LLINKS Law Offices
通力律师事务所

上海
上海市银城中路 68 号
时代金融中心 19 和 16 楼
邮编：200120
电话：+86 21 3135 8666
传真：+86 21 3135 8600

SHANGHAI
19/F&16/F, ONE LUJIAZUI
68 Yin Cheng Road Middle
Shanghai 200120 P.R.China
T: +86 21 3135 8666
F: +86 21 3135 8600

北京
北京市建国门北大街 8 号
华润大厦 4 楼
邮编：100005
电话：+86 10 8519 2266
传真：+86 10 8519 2929

BEIJING
4/F, China Resources Building
8 Jianguomenbei Avenue
Beijing 100005 P.R.China
T: +86 10 8519 2266
F: +86 10 8519 2929

香港
香港中环皇后大道中 5 号
衡怡大厦 27 楼
电话：+852 2969 5300
传真：+852 2997 3385

HONG KONG
27/F, Henley Building
5 Queen's Road Central
Central, Hong Kong
T: +852 2969 5300
F: +852 2997 3385

伦敦
1/F, 3 More London Riverside
London SE1 2RE
United Kingdom
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

LONDON
1/F, 3 More London Riverside
London SE1 2RE
United Kingdom
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

www.llinkslaw.com
master@llinkslaw.com

Llinks Corporate and M&A Bulletin
May 2018

China Cyber Security Law Requirements on Foreign-owned Private Fund Management Business

By Xun Yang

Until May 2018, eleven wholly foreign-owned private fund management companies ("WFOE PFM") have registered with Asset Management Association of China ("AMAC") and been authorized to carry out private fund management business in China. This would become a milestone development for China opening up its private fund business.

The establishment and operation of a private fund business concern a large number of legal issues, including, in particular, protection of cyber security, given the increasingly strengthened cyber security legal regime. This article discusses a number of key cyber security requirements which WFOE PFMs must pay attention to.

1. Overview of WFOE PFMs' IT Structures

Generally speaking, WFOE PFMs prefer adopting an organizational model under which it hires a small-sized China team focusing on local business, including distribution of funds and execution of investment, whilst leaving to offshore teams the back office functions, including compliance check, IT maintenance, and administrative functions. To realize such model, WFOE PFMs typically adopt the following IT structure:

如果您需要本出版物的中文本，
请与下列人员联系：

郭建良: (86 21) 3135 8756
Publication@llinkslaw. com

If you would like other Llinks publications, please contact:

Roy Guo: (86 21) 3135 8756
Publication@llinkslaw. com

Llinks Law Offices
www. llinkslaw. com

(1) An WFOE PFM's local employees use terminals at the WFOE PFM end to submit investment proposals and to place investment orders, which terminals are connected to local servers which are in turn connected to the global servers via VPNs;

(2) An overseas compliance team conduct compliance check and risk control review from terminals which are connected to the global server; and

(3) An overseas IT team maintains IT facilities and provide IT support remotely.

2. Key Cyber Security Law Requirements

The *PRC Cyber Security Law* (the "***Cyber Security Law***"), which was promulgated on 17 November 2016, has come into effect on 1 June 2017. As the first comprehensive legislation on cyber security matters, it not only imposes a series of obligations on network operators but also revives a number of existing cyber security requirements which has been poorly enforced.

The promulgation of the Cyber Security Law and, subsequently, a series of supporting laws, regulations and guidelines trigger attentions from a wide range of businesses, including the financial service business. The private fund management business is, without doubt, affected.

Duties to maintain cyber security

The Cyber Security Law imposes a number of obligations on network operators to protect security of their networks and the information stored on the networks; wherein the term "network operator" is defined broadly to include an owners and administrators of all types of computer systems, including both internet sites and companies' intranet. WFOE PFMs usually operate a network, by which they store client information and process investment transactions as well as administer their internal functions. As such, WFOE PFMs are "network operators" regulated by the Cyber Security Law and obligated to perform cyber security duties thereunder. These duties include:

- to formulate and implement an IT security management policy and, following such policy, to adopt necessary technical measures and managerial measures to ensure the security of the networks, of which measures the security level must be considerable to the importance of the networks;
- to formulate disaster recovery and contingency plans and, following such plans, to back up data during normal operation of business and to mitigate the impact when actual incidents occur;
- to adopt and to implement personal data protection policies in compliance with legal requirements and to protect personal information accordingly; and
- to consider security issues, such as reliability, reliance, and technical redundancy, when procuring IT equipment and IT related services.

Generally speaking, WFOE PFMs heavily rely on their networks to store clients' personal information, to process transactions, and to communicate with the overseas headquarters. Consequently, the security duties which WFOE PFMs ought to perform must reflect the importance of the networks.

CHINA CYBER SECURITY LAW REQUIREMENTS ON FOREIGN-OWNED PRIVATE FUND MANAGEMENT BUSINESS

Protection of personal information

The Cyber Security Law provides for a suite of principles on personal information protections. These principles are not significantly different from EU data protection laws, including (i) to seek data subjects informed consent to the collection; (ii) to adopt proper measures to protect the personal information collected; (iii) to collect only "necessary" personal information; and (iv) not to disclose or use personal information beyond the scope of purposes to which data subjects consent.

These principle requirements seldom bring serious problem for WFOE PFMs as their headquarters usually maintain data protection policies in line with European standard. However, there are still a number of points which WFOE PFMs must pay attentions to:

- Global data protection policies must be localized before being used in China. The localization includes: (i) to amend according to some specific PRC law requirements, such as report of cyber incidents and response to customer complaints; (ii) to reflect unique technical features in China, such as the popular use of social media; and (iii) to translate the policies into Chinese in a read friendly manner.

- With respect to the collection of client vetting information from corporate clients as per overseas anti-money laundry law requirements, WFOE PFMs needs to be aware that the directors whose identity information is collected are not their client per se and, therefore, WFOE PFMs must ensure that their corporate clients have the right to provide the directors' identity information.

- WFOE PFMs may voluntarily propose investment opportunities to clients or potential clients. Here comes the issue whether the information about investment opportunity is considered "investment consultation services" or merely an advertisement. If the latter, WFOE PFMs need to consider whether they have already secured clients' consents to receive such proposals and whether the scopes of consents are sufficient.

Restrictions on data exportation

As illustrated in the business model above, WFOE PFMs export to their overseas headquarters the personal information they collect in China for client vetting and the transactional information they generate in China for approval.

Under the Cyber Security Law, export of personal data and other important business information which operators of critical information infrastructure (***CII***) collect or generate in China is, in principle, prohibited except that if such export arises from business necessity, relevant data and information will be allowed to be exported subject to a strict scrutiny process. The term "CII" is not defined under the Cyber Security Law and the guidance to determine CIIs have not been issued. However, given that most networks which WFOE PFMs operate concern largely private right and not national interest, WFOE PFMs are unlikely considered CII operators.

However, under the draft *Security Assessment Measure for Export of Personal Information and Important Data* (the "***Data Export Measure***"), the export of personal information and other important data by network operators (other than CII operators) is still subject to a security assessment procedure. Although the data Export Measure is still in a draft, it more or less reflects government's view to strengthen the control over data exportation. As a

result, WFOE PFMs, as network operators, need to undergo risk assessment procedures in order to export client information and transactional information, including to consider the sensitivity of the information to be exported, the possibility of information misuse, and proper measures to protect information security.

The performance of risk assessment procedure is not only a good practice to maintain data security but also a defence in case of data leakage during the exportation that WFOE PFMs have acted diligently in exporting client and transactional information.

Data retention requirements

Private fund managers usually prefer storing most client information and transactional data which WFOE PFMs collect and generate centrally on overseas servers and leaving very little information saved on local servers in China. This model help reduces IT costs and administrative burdens to maintain data. However, from a cyber security aspect, this may not be an ideal model.

CSRC has issued a couple of rules on information security applicable to the security and future business sector, under which a copy of client information and transactional records must be saved in China. These rules, at least arguably, apply to only public security fund managers but not private fund managers. Nevertheless, these rules represent the government's view that it is safer to retain a copy in China.

Additionally, to have a duplicated copy in China may be considered a measure to mitigate risks associated data exportation because if the data stored outside of China were destroyed, WFOE PFMs would have a back-up copy in China to recovery so as to avoid business disruption. As such, although it is not mandatory for WFOE PFMs to have a server in China, it is still recommended to at least backup in China the most important information related to Chinese clients and about investment in China.

Use of VPN for business

WFOE PFMs usually communicate and transmit data with their overseas headquarters via VPNs to ensure the security and stableness of commutations. In addition, WFOE PFMs use VPNs for connections to overseas proxy servers so that their staff in China can go onto Internet bypassing government censorship. Consequently, WFOE PFMs' local staff can visit certain websites China government blocks.

The uses of VPNs are heavily regulated in China. Generally speaking, under the current legal regime, VPN is allowed to be used for communications with group members but not for internet connections. In other words, in theory, WFOE PFMs are allowed to use VPNs to transmit client information and transactional information to overseas headquarters but they are not allowed to use VPNs to enable their staff to surf internet bypassing government censorship.

However, the government understands that business operators, such as WFOE PFMs, may have business need to visit certain websites it blocks (e.g., Financial Times) and, as a matter of fact, tolerates the use of VPN for internet connections out of legitimate commercial reasons. This requires that WFOE PFMs make rules on VPN usages and manage the risks associated with such usage. For example, WFOE PFMs are advisable to permit the use of VPNs on a "need" basis and prohibiting misuse of VPNs by both technical and managerial measures

so that WFOE PFMs can defend themselves if some of their employees misuse these VPNs.

Use of encryption technology

WFOE PFMs usually use encryption technology to protect their communications with their headquarters. Under the *PRC Administrative Measure for Encryption* (the "***Encryption Measure***"), generally speaking, companies are allowed to use only encryption products and encryption technology which are produced in China and certified by the government. There is an exception that multinational companies are allowed to use foreign-produced encryption products or technologies for communications between group members *provided* that such products and technologies as well as their usage must be filed with the government. This exception and the filing requirement apply to WFOE PFMs.

The filing requirement was not well enforced. This situation may be changing in the future since the State Council is leading to draft an Encryption Administrative Law which authorizes the Encryption Administrations to regulate the encryption market and to impose licensing and filing requirements. If the law is adopted by the congress at the current form, the filing requirements with respect to use of foreign encryption products or technology would become robust.

As such, WFOE PFMs would need, from both a legal and a practical aspects, to file with the government the encryption products and technologies which they use for communications with their headquarters.

3. Practical Suggestions

Although the government has been tightening its control over the cyber space and imposing cyber security requirements on the networks operators in China, generally speaking, such control and requirements do not prevent WFOE PFMs from operating their business in commercially justifiable manners. Rather, WFOE PFMs are required to act diligently to protect the securities of their networks and the information in their possessions.

In light of cyber security requirements and the cost to maintain cyber securities, WFOE PFMs are advised to consider the following measures to mitigate cyber risks.

Adoption, Localization, and Implementation of IT policies

Under the Cyber Security Law and related regulations, WFOE PFMs (as network operators) are required to adopt a number of IT related policies to govern their uses of IT facilities. These policies include: (i) IT user manuals which govern how employees and contractors ought to use WFOE PFMs' IT facilities, such as not to connect personal device onto the company IT systems, and to use only software programs provided by WFOE PFMs; (ii) security configuration policies, which provide for how WFOE PFMs protect the securities of their networks from technical aspects, such as virus scanning, vulnerability testing, blocking of hazardous sites; (iii) back-up and recovery policies, which govern how WFOE PFMs backup the data processed in their IT system, where to save these data, and how to recover these data; and (iv) contingency plans, which provide for how WFOE PFMs act in response to cyber incidents.

CHINA CYBER SECURITY LAW REQUIREMENTS ON FOREIGN-OWNED PRIVATE FUND MANAGEMENT BUSINESS

These policies have three functions. Firstly, it is WFOE PFMs' legal duties to adopt and implement these policies and, otherwise, WFOE PFMs and their direct responsible persons may be subject to penalties. Secondly, with well-prepared and implemented IT policies, WFOE PFMs would unlikely suffer significant cyber incidents and, even if they suffer cyber incidents, they are more ready to mitigate losses. Thirdly, well-prepared and implemented IT policies can function as a defence against administrative liabilities (and even criminal liabilities) when significant cyber incidents occur.

For those WFOE PFMs of which the group implements a global policy, they must localize their global policies to reflect specific needs in China and document them in Chinese in a reader-friendly manner. Additionally, WFOE PFMs must deliver trainings to their officers, employees, and contractors who have access to their IT systems to improve their IT security awareness.

Establishment Risk Assessment and Diligence Procures

Cyber security laws and guidelines provide for a number of scenarios where network operators are required or recommended as good practice to conduct risk assessment and diligence. These scenarios include: (i) export of personal data and important business information; (ii) procurement of IT related services or products; and (iii) significant outsourcing. These risk assessment and diligence procedures may help network operators control risks and may also function as defence against any administrative (or even criminal liabilities) arising from leakage of data or failure of networks out of these scenarios.

It is worth noting that the risk assessment or diligence is not only IT departments' responsibilities. Rather, the directors or senior managers must be involved in the assessment and decision-making process. Additionally, the process of assessment, diligence, and decision-making must be properly documented and, otherwise, the defensive effect would be prejudiced.

A Prospective Vision

The provisions in the Cyber Security Law are largely vague and principles in nature. Meanwhile, since the promulgation of the Cyber Security Law in November 2016, more than ten regulations, measures, and guidance have been issued to elaborate and to implement cyber security requirements under the Cyber Security Law. Some of these legislations are still in drafts. Question is whether WFOE PFMs should wait for elaborated guidance before taking any action or should they play actively to follow these principles.

The answer to the question may depend on a number of factors including the practicability of these principles and the cost for complying with these principles. Obviously, no WFOE PFM is advised to act too progressive beyond the customary practices. However, it is advisable not only to follow the existing legislations but also to act with a prospective vision,that is to align the business with the legislative trend. The reasons are: on one hand, the government sometimes cites "sprit" of non-binding guidance (even when it has yet come into effect) to administer cyber security matters; and, on the other, the period between the promulgation of a new regulation or measure and its effectiveness will likely be short, a few months or even shorter and, therefore, WFOE PFMs may find it difficult to alter their practice to comply with the new regulation or measure within such a short period of time.

CHINA CYBER SECURITY LAW REQUIREMENTS ON FOREIGN-OWNED PRIVATE FUND MANAGEMENT BUSINESS

Contact Details

If you would like to know more information about the subjects covered in this publication, please feel free to contact the following people or your usual Llinks contact.

Author	
Xun Yang Tel: (86 21) 3135 8799 xun.yang@llinkslaw.com	

Shanghai	
David Yu Tel: +86 21 3135 8686 david.yu@llinkslaw.com	**Bernie Liu** Tel: +86 21 3135 8678 bernie.liu@llinkslaw.com
Selena She Tel: +86 21 3135 8770 selena.she@llinkslaw.com	**Nicholas Lou** Tel: +86 21 3135 8783 nicholas.lou@llinkslaw.com
Dali Qian Tel: +86 21 3135 8676 dali.qian@llinkslaw.com	**Kenneth Kong** Tel: +86 21 3135 8777 kenneth.kong@llinkslaw.com
David Wu Tel: +86 21 6043 3711 david.wu@llinkslaw.com	**David Pan** Tel: +86 21 3135 8701 david.pan@llinkslaw.com
Elyn Jiang Tel: +86 21 6043 3710 elyn.jiang@llinkslaw.com	
Beijing	
David Yu Tel: +86 10 8519 2266 david.yu@llinkslaw.com	**Bernie Liu** Tel: +86 10 8519 2266 bernie.liu@llinkslaw.com
Yuhua Yang Tel: +86 10 8519 1606 yuhua.yang@llinkslaw.com	
Hong Kong (in Association with Vivien Teu & Co LLP)	
David Yu Tel: +86 21 3135 8686 david.yu@llinkslaw.com	**Sandra Lu** Tel: +86 21 3135 8776 sandra.lu@llinkslaw.com
London	
Yuhua Yang Tel: +44 (0)20 3283 4337 yuhua.yang@llinkslaw.com	

© This article was first published in China Business Law Journal, June 2018, Volume 9, Issue 6.