CHINA INTELLECTUAL PROPERTY NEWSLETTER

A special edition on

PRC TRADE SECRETS SERIES

TABLE OF CONTENTS

1  THE IMPACT OF NEWLY AMENDED LAW OF GUARDING STATE SECRETS ON FOREIGN-INVESTED COMPANIES IN CHINA .............................................................. 2

2  HOW TO ESTABLISH A TRADE SECRET PROTECTION PROGRAM AND IMPLEMENT IT IN CHINA ..6

3  SEVERAL ISSUES CONCERNING APPLICATION OF NON-COMPETE CLAUSES IN EMPLOYMENT CONTRACT ............................................................................................................ 11

4  COMMENTS ON THE PROVISIONAL REGULATION ON THE PROTECTION OF TRADE SECRETS FOR CENTRAL STATE-OWNED ENTERPRISES ................................................. 14

5  PENAL PROTECTION OF TRADE SECRETS ............................................................................. 16
The Impact of Newly Amended Law of Guarding State Secrets on Foreign-Invested Companies in China

A new amendment to the Law of Guarding State Secrets (“the Amendment”) was enacted by the Standing Committee of China’s National People's Congress (China's legislative body) late April and will go into full effect on October 1, 2010. There are two points worth paying attention to the implementation of the Amendment. First, it is an attempt to enhance the protection of state secrets in the age of information technology. Second, because of the global concern over Rio Tinto case, Chinese government has developed more stringent policies towards business operations of foreign invested companies in China.

I. The Amendment Strengthened the Management of Information System Storing State Secrets

In light of the information technology, the existence and operation of state secrets have changed dramatically. The storage and transfer of the state secrets have developed from paper media to multimedia such as sound, light, electricity, magnetism and other forms. Most of the leakage of state secrets occurred over the Internet. Therefore, the law has to be amended to perfect the system of storage, processing and transmission of state secrets in the information environment.

The newly added Article 22 provides that proper facilities and equipments shall be built to protect information system carrying state secrets. The facilities and equipments must be planned and constructed together with the information system. The information system should be properly examined by different levels of the administrative agencies before used for storage of state secrets.

The Amendment also provides guidelines on how to use the information system storing state secrets. Article 24 requires that the computer and storage equipment used for state secrets may not be connected to the Internet and other public information networks. No information exchange is allowed between the information system carrying state secrets and the Internet and other public information networks without proper protective measures. The information containing state secrets may not be stored and processed by ordinary computers or other storage devices. The security program and management software may not be uninstalled without permission. The computers or storage devices used for
stated secrets may not be sold, donated or disposed without proper process to permanently erase the state secrets. Article 26 further limits transfer of state secrets using unprotected wired or wireless communications, the Internet or other public networks.

II. The Amendment Defines Confidentiality Obligations and Liabilities of Internet Service Providers

The Amendment has clarified three obligations for Internet Service Providers ("ISPs"): collaborative investigation, stop transfer and delete sensitive information. Article 28 provides that ISPs shall be required to detect, report and delete information deemed to be disclosing state secrets, and to assist the police and state security departments in investigations of leaks of state secrets. Information transmissions should be immediately stopped if they are found to contain state secrets. According to the Amendment, once a leak of a state secret has been discovered, records should be kept and reported to responsible authorities. Information related to disclosure of state secrets shall be removed upon request of public security authorities or administrative agencies responsible for protection of states secrets.

The Chinese government has enacted a series of laws to enforce internet management in the past several months. For example, on December 11, 2009, CNNIC issued a Notice Regarding Domain Name Registration Information Audit requiring users to submit domain name registration application materials online. Individual users cannot register domain names without business license or enterprise organization code. According to the Chinese Tort Law, effective as of July 1, 2010, when internet users infringe the rights of a third party, the infringed party has right to notify an ISP to take necessary measures to delete, block and broken the links to the posted materials. The ISP is jointly and severally liable for the damage increase if he did not take the necessary measures in time after receiving the notice. ISPs are jointly and severally liable to internet users if they knew that internet users infringe the rights of others through the Internet and they did not take the necessary measures. The implementation of a series of laws and regulations leads the legal obligations of internet companies to a new level.

III. The Amendment Seeks A Balance between Information Openness and State Secrets Protection

There were some practical problems during the enforcement of the original law. For example, the levels and authorities of the state secrets are not very clear and sometimes abused by authorities in the past. The Amendment also dictates a more standardized and open process of classifying and declassifying information. The state and provincial governments as well as their authorized agencies may determine three levels of state secrets as extremely confidential, highly confidential and confidential. Cities or
autonomous counties with districts and their authorized agencies may determine two levels of state secrets as highly confidential and confidential.

For the purpose of protecting citizen’s right to information, the Amendment limits the period of confidentiality. Except as otherwise provided, the period for extremely confidential information, highly confidential information and confidential information is no more than thirty years, twenty years and ten years respectively. In addition, the Amendment added reasonable use of information resources as a principle. It further stipulates that information shall be open to the public if the laws and regulations require to do so.

IV. Questions and Suggestions

Prior to the Amendment, a primary problem commonly encountered by companies is lack of exact definition of state secrets and its extent. In many situations, it is difficult to determine what can be considered as state secrets.

The Amendment still followed the original definition of state secrets. Namely, state secrets are defined as any items/matters concerning national security and interests, are only known to certain group of people within certain period in accordance with legal procedures. State secrets have been so broadly defined so that virtually anything, including maps, GPS coordinates, even economic statistics, could fall into the category. The definition leaves a wide scope for administrative agencies in interpreting the law. Government officials sometimes use this as an excuse to avoid disclosing certain information.

According to law, in case of databases, all the statistical data generated by the Bureau of Statistics or other governmental authorities are usually considered as state secrets before being legally disclosed. If any data containing specific enterprise involves military, national security and national monopolized industries (oil and gas, electricity and finance), all the non-disclosed information (according to the Article 9 of the Amendment) may also be treated as state secrets.

According to above, it is important for companies operating in China to identify the source of the information and take appropriate precautions. If the information comes from a sensitive source, it must be used and published with caution. ISPs must have specialized staff and mechanism to monitor the publication of the information. For the information that possibly involves state secrets, necessary measures shall be taken. For example, limits transfer or removes the link. ISPs shall be collaborative to investigations conducted by judicial or administrative authorities. In some instances, there may be conflicts between a confidentiality commitment to users and the duty to cooperate with the authorities. Such situation is more difficult to deal with.
It is still some time away before the Amendment becomes into its full effect. The impact of the foreign companies operating in China, the Internet companies in particular remains to be seen. We recommend that companies take precautions to avoid potential legal risks.
How to Establish a Trade Secret Protection Program and Implement It in China

In today’s competitive business and information environment in China, protecting a company’s trade secrets becomes a critical factor to a competitive advantage over its competitors. We have seen many Chinese companies with relatively complete systems of trade secret protection with strict security measures. However, the implementation of the security measures remains a big problem. While outside consultants and security agencies often are extremely valuable and necessary resources for protecting trade secrets, this article proposes a proactive strategy for protecting trade secrets in China.

I. Definition of a Trade Secret

To determine how to establish and maintain a trade secret protection program, it is important to know what a trade secret is.

Article 10 of the Anti-unfair Competition Law (1993) of China defines a trade secret as follows:

(i) technical and business information that is unknown to the public,
(ii) which has economic value and practical utility, and
(iii) the trade secret owner has taken measures to maintain its confidentiality.

By definition, trade secrets may be considered all corporate information, regardless of forms, including processes, methods, recipes, specification, business and marketing strategies, customer lists, materials, technical and financial information so long as they meet all of the above requirements.

II. Development of a Trade Secret Protection Program

A Trade Secret Protection Program ("TSPP") is a comprehensive written policy for protecting trade secrets. Such written policy is not only evidence of a company’s intent and effort to protect the secret. It also helps employees to identify and protect the company’s trade secrets, demonstrates management’s commitment to that goal and provides notice to third parties that the company claims certain information as a trade secret.
A TSPP generally consists of two phases: realistically determining and identifying what information is a trade secret and deciding how to protect that information.

a) Designate the Personnel or Group Responsible for Implementing the Program

The first step in developing a TSPP is to designate the personnel, group or committee responsible for monitoring and supervising the program.

Selecting a group or personnel will vary from company to company. In some companies, it may be cost and time efficient to have one or two individuals coordinate and implement the entire TSPP. In other companies, there may already be an existing intellectual property group of employees who can easily take on the administrative role of trade secret protection. In some large companies it may be a valuable investment of time and resources to establish a specific managerial function that handles the protection of proprietary information. Since development and implementation of the TSPP is a cross-disciplinary activity that could involve legal, IT, HR, finance and key technical personnel. Such personnel or group will be responsible for identifying, classifying, declassifying and archiving trade secrets, as well as establishing and reviewing the company’s security measures for trade secret protection.

b) Identify Trade Secrets

The second step to set up a TSPP is to identify the trade secrets that a company intends to protect. The actual trade secret information and classification schemes will vary widely from company to company. To determine whether given information is trade secret, the following factors may be considered: (i) extent to which information is known outside the company, (ii) value of information to a business and its competitors, (iii) amount of effort or money spent in collecting or developing information, (iv) ease or difficulty with which information could be properly acquired or duplicated by others, (v) could it be commercially harmful to a business, (vi) competitive advantages a business developed.

c) Conduct a Trade Secret Audit

A company should conduct a balanced trade secret audit to determine: (i) what measures are in place to secure trade secrets, (ii) whether these measures are effective, and (iii) what additional measures need to be put in place. The audit process will improve and ensure the protection of trade secrets. The audit process itself should be implemented in two stages: (i) an initial start-up phase of review, and (ii) periodic reviews of the system.

d) Develop a TSPP
Once a company identified its trade secrets and designated personnel responsible for the protection of trade secrets, it is necessary to develop a program to protect them from misappropriation by employees or competitors.

A TSPP should be in writing and reflect reasonable efforts in the light of the nature of the respective business under the circumstances to safeguard a company’s trade secret. The measures stated below are some illustrative, but not exhaustive to protect trade secrets. Every company should tailor its security measures to its own needs and abilities. The paramount concern should be to protect a company’s trade secret information efficiently, while limiting internal disruption.

i. Contractual Protection of Trade Secrets

Chinese law permits companies to contractually protect their trade secrets. Such agreements may also address issues, such as confidentiality or nondisclosure and non-compete. Due to the high evidentiary burden, written agreements are vital in protecting trade secrets in China.

1. Enter into confidentiality and non-disclosure agreements with employees and third parties concerning the trade secret

Nondisclosure agreements are one of the best and most powerful tools. In pursuing business opportunities, disclosures of trade secret information should occur under a license or non-disclosure agreement that describes the information being disclosed, states purposes for the disclosure and the permitted exclusive uses of the information, and reiterates the other party’s obligation to maintain the secrecy of the information. Employees and business partners should sign non-disclosure agreement at the inception of any relationship.

If a Non-Compete Agreement is used, be sure it is for a reasonable time period with appropriate compensation and applies to an appropriate geographic region. Otherwise, a court may be unwilling to enforce it even though its remaining provisions are enforceable.

2. Establish and distribute written confidentiality policies to all employees.

An effective TSPP must include a program for ensuring that employees are aware of the trade secret status of information and are periodically reminded of their confidentiality obligations.

ii. Physical Protection of Trade Secrets
All companies should institute physical security measures which are the easiest and most cost-effective ways to protect proprietary information. General physical measures may include the following measures:

1. **Document control.** Mark document, items and software containing trade secrets with clear and noticeable proprietary legend, such as “confidential,” with a uniform system.

2. **Control trade secret access to employees and public.** Trade secrets should be segregated from non-trade secrets to differentiate between what the company regards as a trade secret and what it does not. Disclosure of trade secrets should be limited to only those employees who require such information to perform their duties for the company. Reasonable steps to restrict public access to your facilities may include locking trade secrets materials away from business tours and requiring visitors to wear security badges.

3. **Screen speeches and publications.** A company needs to avoid unnecessary disclosure of trade secrets at trade shows, in publications or press releases and during public speeches.

4. **Regularly educate employees and consultants about your TSPP and monitor their compliance.** By educating your employees and consultants about the importance of trade secret protection, and consequences of violating the company’s secrecy procedures helps to minimize the likelihood of disclosure. Trade secret protection should be discussed with employees before they are hired, periodically throughout their employment and upon leaving the company.

5. **Increase computer security.** Protective measures must include efforts to identify and safeguard digital intellectual assets both internally and externally in this information age. For examples: use passwords and change them periodically. Keep trade secret files in coded or encrypted form so outsiders cannot read them.

6. **Physically destroy highly sensitive information on a regular basis.**

7. **Monitor competitors.** Actively monitor the markets that your company moves in and especially your company’s direct competitors for signs that trade secrets have been disclosed and exploited.

### iii. Additional Measures to Protect Trade Secrets

A company may utilize some business considerations to protect its trade secrets. For example:

1. **Adopt incentive approaches for proprietary rights, such as establishment of reward rules for know-how.**
2. Enter into a long-term employment as appropriate. A longer employment relationship can keep key folks on duty so that to prevent employees from bringing confidential information of former employers onto potential competitors.

3. Set up special arrangements to protect trade secrets. Allow trade secret holders or controllers to own part of the equity share of the company. By doing so, it will enable the right owners to adhere to the fate of the business. Such means are widely used in developed countries.

III. Conclusion

It is said that a trade secret once lost is lost forever. Protecting a company’s trade secrets requires vigilance and adherence to a well-developed policy. An effective program will prevent valuable trade secrets from leaking to competitors and ensure that a company maintains its competitive edge. In the real word, very few companies take all of the measures or precautions listed above. A company should realistically appraise its industry and its own security needs. The program should be tailored to the business’ existing structure and procedures. Outside consultations may be required as necessary.
Several Issues Concerning Application of Non-Compete Clauses in Employment Contract

A non-compete clause or covenant not to compete (CNC), is a term used in contract law under which one party (usually an employee) agrees not to pursue a similar profession or trade in competition against another party (usually an employer). As a contract provision, a CNC is bound by traditional contract requirements including the consideration doctrine. The use of such clauses is premised on the possibility that upon their termination or resignation, an employee might begin working for a competitor or starting a business, and gain competitive advantage by abusing confidential information about their former employer's operations or trade secrets, or sensitive information such as customer/client lists, business practices, upcoming products, and marketing plans. Conversely, a business might abuse a non-compete covenant to prevent an employee from working elsewhere at all. Accordingly several issues are still in debate in practice.

I. Standard of the Minimal Compensation within Defined Non-Compete Period

At present, there is no clear policy on the minimal compensation to a former employee bound by a CNC. It is court's discretion to determine the amount of compensation in judicial practice. Generally, the following factors may be considered in determining the amount: (i) wages of the former employee, (ii) the effect on the living of the former employee, (iii) related local laws or regulations or recommended amount, if available, (iv) industrial standard, if available.

In practice, standards may vary from court to court. A meeting held by the Beijing High Court in 2009 determined that the minimal compensation standard was 20-60% of the last wage received by the former employee before leaving. However, the opinion from the Shanghai High Court in March 2009 suggested that the standard be 20-50% of the last wage received by the former employee before leaving.

II. Whether the Compensation Below Standard or No Compensation Will Make the CNC Invalid?

Since compensation from an employer is a bargain for the CNC, it is unfair for a former employee if the amount of compensation is too low. In addition, judges might rule that the CNC is invalid in this situation. The CNC could also become invalid if there is no compensation clause in the employment contract. A typical case is British ABC Specificity Food vs. Yu and Star Inc, where the court ruled that the former employee had no duty to follow the CNC since no compensation clause was included in the employment agreement.
The CNC is normally used to protect the intellectual property rights of an employer. If the CNC becomes invalid due to lack of the compensation clause, it might be a serious problem for the corporation to protect its own intellectual property rights. Therefore, several courts have adapted the opinion that CNC could still be valid even if there is no compensation clause in the employment contract. The amount of compensation could be negotiated by the parties while the suit is pending, or it could be determined by the court. Both High courts in Beijing and Shanghai have expressed similar opinions.

As an employer, in order to effectively protect its intellectual property rights, it is wise to avoid extreme low compensation which may lead the CNC to become invalid. However, given that the uncertainty of the current laws and regulations, the employer may set up more flexible compensation clauses in the employment contract. For example, the employment contract could still include a definite standard of compensation, but with options for a higher amount if the court ruled so. It needs further prescribe that in no event that such stipulation will affect the validity of the CNC.

III. How to Determine the Amount of Compensation for Breach of CNC?

The Chinese Labour Law allows an employer to agree liquidated damages for breach of contract in case of violation of the CNC. No clear guideline on the amount of compensation for breach of contract has been provided. However, it should be based on the possible loss of the employer when the employee violates the CNC. Several factors may be considered when determining this amount:

a) Wages of the former employee.

b) Importance of the employee’s knowledge on the employer’s intellectual property rights.

c) Degree of the violation of CNC.

In Nike v. Zhao, Nike claimed liquidated damages as the amount of CNC compensation which Nike paid to the defendant. This claim was supported by court.

IV. Except for Employment Dispute Settlement Procedures, Whether An Employer Can Directly Bring A Civil Action on Grounds of Unfair Competition after An Employee’s Violation of the CNC?

Based on current judicial practice in China, an employer may bring a civil action on grounds of unfair competition. The defendant could be the former employee and/or the former employee’s new employer. In a case ruled by the Haidian District Court in Beijing in 2005, the court allowed the plaintiff to raise the suit based on a CNC in the employment contract with its former employee. The new employer involved in the unfair competition after its employment of the former employee of the plaintiff. The unfair competition suit was sustained by the court. The court held that "in the present case, the plaintiff sued the
defendants Chen Jin Su and Sobey for unfair competition with a strong allegation that Chen Jin Su violated the agreed CNC. Sobey became an unfair competitor as a joint infringer. The plaintiff's claim on the ground of unfair competition is not incompatible with the law. Therefore, the dispute has been transformed to an ordinary civil and commercial dispute.

There are normally more advantages for an employer to choose a lawsuit based on unfair competition as compared to the dispute resolution in the employment contract. However, several issues must be addressed before the employer brings the civil suit. First, the plaintiff must prove damages caused by the defendant (for example, the disclosure of the trade secret or the loss of the business opportunities). Second, if the new employer of the former employee is involved in the suit, the plaintiff must prove that the new employer knew or should have known the fact of prior employment contract with the plaintiff.

V. What Have to Pay Attention to A Non-compete Agreement From the Perspective of Protecting Intellectual Property Rights?

a) The applicable parties in the CNC are limited to the senior management staff, senior technical staff and other employees responsible for the trade secret in the corporation.

b) The term of the CNC should not exceed two years. From corporate perspective, the employer could utilize more flexible mechanism to adjust the term if the restricted period is less than two years. For example, the employer may add a clause in the contract to extend or cut the term based on actual situation (compensation may also be adjusted accordingly). There could also be a clause to extend the term if the former employee violates the CNC.

c) The amount of compensation may be more flexible. For example, the employer may set up a reasonable amount of compensation in the employment contract, but add that a higher amount may be applicable if the court ruled so. This is to avoid the invalidation of the CNC due to low compensation amount to the former employee.

d) The amount of compensation for breach of contract should be clearly stated in the contract. This amount normally equals to the amount of compensation in the CNC. Another clause may be added that more penalties will be imposed if the actual loss to the employer cannot be determined.
Comments on the Provisional Regulation on the Protection of Trade Secrets for Central State-Owned Enterprises

The recent case of Rio Tinto has revealed a serious situation of trade secret protection in China. With this case in mind, it is not surprising that the Stated-owned Assets Supervision and Administration Commission of the State Council (SASAC) issued the Provisional Regulation on the Protection of Trade Secrets for Central State-Owned Enterprises (the “Regulation”) on March 25, 2010. As the first regulation on trade secret protection in China, it raised a higher standard on trade secret protection issues for Central State-Owned Enterprises (CSEs).

The definition of trade secret in the Regulation is similar to that in Article 10 (3) of the Anti-Unfair Competition Law of China enacted in 1993. Both definitions contain the same four elements. However, the difference is that the Regulation placed operational information before technical information. This change probably is an indication of the attitude of SASAC on the importance of operational information protection.

For the first time, the Regulation has defined the scope of trade secrets in details. The trade secrets include both operational information and technical information. The operational information includes strategic plans, management mechanisms, business models, business organization/reorganization, IPO status, buy-out/buy-back information, financial status, investment plans, purchasing/sales plans, resource management, customer directory, tendering and bidding information, etc. The technical information includes designs, programs, product formula, manufacturing techniques, production methods, know-how, etc. Essentially all the important fields and issues in the manufacturing and operational processes are covered in the Regulation.

The Regulation also clarified the existence of the overlap between trade secrets and state secrets. If any operational information or technical information falls into the definition of the state secrets, it must be protected as the same. It further provides that trade secrets of CSEs may become state secrets according to an adjustment of the scope of state secrets. The right to determine the scope of the state secrets was stipulated in the newly amended Law of Guarding State Secrets which will become into effect on October 1, 2010. The scope of state secrets and the levels of confidentiality are determined by administrative agencies responsible for the protection of state secrets together with other central government bodies including foreign affairs, public security, national security or other associated agencies.

For the internal protection procedures, the Regulation requires all the CSEs establish executive departments and appoint specialized staff for the task of trade secret protection.
The established department must determine the scope, degree and term of the trade secrets. A Confidentiality Agreement or Non-Compete Agreement stipulating the rights and obligations may be signed with employees who require such information to perform their duties for the company. Such agreements shall clarify responsible departments and areas involving trade secrets, information carriers as well as information security of computer system.

For the external protection procedures, the Regulation has established three different levels of confidentiality. First, the CSEs must enter into a confidentiality agreement with relevant parties if trade secrets are involved in the consultation, negotiation, technical review, achievement appraisal, collaboration, technology transfer, stock/shares buying or selling, external auditing, due-diligence investigation or bankruptcy. Second, the CSEs shall establish and improve trade secrets review procedures, clarify the confidentiality obligations of relevant departments, agencies and employees if trade secrets are involved in the domestic or overseas stock/share issuance, IPO or information disclosure of listed companies and other activities. Third, the trade secret protection procedures must be established before beginning of any key projects, important negotiations and major programs. If these projects or programs are related to the national security, they must be reported to relevant state authorities.

Not only does the Regulation provide important legal basis for protecting trade secrets, but also it sets up higher standards for establishment and improvement of the trade secrets protection system within CSEs. In compliance with the Regulation, the establishment of trade secrets protection system becomes imminent. From our practical experience, an effective trade secrets protection system should include at least the following aspects: an identification system of trade secrets, trade secrets protection program, rules or policies on protection of trade secrets for employees, internal executive departments for implementing the trade secret protection program, improvements of physical protection of trade secrets, prevention of disclosure of trade secrets through information technology and the Internet.
Penal Protection of Trade Secrets

According to Chinese law, an owner or right holder of a trade secret (the “right holder”) may explore several pathways to protect its rights against infringement of its trade secret and recover the damages caused by infringement. Two major pathways are through administrative and judicial protections. Penal protection is one of the strongest and most effective measures in the juridical route. There are still many problems in seeking penal protection to protect the trade secret right. For example, the burden of proof is too high to the victim. The jurisdiction and filing standards are still not very clear. Judicial authorities and authentication agencies still lack experience.

Zhong Lun Law Firm has handled a number of influential criminal cases related to trade secrets in recent years. Lawyers have tried to accumulate extensive experience in this area of law. In this communication we would like to share our experience and offer some tips to our clients regarding to penal protection of trade secrets.

I. Jurisdiction of Criminal Cases Related to Trade Secrets

It is important to carefully determine a proper venue and court with jurisdiction before initiating a lawsuit because of some constraints such as local protectionism and lack of experience. Such analysis may affect the outcome of the case.

The possible jurisdictions for a criminal case involving trade secrets include the location of the victim (the infringed company), the place of the suspect who implements the infringing technology or the place where the infringing products are sold. There is a dilemma in the preparation stage of the cases due to the uncertainty of the jurisdiction. In particular, whether the Public Security Bureau where the infringed party locates has jurisdiction over the case remains a question. On the one hand, some cases are not accepted by any theoretical jurisdictions. Cases are transferred from one jurisdiction to another. On the other hand, the judicial powers are abused by some courts impeding free movement of talented people and technology dissemination. According to Article 24 of the Criminal Procedure Law, a criminal case shall be under the jurisdiction of the people's court in the place where the crime was committed. An employee in breach of the employment contract or taking the trade secret away without permission may be considered as a preparation of the criminal act. Therefore, the place where the infringed company registers or operates thus has the jurisdiction over the case. This opinion is generally accepted by many case laws.

II. Filing Standard of Criminal Cases Related to Trade Secrets
Pursuant to the Rules on the Standards of Prosecution of Economic Crime Cases (April 18, 2010, No. 11 [2001] promulgated jointly by the Supreme People's Procuratorate and the Ministry of Public Security, allegedly one of the following circumstances should be prosecuted in violation of trade secrets: (i) the direct damage to the right holder is more than RMB 500,000; or (ii) the infringement caused bankruptcy of the right holder or resulted in other serious consequences. Pursuant to Article 7 of the Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Certain Issues Concerning the Application of Law in Handling Criminal Cases Involving Infringement of Intellectual Property Rights, any person or enterprise committing any of the acts mentioned in Article 219 of the Criminal Law, if the amount of losses caused to the right holder of trade secrets is not less than RMB 500,000, shall be deemed as "causing heavy losses to the right holder of trade secrets", and shall be convicted of infringing the trade secrets and sentenced to a fixed-term imprisonment of not more than three years or criminal detention with the concurrent imposition of a fine, or shall be subject to a fine alone. If the amount of losses caused to the right holder of trade secrets is RMB 2,500,000 or above, the infringer shall be deemed as "causing especially serious consequences", and shall be convicted of infringing the trade secrets and sentenced to a fixed-term imprisonment of not less than three years but not more than seven years, with the concurrent imposition of a fine.

There is still no clear definition of “causing other serious consequences.” No judicial interpretation in this regard has been issued. According to judicial practice, we believe that one of the following circumstances shall be considered as serious consequence to the right holder:

a) Misappropriation of trade secrets caused the loss of competitive advantage or corporate closure of the right holder.

b) The reputation of the right holder is severely affected due to the misappropriation of trade secrets.

c) Misappropriation of trade secrets caused serious injury or death of the right holder.

d) Misappropriation of trade secrets caused irreparable harms.

III. Burden of Proof in Criminal Cases Related to Trade Secrets

A common feature in the Rules on the Standards of Prosecution of Criminal Cases among the Ministry of Public Security, the Supreme People’s Court and the Supreme People's Procuratorate is that a specific amount of economic loss is required. In the early stage of committing a crime, the right holder probably does not know the exact amount of damage, or the exact amount of damage is difficult to assess. It has set up a significant high threshold for a right holder seeking penal protection. Specific data resulting from infringement act must be supported by certain investigation techniques. However, the investigation may be permitted only after the start of the criminal prosecution. Sometimes it is a paradox for the right holder.
Usually, the Ministry of Public Security will review the evidence based on the following criteria at the inception of acceptance of a criminal case related to the misappropriation of trade secrets:

a) Evidence proving the effectiveness of the alleged trade secret.
b) Initial evidence proving that the suspect has accessed to the trade secret.
c) Damage to the right holder is more than RMB 500,000; or research and development cost is more than RMB 1,000,000 million.
d) Initial evidence showing that the suspect has used the trade secret if unlawful use of the trade secret is accused.

To follow the above requirements, the victim has to collect the following evidence upon filing a criminal case:

a) The evidence to prove existence of the right holder and the trade secret

The evidence shall include: the basic information of the right holder, the content of the trade secret, the media carrying the trade secret (such as drawings and blueprints), documents related to the development process, documents proving cost of research and development and the evidence of utilization of the trade secret by the right holder.

b) The evidence to prove the secrecy of the trade secret

These should include: technical opinions from the experts in the field, opinions from the administrative agencies, search reports provided by scientific Information agencies; achievement evaluation certificate and report, etc.

Whether or not it is necessary to prove the secrecy of the trade secret is still controversial in judicial practice. Some people viewed that the secrecy is a kind of passive fact and cannot be proved. The plaintiff (or the victim) should not be required to provide the evidence of secrecy. The burden of proof should be shifted to the defendant (or the suspect). Other people consider that the plaintiff (or the victim) has the duty to provide some initial evidence of secrecy for filing purpose. The plaintiff should search for related databases or archives to determine the initial secrecy. In theory, we agree with the first opinion. However, in practice we endeavour to fulfill the strictest burden of prove in the progress of criminal cases.

c) The evidence to prove protective measures of the trade secret

The evidence may include: trade secret protection system of the right holder, confidentiality agreement(s), the classification of the trade secret based on the level of secrecy, the distribution policy of the documents, the network management policy, and the password policy used in guarding trade secret.
d) The evidence to prove the value and practical utility of the trade secret

Generally, the economic and practical value of trade secrets does not produce much controversy. If a product or technology containing the trade secret has been commercialized, the commercialization of the trade secret itself is a prima facie evidence to prove its economic and practical value. If a product or technology containing the trade secret has not been placed into the market, its value shall be proved by showing its supremacy of the technology or the potential commercial value.

e) The evidence to prove illegal acquirement of the trade secret by the suspect

The evidence includes theft, inducement, bribery, coercion, misrepresentation, breach or induce breach of confidentiality obligations, or by electronic or other means of espionage, or evidence proving that a person who has access to the trade secret reproduced or used it by memory.

f) The evidence to prove abuse of the trade secret

These should include access, use or permit others to use the trade secret in illegal ways. Sometimes the suspect may have access to the trade secret with the permission of the right holder with confidentiality obligations. In this situation, the main tasks are to collect evidence of control of the trade secret, confidentiality obligations as well as unlawful use of the trade secret by criminal suspects.

g) The evidence to prove damages

The damage to the right holder should be comprehensively evaluated. The following evidence may be collected: (i) business cost relating to development of the trade secret, maturity of the trade secret, use cycle, possibility of repeated use, market supply and demands. (ii) market value and licensing of the trade secret. (ii) reduction of income due to the infringement act. For example, a specific order has transferred to the suspect, the market decline or incremental decrease in sales amount, income forced to reduce. (iv) the profits made by the infringer of the trade secret through use or assignment.

IV. Conclusion

The victim and its lawyer’s solid evidence preparation in a trade secret misappropriation case is extremely vital due to a high burden of proof. In a case relating to trade secret misappropriation involving a chip company, we have achieved favourable results because of careful planning and preparation of the evidences in advance.
The editorial panel of this issue includes:
  - Mr. Chen, Jihong, Partner
  - Ms. Cheng, Bing, Senior Associate
  - Mr. Zhang, Hongbin, Associate
  - Ms. Yang Weihua, Associate
  - Ms. Liu, Jianing, Associate

This Newsletter is intended only for reference use, and does not represent any legal opinion from Zhong Lun Law Firm. If you need further information or discussion, please reach us at:

CHEN, Jihong, Partner
T: +86-10-5957-2288 | 5957-2003(direct)
E: chenjihong@zhonglun.com | www.zhonglun.com