.3 Other legislation concerning trade secrets

Taiwan's Personal Information Protection Act ("**PIPA**") is the law governing personal data protection, and applies to any collection, processing and use of personal identifiable information ("**PII**") that occurs within the jurisdiction of Taiwan, regardless of whether the owners of the PII ("**Data Owner**") are local or foreign entities. PIPA applies both to local and foreign individuals whose data is collected, processed or used ("**Data Subject**"). Theft or misuse of the PII of a Data Subject is subject to civil and criminal penalties. Thus, theft of client lists or client contacts should be investigated as potential PIPA violations.

1.4 Proper plaintiff to initiate civil or criminal actions

In either a civil or criminal case, the plaintiff may be an individual or corporate entity. Individuals without a domicile or corporations without a fixed place of business in Taiwan must first satisfy relevant procedural steps in order to initiate the actions, such as payment of court fees and placing a security deposit with the court. If they engage a local legal advisor in Taiwan, they would issue a power of attorney that authorizes the legal advisor to represent them in Taiwan.

2. Jurisdiction

2.1 Judicial venues for enforcement actions involving trade secret violation

Taiwan has an Intellectual Property Court that handles both civil and criminal cases involving intellectual property, including trade secrets. Although a relatively new institution, the Intellectual Property Court judges have developed a reputation for efficiency and professional knowledge.

The common venue for civil and criminal cases is the appropriate district court in Taiwan where the theft has taken place. Under Taiwan's 3-tier court system, appeals would be filed with the High Court and subsequently the Supreme Court (equivalent to the court of final appeal). Actions seeking FTC's intervention would be filed directly with the FTC.

2.2 Practical limitations when pursuing enforcement actions in Taiwan

There are two important limitations to consider when filing a trade secret protection and enforcement action in Taiwan, one of which is the lack of mandatory discovery procedures and the other is the absence of jury trials. The latter is founded in the fundamental difference between common law and civil law systems, and the former relates to the availability and gathering of evidence. In civil cases, most evidence is in the hands of the perpetrator. In the event that the perpetrator intentionally withholds evidence, the plaintiff will have the burden to gather the evidence on his/her/its own account under Taiwan's Civil Procedure Code. However, such limitation will not be a barrier in criminal cases, because the prosecutor can directly search the perpetrator and seize all relevant evidence with a search and seizure warrant.

3. Issues concerning employment in relation to trade secrets

3.1 Enforcement issues concerning non-competition clause

Generally, the court, when reviewing a non-competition clause, mainly focuses on whether the clause is legally valid and binding, i.e., whether the period and location limited by the non-competition clause is reasonable. As such, cases concerning the enforcement of non-competition clause tend to be in favor of the employers. However, the courts also exercise discretion on the default payment in the event of breach of non-competition clause, which commonly reduces the amount of damages.

3.2 Considerations when enforcing non-competition clause against junior employees

In the rapidly developing industry of mobile applications, junior employees tend to switch employers more frequently, leading to increasing trade secrets theft incidents.

In our experience, provisional injunctions enforcing non-competition clause against junior employees can be challenging. Judges often set a higher burden of proving material harm or imminent danger to the employer because a junior employee's switching to the employ of a competitor is a factor that is considered in conjunction with the junior employee's right to employment.

4. Other Industries

4.1 Financial Industry

Taiwan has a highly competitive financial industry in which employees often change employers, thus increasing the inherent risk of trade secrets theft. As Taiwan's financial industry is highly regulated and closely monitored by government agencies, the employees have the obligation to maintain the confidentiality of customer data. Therefore, in addition to the other legal remedies in relation to trade secrets as presented above, theft of client data by employees in Taiwan's financial industry may also constitute violations of the applicable financial regulations. As such, the standard of proof for actions against employees in Taiwan's financial industry may be lower than that in the other industries.

In addition, professionals in Taiwan's financial industry who are required to be licensed by the competent authority or trade associations for provision of services may face disciplinary action (e.g., suspension or revocation of license) if trade secret theft is proven. Therefore, compared to those in the other industries, professionals in Taiwan's financial industry are less inclined to be involved in commercial espionage.

5. Cases outside of the jurisdiction of Taiwan

5.1 Enforceability of foreign judgments in Taiwan

A final, binding foreign judgment or arbitral award is often enforceable in Taiwan subject to a multiple tests that include, among others, principle of reciprocity and non-contradiction to public policy or public morals in Taiwan.

Strategically, a plaintiff may institute concurrent legal proceedings in both Taiwan and the foreign jurisdiction for trade secret violation if personal jurisdiction requirements are met for civil and/or criminal actions. In that way, plaintiff may enforce the judgment in either jurisdiction as additional security.

5.2 Remedies available against former employees currently employed outside of Taiwan

There were several high profile trade secret protection cases in the high-tech sector in Taiwan, most of which involved former employees taking trade secrets and subsequently joining a competitor overseas, e.g., China and South Korea. In such cases, the owner company of the stolen trade secrets can initiate criminal prosecution procedures under the TSA and, subject to available extradition treaties, seek extradition of the perpetrator back to Taiwan. Moreover, in order to further protect its business interests, the victim company may concurrently files a prohibitive injunction with the U.S. International Trade Commission (ITC) against the competitor company to prohibit the import of its services or goods into the United States which contain the stolen trade secrets.

6. Best Practices

6.1 Recommended implementation measures to satisfy TSA requirements

In order for the relevant data to constitute protected trade secret under the TSA, the TSA sets out 3 requirements: (i) it is not generally known to public, (ii) it has economic value due to its secretive nature, and (iii) its owner has taken reasonable measures to maintain its secrecy.

The reasonable measure requirement is often one of the key elements that determine whether the data becomes a trade secret under the TSA. In practice, there are some best practices that companies may follow to satisfy the reasonableness test:

(i) First and foremost, the company should establish internal regulations and policies relating to the definition and classification of trade secrets, in order to establish a uniform understanding within the company as to what constitutes a trade secret and the level of access, depending on the work scope, to the trade secrets.

(ii) Subsequently, the company must establish a protective / restrictive access system to internal channels or areas which may hold trade secrets, such as access limitations to certain network drives, password protection to certain folders or documents and restrictions on access to areas which stores trade secret in physical form.

(iii) The company must also implement periodic hardware and software upgrades to ensure computer and network security.

(iv) The company should set up surveillance and access control systems in areas where trade secrets are stored or operated.

6.2 Recommended key documents and work rules to satisfy TSA requirements

(i) Require employees to sign non-disclosure agreements upon commencement and termination of employment, and when the employees need to know trade secrets due to their scope of work or duties;

(ii) Include in the employment contract the non-competition provisions specific to the employee's role and level of seniority;

(iii) Ensure, through codes of conduct and/or company policies, that all employees within the company in both Taiwan and overseas offices are aware of and acknowledge their obligations in relation to trade secrets;

(iv) Provide mandatory, periodic training on trade secret protection policies and internal materials that emphasize on the importance and value of the company's trade secrets.

7. Recent case in Taiwan and its impact: TSMC v. Liang Mong-song

7.1 Court decision

In a judgment rendered on August 24, 2015, Taiwan's Supreme Court (the final appellate court) issued a ruling in the case of Taiwan Semiconductor Manufacturing Co., Ltd. v. Liang Mong-song.

The defendant, Liang, was a 17-year veteran at Taiwan Semiconductor Manufacturing Co., Ltd. ("**TSMC**"). In 2009, Liang resigned from TSMC, upon which a two-year non-competition clause in his employment agreement with TSMC came into effect. Shortly after his resignation, Liang became a faculty member at Sungkyunkwan University in Korea, a university that closely collaborates with Samsung; subsequently in 2011, Liang commenced employment at Samsung in Korea.

TSMC sought the following legal remedies: (i) prohibiting Liang from disclosing trade secrets, (ii) imposing a non-competition period (to the effect of prohibiting Liang from working at Samsung) until December 31, 2015, and (iii) prohibiting Liang from assisting Samsung in soliciting TSMC employees to work for Samsung.

At trial in Taiwan's Intellectual Property Court, the court ruled for TSMC on Items (i) and (iii), but rejected TSMC's petition to impose a non-competition period on Liang's employment at Samsung. On appeal, the Intellectual Property Court ruled in favor of TSMC on all counts, including the prohibition from employment at Samsung. The Supreme Court upheld the appellate court's ruling.

7.2 Legislative Response

In partial response to industry concerns that arose from this case, while the matter was pending before the courts, Taiwan's Legislative Yuan amended the TSA to impose

rigid criminal liabilities for trade secret disclosure (Article 13-1) and criminalize the use of stolen trade secrets in foreign jurisdictions, including China (Article 13-2). In addition, where the representative, proxy, employee or personnel of a corporation or natural person commits the criminal activities listed in Articles 13-1 and 13-2 in the course of performing his/her/its work duties, the corporation or natural person may be fined as the penalty independent of the criminal liability imposed on the offender (Article 13-4).

7.3 Impact on Trade Secret Protection

Similar to the law in other jurisdictions, the judicial adjudication of non-competition provisions in Taiwan rests on the reasonableness of the restrictions as to the duration of the restriction, the geographical restrictions and role of the individual subject to the non-competition agreement. TSMC's case deserves special attention because the court recognized TSMC's claim that the non-competition period should be extended even after the originally agreed period of 2 years, and that the geographical restriction should be extended from Taiwan to a foreign jurisdiction, i.e., Korea.

Unfortunately, most of the judgment in TSMC v. Liang Mong-song has been sealed upon the request of both parties. However, according to media reports, the decision of the court was based on concerns over the potential impact on TSMC's market position in the semi-conductor industry, in the event that no restrictions would be applicable to Liang after he signed from TSMC and joined Samsung.

The willingness of Taiwan courts to agree to a plaintiff's request for a non-competition period in excess of what the parties agreed upon in the employment agreement is a potentially powerful tool for employers seeking judicial relief when senior employees depart the company and join a competitor company.

8. Recent investigation

Due to the value and secrecy of the information in cases concerning trade secrets, most court decisions are restricted or sealed one way or another. However, recent news reports have revealed a potential new case in Taiwan which is worth following. The case relates to Marketech International Corp ("MIC") and RBC Bioscience Corp. ("RBC"). MIC is a Taiwanese company headquartered in Taipei with global operations and branch offices in the Netherlands, Indonesia, Singapore, United States and other locations, and is one of the biggest semi-conductor system integration providers and an important player within the Foxconn conglomerate. RBC is a local manufacturer of reagents and devices for life science and molecular diagnosis, with distribution networks throughout the world. RBC has business with, and purchases devices from, MIC.

According to news reports, two MIC employees left the company and joined RBC, for which MIC alleged that the former employees had taken MIC's trade secrets relating to the design and technical information of certain proprietary devices. MIC therefore

instituted legal actions under the TSA against the two former employees and their supervisor at RBC, which resulted in the search by the prosecutor of both RBC offices and the former employees' residence.

Media also reported that, prior to the departure of the two employees from MIC, MIC had warned RBC that the two employees were not competent and, if RBC employed them, MIC would take legal actions against the two employees. In an unusual turn of events, a week after the first media report, RBC issued a press release which stated (i) MIC's claims were false, (ii) MIC was leveraging on wrongful TSA accusations and criminal procedures to harass RBC's employees with a view to impeding RBC's R&D efforts, (iii) MIC devices had a high defective rates substantially affecting RBC's sales performance, (iv) MIC employees, including the two former employees, had left the employ of MIC because of lengthy overtime spent on fixing defects in MIC's devices, (v) MIC only warned RBC that the employees were not competent but did not mention any concern over trade secrets, (vi) RBC had owned all key or relevant technology, thus did not require any competitor's or suppliers' trade secrets. RBC also stated that MIC's legal actions had significantly affected its commercial reputation, and therefore reserved all right to institute legal proceedings against MIC.

As of July 9, 2019, the two employees involved were posted bail.

The investigation of this case continues, and no charges have been pressed as of the date of this publication.

Lin & Partners
Offices: Taipei, Taiwan
Tel: +886 2 2771 5929 Fax: +886 2 2731 2896
Email: attorneys@linandpartners.com.tw

Dr. George Lin
Managing Partner
attorneys@linandpartners.com.