MWE China Law Offices 律师事务所
McDermott Will & Emery

JUNE 2015

Focus on China Compliance

Welcome to the third issue of *Focus on China Compliance*. Running the Chinese operations of an international business is undeniably challenging, but it can be extremely rewarding for those businesses that work with local experts. In a survey conducted by the US Chamber of Commerce, 74 per cent of senior executives representing US companies working in the Pacific Rim region said their company's level of trade and investment had increased over the last two years. To this end, this issue provides practical, business-focused advice for handling foreseeable challenges, such as preparing for the China Securities Regulatory Commission's crackdown on insider trading and manipulation in China's capital markets, working with employees to facilitate effective compliance investigations, and dealing with data security breaches.

McDermott Will & Emery LLP enjoys a unique strategic alliance with MWE China Law Offices in Shanghai. We intend for this publication to provide regular insight into the rapidly evolving China compliance landscape. If there is a topic you would like to see covered in a future issue, please e-mail an editor.

John C. Kocoras
Partner, McDermott Will & Emery

Leon C.G. Liu
Partner, MWE China Law Offices

Increased Scrutiny by Chinese Securities Regulators Will Have Global Implications

Kirk Watkins and John C. Kocoras

The China Securities Regulatory Commission (CSRC)—which, like the US Securities and Exchange Commission (SEC), is tasked with regulating and overseeing the issuance and trading of stocks on domestic exchanges—recently announced a campaign to crack down on insider trading and market manipulation in China's growing capital markets. This new campaign is just one example of the CSRC's increased focus on insider trading and its effects on retail investors, under the helm of its new chairman, Xiao Gang. This focus in mainland China corresponds to an increased interest in insider trading abroad on the heels of a recent US appellate court decision, *United States v Newman*, 773 F.3d 438 (2d Cir. 2014), which heightened the standards for proving insider trading in certain circumstances.

The impact of the most recent campaign and related efforts to address insider trading affecting Chinese stock exchanges will likely extend beyond China's borders, owing to foreign investors' participation in China's capital markets, and potential cooperation between the CSRC and overseas securities regulators like the SEC. Businesses investing in China, and those considering doing so, should pay close attention to these developments and ensure they have in place policies prohibiting deceptive or manipulative practices, and that these policies are effectively communicated to employees, agents and officers.

CSRC Enforcement: Recent Announcement on Insider Trading and Market Manipulation

On April 24, 2015, the CSRC unveiled a campaign to address concerns over insider trading and stock manipulation in China's expanding capital markets. "False statements, insider trading and market manipulation" have "gravely disturbed the market order," said the CSRC in a statement accompanying the new campaign. According to the statement, the initial phase of the campaign will focus on five categories of illegal activity:

1. Financial fraud involving mergers and acquisitions of listed companies
2. Stock price manipulation using information advantages
3. Insider trading on the share transfer platform for unlisted companies
4. Trading on the basis of nonpublic information by employees of securities firms
5. Futures market manipulation.

In connection with this announcement, the CSRC provided two further indications on the steps it intends to take in applying a "tightened grip" on insider trading. First, the agency signaled an investigatory focus on what a CSRC spokesman described as "[s]ome new and hard-to-detect illegal trading tactics [that] have emerged along with innovative reform in the country's private equity sector, the over-the-counter market, the futures market and the new business of margin trading and short-selling." Second, in addition to oversight of the two main stock exchanges in Shanghai and Shenzhen, the CSRC committed to increase oversight of the National Equities Exchange and Quotations, an over-the-counter equity exchange primarily used by unlisted technology companies. According to the Chinese media, large valuations and increasing transaction volumes on this exchange have caught the CSRC's attention.

CSRC Background: Agency Structure and Enforcement Trends

The announcement of the CSRC's campaign is only the most recent example of an increased focus on insider trading by a developing agency under the direction of a new chairman. The CSRC is a ministry-level agency that regulates China's securities and futures markets under the authority of the State Council. Established in 1992, the CSRC operates in a similar manner to the SEC, regulating stock markets, and the US Commodity Futures Trading Commission (CFTC), regulating futures markets. The CSRC, like its US counterparts, was granted authority to regulate the securities and futures markets by national, comprehensive legislation (China's Securities Law). Through its various divisions, the CSRC exercises market oversight, enforcement and rule-making functions, and has responsibility over the issuance and trading of Chinese stocks and derivative products.

The current chairman of the CSRC is Xiao Gang. Xiao previously worked at the Bank of China, the country's central bank, for over 30 years and served as its chairman from 2003 to 2013. Notably, Xiao was chairman of the Bank of China during a period of growth in wealth management products and, upon his appointment to the CSRC in 2013, the *South China Morning Post* noted that investors and bankers spoke highly of his "outspoken style after the recent scandals involving [these] products."

Almost immediately after Xiao's appointment, the CSRC began to signal that insider trading and market manipulation were to be significant areas of the agency's enforcement efforts. In October 2013, Xiao published an article in China's state-run newspaper stating that "[p]rotecting the interest of small investors has been a key hurdle of the development of the capital markets," and noted that such retail investors often suffer from inadequate information and illegal behavior in the market. Two months later, in December 2014, the CSRC announced plans to establish a task force to investigate companies and individuals suspected of manipulating certain stocks. In a January 2015 press release, the CSRC announced that investigations into insider trading alerts and registered insider trading cases increased by 21 per cent and 33 per cent respectively on a year-on-year basis, and that the agency has referred 125 individuals and three companies to law enforcement officials based on insider trading concerns during that time. Insider trading is "a malignant tumor of the capital market," the CSRC said in the January 2015 press release, and a "violation of the fairness, justice and transparency of the market."

Beyond China: Insider Trading and Securities Enforcement in the United States

The CSRC's efforts to address insider trading also follow an increased focus abroad, much of which centers on *United States v Newman*'s direction of how authorities must prove insider trading at trial.

In the United States, securities laws and regulations prohibit the use "in connection with the purchase or sale of any security . . . [of] any manipulative or deceptive device or contrivance," (15 USC § 78j(b)), which includes insider trading. Authorities generally can establish a person's liability for insider trading under one of three theories:

1. Situations where a corporate insider trades a corporation's securities on the basis of material, nonpublic information (the "classical" theory)
2. Situations where a corporate outsider trades a corporation's securities on the basis of material, nonpublic information in breach of a duty to the owner of the information (the "misappropriation" theory)
3. Situations where an insider provides material, nonpublic information to a third party—a "tippee"—for a personal benefit (the "tipping" theory).

In *Newman*, the Second Circuit Court of Appeals held that for a tippee to be liable for insider trading, the government must prove that the tippee actually knew, or should have known, that the information was obtained by a corporate insider's breach of a fiduciary duty (often more difficult to prove the further removed the tippee is from the insider) and that the corporate insider obtained a tangible *quid pro quo* benefit of a "potential gain of a pecuniary or similarly valuable nature."

The long-term impact of the *Newman* decision is currently unknown. The securities and white-collar criminal defense bar has aggressively used *Newman* to challenge recent insider trading convictions and prosecutions. On the other side, the US Attorney for the Southern District of New York—who prosecutes a large number of Wall Street financial crimes, including many insider trading cases—has spoken publicly against *Newman* and may appeal the decision to the US Supreme Court. Mary Jo White—Xia's equivalent at the SEC and, like Xia, an enforcement-focused securities regulator appointed in 2013—has expressed "concern" over *Newman*, which she calls an "overly narrow view of the insider trading law." She has also raised the possibility of the SEC creating a new rule to prohibit trading on material, nonpublic information, regardless of personal benefits or knowledge thereof, in essence reversing *Newman*. US lawmakers have proposed similar bills to this effect.

While the eventual resolution of this issue in the United States has no direct effect on Chinese securities laws and regulations, the CSRC reportedly has a close working relationship with its US counterparts. For example, the more-established SEC provides ongoing training and technical support to the CSRC, and the development of insider trading law in the United States and the lasting effect of *Newman* could impact the development of insider trading enforcement in mainland China.

International Concern: Opening Markets and Cross-Border Cooperation

Alternatively, the CSRC's campaign against insider trading in mainland China could affect individuals and entities abroad. China's capital markets have greatly expanded in the last 25 years, and continue to do so at a considerable rate. The Shanghai stock exchange is the third largest in the world by market capitalization (US$5.5 trillion), and an index based on this exchange has doubled in price over the past year. Many foreign investment banks have formed joint ventures with, or bought stakes in, Chinese securities or brokerage firms.

Additionally, foreign investors can invest in Chinese companies through the direct purchase of B-shares, or the purchase of A-shares through the tightly-regulated Qualified Foreign Institutional Investor (QFII) system. Opportunities for foreign investment are not limited to Chinese stocks; in January 2015, the CSRC sought public comments on proposed rules that would open the Chinese futures markets to direct trading by foreigners for both speculative and hedging purposes.

The CSRC's cooperation with securities regulators in other countries also could affect foreign individuals and entities. As of February 2015, the CSRC has entered into memoranda of understanding with at least 59 overseas authorities, including the SEC and the CFTC. Notably, the SEC recently sanctioned four accounting firms for their refusal to turn over documents in

China related to investigations of potential fraud in the United States, and the SEC has announced plans to work with the CSRC in obtaining documents for US regulatory compliance.

Recommendations

Based on China's enforcement history in other areas of government focus, particularly areas related to its attractiveness to foreign investors, it would not be surprising to see Chinese authorities bring high-profile insider trading and manipulation cases in an effort to boost confidence in the integrity of their markets.

Companies that are involved in trading activity in China, and companies with securities traded in China, would be well-served to adopt insider trading and anti-manipulation policies and procedures, and provide associated training. US policies, procedures and training materials could be adapted for those purposes, with a review by China counsel for compliance with China securities laws and regulations. Companies without such policies or procedures in place—but whose conduct or securities may interest the CSRC—should urgently put them in place in response to the CSRC's warnings.

Kirk Watkins is an associate based in the Firm's Chicago office. He focuses his practice on complex litigation, including securities defense, ERISA litigation and class action defense

John Kocoras is a partner in the Chicago office in the White Collar & Securities Defense group.

Effective Employee Suspension Agreements to Facilitate Compliance Investigations

Wilson Wan

Corporate internal investigations and government investigations typically focus on employees who are identified by authorities or internal sources, including whistleblowers, as potentially involved in misconduct. Such employees often occupy senior positions within the company or otherwise exert significant influence. Properly handling the employees involved in allegations, particularly those under investigation, is crucial to ensuring effective compliance investigations that minimize disruption to the organization.

In order to achieve the goals of the investigation and limit liability risks, companies may need to distance certain employees from investigations. This distance might include reducing their contact with other employees as much as possible to create an environment conducive to an investigation. At the same time, the companies typically must seek maximum cooperation from the same distanced employees. Because the employees have been singled out for investigation and their reputations placed at stake, they often become mistrusting or hostile, adding to the challenges of managing an investigation effectively.

Fortunately, based on our experience in a broad range of compliance investigations, MWE China has developed a general set of best practices for successfully managing these challenges. Each investigation presents unique issues that must be addressed on a case-by-case basis, but these general principles are important to keep in mind.

The first step often involves entering a suspension agreement with employees whose conduct is being investigated. A well-tailored suspension agreement will properly balance the company's and relevant employees' interests, and manage the investigation risks posed by their potentially competing interests.

Key Elements of an Effective Suspension Agreement

The employee usually should be placed on what is sometimes referred to colloquially as "gardening leave." This is leave of an open-ended term, during which the employee continues to receive the same salary and benefits. The employee should be required to return all company-issued computers and phones, and all hard copy company documents and data, plus the employer should be decided whether or not to freeze his or her company email account.

Not only does this form of leave comply with People's Republic of China employment law, it might help reduce the employee's hostility while limiting opportunities to damage the company and obstruct the investigation. It does, however, also increase the burden on the company, which will need to find another employee to fill the role of the employee on leave.

The suspension agreement should usually include a clause requiring the employee on leave to cooperate with the investigation. The provisions often mandate that the employee maintains open communication with the company, provides truthful and timely responses to any questions posed by the company and/or the company's counsel, attends any interviews requested by the company at a location of its choosing, and provides any documents requested by the company or letters of authorization necessary for the company to complete the investigation within an appropriate timeframe.

The employee should be explicitly prohibited from interfering with the investigation. The restriction should be broad enough to prohibit any activity that would hinder the investigation, such as destroying any materials related to the conduct at issue, communicating with other employees involved in the investigation, and threatening other company employees or third parties.

Securing an Agreement

In our experience, negotiating this type of agreement is a highly adversarial process. To protect themselves, employees may resist any restrictions on their conduct. Alternatively, they often ask the company for broad concessions in exchange for cooperating or agreeing to basic restrictions, such as immunity from punishment by the company for any misconduct. It is essential that the company does not enter any purported "immunity" agreements for a variety of reasons. These include the fact that such an agreement can create the mistaken impression that the company has the authority to determine whether or not a criminal action should be brought, and the risk that the company appears committed to employing someone who it might discover has created substantial liability.

Successful negotiation depends on careful preparation that takes into account a variety of factors, including the employee's personality and the particular reputational damage that will result from being placed on leave. Success typically requires experienced lawyers, among other company resources, who collaborate on a robust strategy to present an agreement that convincingly balances all parties' interests.

Wilson Wan is Counsel at MWE China Law Offices. Wilson has more than 10 years' experience in devising and implementing investigation plans involving allegations of white collar crime and compliance violations for multinational companies doing business in China.

Protecting Against Counterfeit *Fapiaos*

Rex Homme, StoneTurn Group

As the Chinese Government increases its anticorruption crackdown, and US regulators continue to conduct global investigations, multinational companies should consider ramping up proactive transaction monitoring to identify potential corruption issues before US or Chinese regulators come knocking. High-profile investigations in China have yielded insights for regulators across a variety of industries. One, in particular, involves the reliability of supporting documentation, or *fapiaos*, required for business transactions in China.

What is a *Fapiao*?

Fapiaos are legal receipts or invoices for everything from taxi rides to travel agency fees and are required by law for every business transaction in China. They are printed and issued by the tax authorities of the provinces, autonomous regions and municipalities directly under the Central Government. They contain the tax authority's seal and invoice numbers and their exact form varies from industry to industry. While *fapiaos* serve as supporting documentation for payments, the government's primary objective is to monitor the tax paid for any transaction.

Since taxpaying businesses are required to purchase *fapiaos* from the government to issue to their customers, regulators have insight into the level of the taxpaying business' activity. Further, since some *fapiaos* are sold in preprinted amounts, the government can, to a certain extent, track actual transaction activity through *fapiaos*.

Because *fapiaos* represent evidence of payment, there is black market demand for counterfeit and original ones to document expenditures. Simply by walking the streets of major cities in China or by surfing the internet, one can easily find a willing seller.

How problematic are fake *fapiaos* in China? In a recent, high-profile investigation, Chinese authorities accused a UK-based company of paying approximately US$500 million in bribes to doctors and government officials in China. Media sources reported that the scheme was perpetrated in part through the use of fake *fapiaos* involving travel agencies. It would therefore be fair to say that they are very problematic.

Transaction Monitoring

A common phrase of wisdom in compliance is: "If you don't know what you are looking for, how will you know if you find it?" To implement effective transaction monitoring, companies should perform a risk assessment for the respective countries in which they are conducting an analysis, and consider both the quantitative and qualitative risks in that market. This includes evaluating transactions by industry and country.

Specifically, companies should review and analyze general ledger detail, disbursements and accounts payable data, and sales information to identify any potential red flags that may warrant further investigation. Quantitative risks include round amounts and recurring, similar payments to suspicious vendors; unusual discounts given to customers; and abnormal total spend activity, among other activities. Qualitative risks include geographic risks, the company's product mix, past audit/investigations findings, business unit characteristics and other factors.

While there is often a focus on payments to third parties as the primary risk for corruption investigations, employees can use *fapiaos* to inflate their expense reimbursements to generate excess cash to bribe government officials or to perpetrate an internal fraud against the company. Accounting departments often rely on *fapiaos* as support for expense reimbursements and do not question the reasonableness of the amount and the necessity of the reimbursements.

Taking into account the concerns discussed above, relying solely on *fapiaos* as proof of payment carries considerable risk. Companies should consider reviewing bank statements or credit card statements to confirm that the expenses their employees are claiming were actually incurred and paid. More importantly, however, like any proper substantive testing analysis, companies should assess the reasonableness and timing of the payments.

Conclusion

Just as financial institutions are required to follow "know your customer" procedures to combat money laundering schemes, companies should adequately identify, assess and evaluate the risks inherent in transactions and proactively monitor them. Companies operating in China should give the proper weight and scrutiny to *fapiaos* when analyzing and testing transactions. Not only can transaction monitoring instill piece of mind from a regulatory compliance standpoint, but it can also help increase efficiency from both a cost and timing perspective if, and when, issues arise.

Rex Homme is a Partner at StoneTurn Group. He has 25 years of experience in providing clients with financial consulting and accounting advice on forensic accounting investigations, complex business litigation matters and general business-related disputes.

Preventing International E-mail Fraud

Jacky Li

Let's imagine for a moment that you are the Chief Executive Officer of a US-based company. The Chief Financial Officer asks you for an update on a remittance to an account in Mainland China belonging to a Hong Kong-based supplier, sent according to your instruction. This is confusing, as you never sent any such instruction. After reviewing the e-mail, you realise that your e-mail account has been hacked or your e-mail address spoofed by fraudsters, and they sent the instruction. You contact your US bank, which tells you the money has already been transferred and there is nothing they can do. The destination bank in Mainland China tells you they are unable to help since the remittance was transferred according to their procedures.

The US law enforcement agencies say they have limited investigative power because the hacker came from another country and they have no jurisdiction over China. The Mainland China law enforcement agencies inform you that the hacker's company is registered in Hong Kong and you the victim are in the United States, so they have no jurisdiction over the case. The Hong Kong police tell you that innumerable shell companies are set up and operate in Hong Kong and it is difficult to conduct an investigation and obtain evidence as the

people involved might never have been in Hong Kong, even though the company is registered there.

At that moment, you realize that you are largely powerless against international e-mail frauds that take place in a modern society with advanced technologies and despite sophisticated laws. All you can do is to accept the losses and wait to be compensated by your insurance company, if you have the right type of insurance and the actions of you and your team so far havenot jeopardized your insurance claim. .

The Extent and Cost of International E-mail Fraud

The fraud described above is so common, the Federal Bureau of Investigation (FBI) and antifraud community refer to it by a universal name: the Business E-mail Compromise (BEC). BEC is a sophisticated deception targeting businesses working with foreign suppliers and other businesses that regularly make wire transfer payments.

In 2014, the US Internet Crime Complaint Center (a partnership between the FBI and the National White Collar Crime Center) received BEC complaint data from victims in every US state and 45 countries, totalling 2,126 victims and a combined total worldwide loss of US$214.97 million.

According to statistics released by the Chinese Public Security Ministry, in 2013 the total number of suspects arrested for e-mail fraud was more than 250,000, which marks a 15 per cent increase on 2012. A research report on network criminal data from the first quarter of 2015 published by the Network Security Guarding Corps of Shanghai Public Security Bureau and Beijing Network Security and Anti-Fraud Alliance (BNSAA) and the 360 Network Security Center shows that the BNSAA opened 4,920 cases relating to e-mail fraud in the first quarter of 2015, with an average loss per case of around RMB 3602 (approximately US$580.51), making a total loss of more than RMB 17.72 million (US$2.86 million).

Aside from financial losses, international e-mail fraud can damage companies' internal information systems. In addition to the risk of theft of data by fraudsters with access to the company's e-mail system, hacking activities can create a "hole" that allows other hackers access. Confidential data, including sensitive business data and trade secrets, are at risk of being stolen. If such data fall into the hands of criminals, the trust between the company and its clients can be irreparably damaged and the company may become the target of lawsuits.

Common Characteristics of International E-mail Fraud

According to the FBI, e-mail frauds often have the following characteristics in common:

- The businesses use open source e-mail.
- The targeted individuals are those responsible for authorizing and processing wire transfers.
- The fake e-mails mimic legitimate e-mails very closely in that they are specific to the business and well-worded so as not to arouse suspicion.
- The phrases "code to admin expenses" and "urgent wire transfer" often appear in the fraudulent e-mail requests.
- The amount of the fraudulent wire transfer request is business specific; dollar amounts requested are similar to normal business transaction amounts and therefore do not trigger any alarms.
- Fraudulent emails were received on dates that coincide with periods when the executives whose e-mails were spoofed were on business trips.
- IP addresses frequently trace back to free domain registrars.

Responding to E-mail Fraud

The actions listed below can help reduce losses and will generally help to maximize the possibility of them being covered by existing insurance policies.

CONTACT THE BANKS IMMEDIATELY

If the company is fortunate to discover the scam quickly after the remittance is sent, then it should contact the bank and stop the payment immediately. There have been cases where the companies discovered the fraud in time to prevent the payment being made.

TELL LAW ENFORCEMENT AGENCIES

It is important to report the fraud to the law enforcement agencies in all the countries affected by the fraud. Although the authorities may not be able to help because of jurisdictional issues, it is often necessary to report the incident for insurance purposes and to enable the authorities to get a full picture of the extent of this type of crime.

SEEK LEGAL ASSISTANCE

Instructing a legal team with multi-jurisdictional capability and experience is often vital to maximize the chances of recovering losses and avoiding falling victim to similar frauds in the future. Because of the multi-jurisdictional nature of such frauds, it is imperative to involve lawyers who are familiar with, and have ready capacity to cover the different legal systems of all the countries involved, to enable them to pursue your case from the outset and increase the chances that the fraud will receive the full attention of the relevant law enforcement authorities.

SEEK ASSISTANCE FROM THIRD PARTY INVESTIGATION FIRMS

Law enforcement agencies are reluctant to get involved in investigating e-mail frauds because of the difficulties in finding any usable evidence. A third party investigation firm may be able to uncover enough information on the perpetrators to convince the law enforcement agencies to pursue a case.

FILE INSURANCE CLAIMS

The company's insurer should be contacted and insurance claims prepared with the help of insurance specialists.

Preventative Measures

Ideally, of course, companies should ensure they cannot fall victim to such crimes. The following measures will help protect businesses from falling victims to the BEC.

IMPROVE THE COMPANY'S E-MAIL MANAGEMENT SYSTEM

- Do not use free web-based e-mail without strong security controls; create a company domain and use it to create secure company e-mail accounts.
- Be careful about what is posted on social media and company websites. Outlines of who is responsible for what, hierarchal information, and details of when executives are out of the office all give hackers valuable insight into the workings of your company.
- Update software, hardware and antivirus systems thoroughly and often.
- Immediately delete unsolicited e-mails (spam) from unknown parties. Do not open spam e-mails, click on links contained in them or open attachments, as these often contain malware that will give hackers access to your computer system.

CREATE AND ENFORCE FINANCIAL TRANSACTION VERIFICATION PROCEDURES

- Verify and monitor all financial transactions by setting up a system of checks and risk prevention procedures to be implemented by a dedicated department staffed by qualified professionals.
- Use other communication channels, such as telephone calls, to verify significant transactions. Arrange this second-step authentication process immediately on reaching an agreement with a new supplier and establish it through a channel other than e-mail to avoid interception by a hacker.
- If possible, use digital signatures where the email technology allows and the practice would not violate local laws limiting the use of encryption.

UPDATE INTERNAL ANTI-FRAUD TRAINING AND BEST PRACTICES

Employees should be made aware of some of the most common signs of fraudulent activity so they can identify and report it quickly. These common signs include requests for secrecy or pressure to take action quickly, and sudden changes in business practices such as changing the methods of communication. Always confirm *via* other channels that you are still communicating with your legitimate business partner and not a fraudster.

The easiest but most effective change employees can make is to always use the "forward" option rather than "reply" when responding to an e-mail involving a request for payment. Employees should select "forward" and type in the correct e-mail address or select it from the e-mail address book to ensure the intended recipient's correct e-mail address is used.

PURCHASE INSURANCE

The market for cybercrime insurance reportedly is outgrowing other segments of the insurance market, but many companies have not yet aligned their coverage to the risks in this area. Because of the difficulties in investigating fraudsters and recouping losses, and the unfortunate proliferation of cybercrime, purchasing appropriate insurance is usually worth the money and effort.

Jacky Li is an associate at MWE China Law Offices. Jacky is a former officer of the Public Security Bureau (China national police) with extensive experience in forensic investigations.

Data Breaches in China: A Roadmap to Successful Mitigation

Jared Nelson

Data breaches and data theft are growing phenomena in China, posing a significant threat to businesses' data security across all industries. According to a 2015 American Chamber of Commerce survey of US businesses operating in China, 96 per cent stated that the data security risks in China are greater than or equal to the risks in other jurisdictions. Victims are not only subject to potential leakage or illegal disclosure of their important commercial information, but may also suffer significant reputational damage and face serious legal liability.

A clear roadmap for dealing with breaches is a crucial tool in fighting the most difficult challenge posed by these problems: making the correct decisions very quickly while under immense pressure.

Step 0: Understand Your Notification Duties and Know Your Potential Liabilities

The starting point in preparing for and reacting to a breach event is to know your legal obligations and risks. Companies operating in China are subject to significant self-review and reporting obligations and the Chinese Government has recently been tightened its scrutiny on information security and the enforcement of related laws. There are now more than 50 laws, rules and policies in China regulating data privacy and penalizing data breaches and data theft.

Breaches that trigger liability are not confined to events involving external hackers. As in the United States, breaches committed by employees may also create liability for their employers. In addition, distinct liabilities and differing punishments apply based on the industry in which the breach occurs. For example, pursuant to Article 20 of the Regulations of the People's Republic of China for Safety Protection of Computer Information Systems, a data breach in an IT company may lead to the suspension of its business license, while a breach happening in a financial company may result in criminal liability or substantial fines.

Against this backdrop, it is often imperative for a company that falls victim to a data breach or theft to engage experienced counsel and immediately take swift action to mitigate the risks. External advisors can play a crucial role in this process and also subsequently review and restructure the company's internal security system and policies to find and fix loopholes.

GENERAL DUTY OF NOTIFICATION

When implementing and enforcing relevant laws, local governments tend to take the hardest stance against data breaches that involve the loss of customer information, which is the focus for most notification rules. For example, the Shanghai Municipal Government recently promulgated the Regulations of the Shanghai Municipality on the Protection of Consumers' Rights and Interests, an implementation rule which mandates that local entities inform affected customers "in a timely manner" and immediately adopt rectifying measures. Under such circumstances, it can be cumbersome and costly for companies with a considerable customer base to comply with notification obligations if there has not been substantial preparation ahead of the breach event.

NOTIFY AND INVOLVE THE GOVERNMENT

In some situations, a company experiencing a data breach is obliged to report it to the government. For example, according to Article 14 of the Provisions on Protecting the Personal Information of Telecommunications and Internet Users, a telecommunications company or an internet information service provider must immediately report a data breach to the government. The government may initiate investigations into large-scale data breach incidents involving hundreds of thousands or records, and full cooperation by the company would be required.

Under such circumstances, it is imperative for the company to come up with a comprehensive crisis management strategy that works alongside the government investigation which, unfortunately, can often significantly interrupt normal business operations. Understanding the government's investigation goals and enforcement standards is also crucial to eventually reaching a favorable settlement if there is an enforcement action.

Step 1: Identify the Method, Scope, and Types of Data Involved in the Breach

When a breach happens, the first task is to gain a clear understanding of what types of data have been lost, how much was taken, and the method used to compromise security.

E-DISCOVERY

Just as e-discovery can be used to efficiently sort through millions of e-mails to determine which are protected by attorney-client privilege, the same advanced technology and methods can be used to rapidly understand and identify the types of data involved in a breach. In China this is equally important for mitigating the harm from a breach and meeting legal obligations, because different types of data give rise to different requirements when reacting to a breach.

If **state secrets** are involved in the breach, the Implementing Regulations of the Law of the People's Republic of China on Guarding State Secrets provides a special duty to notify the Administrative Department for Protection of State Secrets within 24 hours after a state secret has been, or is likely to be, divulged. In addition, the nature of the mitigation efforts and the company's potential liabilities are affected by whether state secrets were involved in the breach.

The presence of **consumer data** may open the company to additional liability and lawsuits according to the new PRC Law on the Protection of Consumer Rights and Interest. It would also create different notification requirements and specific duties to rectify damage.

The Criminal Law also stipulates that wrongful use of **sensitive personal data** may lead to substantial liabilities, including up to three years' imprisonment and significant fines. Sensitive data includes personal information that, once lost or modified, can adversely affect the data subject. Article 168 of the Criminal Law allows for heavy penalties for illegally obtaining personal information relating to Chinese citizens. While this liability would usually apply to the people or entities that caused the breach and took the data, because a large portion of breaches arise out of intentional or negligent behavior within the company, there is a significant risk of the company being found guilty of failing to adequately protect its data.

Medical institutions may face administrative warnings, suspension of licenses and civil law suits for intentionally leaking the **personal health information** of patients, as stipulated by the Law of the People's Republic of China on the Prevention and Control of Infectious Diseases as well as the Tort Law. The determination of whether a breach was intentional will rely partially on an analysis of the types of systems and controls that the target had in place to prevent or defend against an attack.

Because large-scale breaches of **financial data** may trigger significant security concerns and economic losses, the government weaves a tight net around the financial industry. For example, according to the rules on Strengthening the Safety Management of Bank Cards, Preventing and Cracking down on Crimes Relating to Bank Cards, banks must notify a bank account card owner once his or her information is leaked. Similarly, insurance companies must report breaches of their data to the China Insurance Regulatory Commission, in accordance with the Guidelines for the Management of Major Emergencies in Insurance Asset Management.

IT FORENSICS

Forensic analysis may help identify the source and method of the data breach. This can be crucial to determining whether the breach pathway is still open and the company's data is still at risk. This is also the best way to fully understand the exact nature of the breach in order to promptly rectify it and prevent it from happening again in the future.

Step 2: Manage Relationships with Stakeholders

In addition to immediately fulfilling legal reporting obligations, the victim company should designate a response team that includes experienced communicators, internal and external legal counsel, IT forensic specialists and senior managers.

This team should be responsible for communicating with the stakeholders affected by the data breach, most notably customers, business partners and employees.

Communications with people affected by the breach should be issued promptly after the discovery of the incident, and should summarise key points: the data that was lost, how this might affect the stakeholder, the good-faith efforts that are currently underway and the preventative measures that are planned for the immediate future. In addition, a statement should often be issued to the press in order to help keep media reports accurate and limit reputational damage from false reporting. These statements likewise should typically include confirmed facts about the data breach, the implications for stakeholders and the steps being taken to rectify these issues.

Step 3: Mitigate Legal Liabilities

ADMINISTRATIVE PENALTIES

In addition to fulfilling potential legal obligations, notifying the government early in the process can have a variety of benefits, including gaining credibility and reducing administrative penalties through non-contentious settlements.

CRIMINAL SANCTIONS

Under the Criminal Law, one of the most serious data-related charges against a company is that it intentionally leaked sensitive information. If sensitive information is involved in a breach, the company should immediately take steps to determine if any employees are responsible, either by directly participating in the breach or allowing it though negligence. If employees are involved, the company should isolate and discipline those employees in order to send a message to the authorities that the company does not condone their actions and that the violations originated from rogue employees instead of the company itself.

CIVIL LIABILITY

In accordance with Chinese consumer rights laws, companies should take remedial measures to minimize the losses of customers once a data breach has happened. An effective incident response plan that is quickly implemented and well documented will help show that the company took concrete steps to reduce the potential damage to its customers, and may limit future claims of liability.

Prevention: What You Can Do Now to Prepare

To help prevent and defend against claims arising out of breach events, companies should build a holistic system that includes IT, legal and compliance.

IT BEST PRACTICES

The first and most important item in preparing for a breach is to establish and implement effective information security management procedures and structures, most notably by carefully restricting access of highly confidential data to segregate and contain the most important data. A well-designed data architecture and a comprehensive information security plan should include advanced encryption, strong email filtering mechanisms and robust password requirements. An internal audit department comprising IT and forensic staff can be an effective oversight group, especially if they implement a routine auditing schedule. This group may include outside "white hat hacker" consultants and should particularly pay attention to verifying that all available security patches have been correctly implemented in a timely manner.

PERSONNEL BEST PRACTICES

The weak link in any data protection system is nearly always personnel. Companies must routinely train all employees to be aware of the constant dangers of data breaches and ensure proper implementation of IT best practices. In addition, companies should have strong checks and balances in place to ensure that employees may not abuse their IT privileges in order to unintentionally or intentionally weaken security systems or cause a breach.

IDENTIFY DATA TYPES ON AN ONGOING BASIS

Document and knowledge management systems should offer a clear method of identifying a company's data as it is added to the system. Identification, labeling and segregation before a breach occurs can be invaluable for ensuring that a quick, high-level understanding of the lost data can be obtained from the outset in order to better shape key decisions later in the process.

CREATE AND UPDATE AN INCIDENT RESPONSE PLAN

It is vitally important to have the right incident response plan in place and to continuously update it. An effective and efficient

plan should include specialized personnel, standardized processes, task checklists and contact details to quickly execute all required actions. In some jurisdictions, this plan may be a legal requirement. For example, the Regulations of the Shanghai Municipality on the Protection of Consumers' Rights and Interests requires business operators handling consumer information to "develop information security emergency response plans" and, when a breach occurs, "immediately activate the emergency response plan".

CONTINUE MONITORING THE CHANGING REGULATORY ENVIRONMENT

Over the course of the next several years, there is likely to be a significant increase in the number and scope of laws and rules that address data breaches, especially at the local provincial and city levels. Constant monitoring and continuing education will be key to maintaining full compliance with these new rules as this important system develops.

Jared Nelson is a Foreign Counsel at MWE China Law Offices. Jared leads MWE China's e-discovery team and heads the MWE China Data Center.

EDITORS

For more information, please contact your regular McDermott lawyer, or:

John C. Kocoras
+1 312 984 7688
jkocoras@mwe.com

John C. Kocoras is a partner in the Firm's Chicago office. He focuses his practice on internal investigations including Foreign Corrupt Practices Act cases, global compliance counselling, white-collar criminal defense and complex litigation. John is a former federal prosecutor and has served as managing director and regional counsel of a global investigations company.

Leon C.G. Liu
+86 21 6105 0533
lliu@mwechinalaw.com

Leon C.G. Liu is a partner at MWE China Law Offices. He focuses his practice on regulatory compliance, anti-corruption and Foreign Corrupt Practices Act, white-collar crime and government investigation. Prior to joining the Firm, Leon was a prosecutor in China.

Visit www.mwechinalaw.com or www.mwe.com to learn more.

Office Locations

BOSTON
28 State Street
Boston, MA 02109
USA
Tel: +1 617 535 4000
Fax: +1 617 535 3800

BRUSSELS
Avenue des Nerviens 9-31
1040 Brussels
Belgium
Tel: +32 2 230 50 59
Fax: +32 2 230 57 13

CHICAGO
227 West Monroe Street
Chicago, IL 60606
USA
Tel: +1 312 372 2000
Fax: +1 312 984 7700

DALLAS
3811 Turtle Creek Boulevard, Suite 500
Dallas, TX 75219
Tel: +1 972 232 3100
Fax: +1 972 232 3098

DÜSSELDORF
Stadttor 1
40219 Düsseldorf
Germany
Tel: +49 211 30211 0
Fax: +49 211 30211 555

FRANKFURT
Feldbergstraße 35
60323 Frankfurt a. M.
Germany
Tel: +49 69 951145 0
Fax: + 49 69 271599 633

HOUSTON
1000 Louisiana Street, Suite 3900
Houston, TX 77002
USA
Tel: +1 713 653 1700
Fax: +1 713 739 7592

LONDON
110 Bishopsgate
London EC2N 4AY
United Kingdom
Tel: +44 20 7577 6900
Fax: +44 20 7577 6950

LOS ANGELES
2049 Century Park East, 38th Floor
Los Angeles, CA 90067
USA
Tel: +1 310 277 4110
Fax: +1 310 277 4730

MIAMI
333 Avenue of the Americas, Suite 4500
Miami, FL 33131
USA
Tel: +1 305 358 3500
Fax: +1 305 347 6500

MILAN
Via dei Bossi, 4/6
20121 Milan
Italy
Tel: +39 02 78627300
Fax: +39 02 78627333

MUNICH
Nymphenburger Str. 3
80335 München
Germany
Tel: +49 89 12712 0
Fax: +49 89 12712 111

NEW YORK
340 Madison Avenue
New York, NY 10173
USA
Tel: +1 212 547 5400
Fax: +1 212 547 5444

ORANGE COUNTY
4 Park Plaza, Suite 1700
Irvine, CA 92614
USA
Tel: +1 949 851 0633
Fax: +1 949 851 9348

PARIS
23 rue de l'Université
75007 Paris
France
Tel: +33 1 81 69 15 00
Fax: +33 1 81 69 15 15

ROME
Via Luisa di Savoia, 18
00196 Rome
Italy
Tel: +39 06 462024 1
Fax: +39 06 489062 85

SEOUL
18F West Tower
Mirae Asset Center1
26, Eulji-ro 5-gil, Jung-gu
Seoul 100-210
Korea
Tel: +82 2 6030 3600
Fax: +82 2 6322 9886

SHANGHAI
MWE China Law Offices
Strategic alliance with
McDermott Will & Emery
28th Floor Jin Mao Building
88 Century Boulevard
Shanghai Pudong New Area
P.R.China 200121
Tel: +86 21 6105 0500
Fax: +86 21 6105 0501

SILICON VALLEY
275 Middlefield Road, Suite 100
Menlo Park, CA 94025
USA
Tel: +1 650 815 7400
Fax: +1 650 815 7401

WASHINGTON, D.C.
The McDermott Building
500 North Capitol Street, N.W.
Washington, D.C. 20001
USA
Tel: +1 202 756 8000
Fax: +1 202 756 8087