HAN KUN
汉 坤 律 师 事 务 所
Han Kun Law Offices

Han Kun Newsletter

Issue 178 (2nd edition of 2022)

Legal Updates

1. A Step Forward: MIIT Again Seeks Public Comments on Administrative Measures for Data Security
2. A Solid Step Toward Improving AML of Financial Institutions

1. A Step Forward: MIIT Again Seeks Public Comments on Administrative Measures for Data Security

Authors: Kevin DUAN | Kemeng CAI[1]

On February 10, 2022, the Ministry of Industry and Information Technology ("**MIIT**") issued a second draft of the *Measures for Administration of Data Security in the Field of Industry and Informatization (for Trial Implementation) (Draft for Comment)* (the "**Measures**"), which makes revisions to the first draft in response to public comments received following its issuance on September 30, 2021. This second draft opened for public comments until February 21, 2022.

Since 2021, the MIIT and the Cyberspace Administration of China ("**CAC**") have proposed detailed rules to implement the *Data Security Law of the People's Republic of China* (the "**Data Security Law**") and the *Personal Information Protection Law of the People's Republic of China* (the "**PIPL**"), which focus on implementation in distinct fields. To strengthen data security management in the field of industry and informatization, the MIIT has issued the Measures to implement provisions of the Data Security Law and other relevant laws and regulations. The Measures provide approaches to apply the national data security management mechanism in the field of industry and informatization in an effort to establish the data security supervision and administration system in the field of industry and informatization, through further clarification of the data classification and data grading system, management of important data and core data, and other specific requirements[2]. In respect of cyber data[3], the CAC released the *Regulations for the Administration of Cyber Data Security (Draft for Comment)* ("**Cyber Data Regulations**") for public comment on November 14, 2021. The Cyber Data Regulations propose rules for implementing relevant systems established by the Data Security Law and the PIPL; they also refine relevant requirements imposed by those laws while creating some new ones, such as the filing and annual reporting obligations of important data processors, security management duties of data processors that undertake cross-border data transfers, and responsibilities to be assumed by Internet platform operators.

Both at their formulation stage, the Measures and the Cyber Data Regulations are implementing rules respectively issued by China's two major data security regulators. Despite certain overlap between the two, they highlight different regulatory aspects due to the nature of the data they regulate, reflecting the different regulatory scopes and approaches adopted by the MIIT and the CAC.

As revised, the Measures comprise 41 articles in eight chapters (fewer than the previous 44 articles) and differ from the first draft in the following aspects:

---

[1] Yibing Zhao, a Han Kun intern, also contributed to this legal commentary.

[2] Please refer to the drafting notes of the *Measures for Administration of Data Security in the Field of Industry and Informatization (for Trial Implementation) (Draft for Comment)* by clicking: https: //www.miit.gov.cn/cms_files/filemanager/1226211233/attach/20219/1d1668e46e644b42b04a95db43854607.pdf.

[3] "Cyber data" refers to any data recorded in electronic form, which is not limited to data generated by using the internet or network or processed therein. For more information, please click: https：//mp.weixin.qq.com/s/3uewzfNMEP_2Rr9SpaULnw.

- Separate protection for personal information: PIPL added as an enabling law.
- Expanding definition of data: includes radio data into the regulatory scope.
- Further clarifies regulators' scope of authority: confirms MIIT's supervisory role over local regulatory departments.
- Revises data classification and data grading standards: changes made to grading criteria and categorization methods.
- Clearer guidance for the filing system: more specific requirements for filing applications, filing reviews, and change filings.
- Persons responsible for data security: shifts primary responsibility to legal representatives and tightens internal management requirements for enterprises.
- Updated requirements for full life-cycle data management: removes language prohibiting core data exports and imposes security obligations for processing core data among different persons.
- Coordinates data security reviews: adds flexibility to provisions on security assessments, cooperation with supervision, and other requirements.

Below, by comparing the first draft Measures (0930) and the revised draft Measures (0210), we summarize and comment on key adjustments made in the revised draft.

Separate protection for personal information: PIPL added as an enabling law

As stressed in its drafting notes, the Measures (0930) adhere to the philosophy of the Data Security Law, which emphasizes control over personal information by categorizing it in catalogues of important data and core data, thus implementing full life-cycle security management of personal information without imposing any separate protection requirements for personal information[4]. Given that, the Measures (0930) cited as their enabling laws the Cybersecurity Law and the Data Security Law, not the Personal Information Protection Law. However, the Measures (0210) add the PIPL to the list of enabling laws and correspondingly adjust other relevant provisions with respect to personal information. For example:

- "Personal information" is removed from the list of data categories in Article 8 (Methods of Data Classification and Data Grading), where non-personal information categories are retained, such as management data, operation and maintenance data, and research and development data.
- The following provision is added as Article 37 (Personal Information Protection) in Chapter 8 (Supplementary Provisions): "Data processing activities involving personal information shall also be subject to relevant laws and administrative regulations."

Given the above changes in the Measures (0210), it appears that the MIIT has turned its personal information protection approach away from "unified management by categorizing personal information in

[4] Please refer to the drafting notes of the *Measures for Administration of Data Security in the Field of Industry and Informatization (for Trial Implementation) (Draft for Comment)* by clicking: https://www.miit.gov.cn/cms_files/filemanager/1226211233/attach/20219/1d1668e46e644b42b04a95db43854607.pdf

the catalogue of important data and core data" and is heading toward separate protection of personal information. This shift of direction conforms to regulatory documents issued mainly after the Measures (0930). On November 14, 2021, the Cyber Data Regulations were issued for public comments, in which personal information was not covered by the specified definitions of important data and core data. In addition, a revised public comment draft of the *Information Security Technology - Guideline for Identification of Critical Data (Draft for Comment)* (the "**Guideline**") issued by the Secretariat of the National Information Security Standardization Technical Committee on January 13, 2022, as well as its initial draft for public comment released on September 23, 2021, both define important data clearly as "not including state secrets and personal information, but may include statistical data and derived data formed on the basis of massive quantities of personal information." To achieve consistency and coordination among relevant laws and regulations, the Measures (0210) change their approach to personal information management, emphasizing the PIPL's role as the legal basis for personal information protection.

Expanded definition of data: includes radio data into the regulatory scope

The Measures (0210) revise Article 3 (Definition of Data) as follows:

- Data in the field of industry and informatization are clearly categorized into three types, namely industrial data, telecoms data, and radio data.
- Specifically enumerated industry fields are removed: Article 3 of the Measures (0930) enumerated several industries in the field of industry and informatization, such as "raw material industries, equipment industries, consumer goods industries, electronic information and manufacturing industries, software and information technology service industries, and industrial explosive materials industries". The Measures (0210) replace this enumeration with a generalized, more abstract expression, i.e., "the field of industry and informatization", to avoid legal issues that may arise in reconciling a non-exhaustive list and changes in practice.
- Adds the definition of radio data: "Radio data refers to radio frequencies, radio stations and other radio wave parameters data generated and collected in the course of radio service activities". Corresponding changes are also made in other provisions. For example, "users of radio frequencies and stations" are added as data processors in the industry and informatization field; radio regulatory authorities are recognized as data security regulators; and electromagnetic security is included as an affected area when identifying important data and core data.

Further clarifies regulators' scope of authority: confirms MIIT's supervisory role over local regulatory departments

The Measures (0210) further specify the functions and powers of data security regulators at the central and local levels:

- The central level: The MIIT's supervision and administration activities should be subject to the State's coordinated data security working mechanism. This precondition underlies the State's overall coordination over data security work at all levels and is added to cope with existing situations where data security regulation is decentralized among multiple authorities.

- The local level: the Measures (0210) call for a hierarchical supervision framework, which is absent in the Measures (0930), specifically the MIIT's responsibility to supervise and direct local departments of industry and information technology, local telecommunications administrations, and local radio regulatory authorities in all provinces, autonomous regions, municipalities directly under the central government and municipalities with independent planning status, and the Xinjiang Production and Construction Corps; also, local industry and information technology authorities, local telecommunications administrations and local radio regulatory authorities are responsible for supervising data processing activities within their jurisdictions.
- Particularly, local regulators of the industries/fields above are required to cooperate with competent authorities in carrying out data security supervision and administration activities pursuant to relevant laws and administrative regulations.

Revises data classification and data grading standards: changes made to grading criteria and categorization methods

The Measures reiterate management requirements for data classification and data grading stipulated in the Data Security Law. The Measures (0210) make revisions to the data classification and grading working requirements and methods, as well as the criteria for identifying general data, important data, and core data, mainly in the following aspects.

- Working requirements: In the Measures (0210), the provision entitled "working requirements for data classification and data grading" is set forth as Article 7; in addition to the obligations to report catalogues of important data and core data to the MIIT, local industry and information technology departments, telecommunications administrations, and radio regulatory authorities are also required to report changes and updates to those catalogues; moreover, the requirement for enterprises to "first classify data, then grade data" is removed.
- Data classification and grading methods: According to the Measures (0210), data processors in the field of industry and information technology are allowed to subdivide the categories and grades of data based on a three-tier grading system under the Measures.
- Grading criteria: the test for distinguishing general data and important data is removed, i.e., "the price range for recovery of data or elimination of negative impacts"; a radio data-related scenario is added to the criteria for identifying core data.

However, enterprises still await clearer guidance in practice for how to implement the classification and grading of important data and core data, because the Measures lack quantified standards to identify factors such as "materially affect", "severely affect", or "materially damage".

Clearer guidance for the filing system: more specific requirements for filing applications, filing reviews, and change filings

Based on the Measures (0930), the Measures (0210) provide further guidance for data processors' obligations to file catalogues of important data and core data, specifically in the following aspects.

- Filing authorities: Data processors in the field of industry and information technology are required to file their catalogues of important data and core data with the local industry and information technology authorities (industrial field), telecommunications administrations (telecoms field), or radio regulatory authorities (radio services field).
- Filing content: In the Measures (0210), the description of the filing content is more concise and it is clarified that the content to be filed does not include the relevant data *per se*.
- Time limit for review: Local industry and information technology authorities, telecommunications administrations, and radio regulatory authorities are required to complete their review of filings within 20 working days from acceptance of the filing application.
- Review decision: If the filing is approved, the local authority should issue a filing certificate to the applicant and report the same to the MIIT; where the filing is rejected, the local authority should promptly communicate the decision, along with the grounds for rejection, to the applicant.
- Change filings: If the category or quantity of important data and core data changes by more than 30%, or, if there are significant changes with respect to other particulars, the data processor is required to complete a filing for such changes within three months after they occur.
- Update filing status: In case of destruction of important data and core data, the data processor is required to update the relevant filing status with its filing authority.

Persons responsible for data security: shifts primary responsibility to legal representatives and tightens internal management requirements for enterprises

The Measures (0930) stipulated that the first step for enterprises in fulfilling their data security management obligations was to establish and improve their data security leadership system. The Measures (0930) further provided that the Party committee (group) or leadership team would undertake primary responsibility for data security, the head of the enterprise is the first responsible person for data security, and the person in charge of data security is the person directly responsible for data security. The Measures (0210) consolidate the previous Article 13 (Subject Responsibilities), Article 14 (Working Systems), Article 15 (Key Position Management), and Article 16 (Data Collection) into a sole Article 13 (Subject Responsibilities) and modify the provisions as follows.

- Legal representative as the first responsible person: The “primary responsibility for data security” taken by “the Party committee (group) or leadership team of an enterprise” under the Measures (0930) is shifted to “the legal representative or head of the enterprise”, who would be “the first responsible person for data security” under the Measures (0210). The shift is sensible in that the Party committee (group) or leadership team, as an administerial organizational design, is not applicable to all enterprises, whereas a legal representative, the essential, principal role created by the Company Law, is more suitable to take primary responsibility for the data security of an enterprise.
- Stricter internal management requirements for data processors: Stricter requirements are imposed on important data and core data processors to “establish internal registration and approval

mechanisms to strengthen management and keep track of important data and core data processing activities".

Therefore, we recommend enterprises that process important data and core data to pay close attention to the above changes and to adjust their organizational structures going forward. Legal representatives, first responsible persons, directly responsible persons, and key personnel who are subject to data security responsibilities should attach greater importance to data compliance and take active part in data security trainings, so as to improve their data management expertise.

Updated requirements for full life-cycle data management: removes language prohibiting core data exports and imposes security obligations for processing core data among different persons

The Measures (0210) update the general requirements for protection of various grades of data in the full life-cycle of data management, as well as the additional requirements for the processing of important data and core data. We recommend enterprises to pay attention to the following changes in the compliance requirements:

- Data storage: Data processors that store important data and core data are required to carry out data recovery tests on a regular basis.
- Data use and data processing: The Measures (0210) remove the provision that prohibits data processors from "conducting unauthorized data processing activities such as precise user profiling and data recovery targeting specific subjects by using data mining, association analysis, or other technical means".
- Data disclosure: The provision is also removed that prohibits disclosure of data "involving individual privacy, personal information, trade secrets, and confidential business information".
- Destruction of data: The Measures (0210) add a provision that requires data processors who desire to "destroy important data and core data" to "update the relevant filing status with their local industry and information technology department industrial field), telecommunications administration (telecoms field), or radio regulatory authority (radio service field)".
- Data exports: The provision is removed that prohibits cross-border transmission of core data. Instead, the Measures (0210) stipulate that, where it is truly necessary to transfer core data and important data abroad, data processors must conduct a data export security assessment in accordance with laws and regulations.
- Processing core data among different persons: The Measures (0210) add the following provision as Article 24: Where different persons are involved in the provision, transfer, or entrusted processing of core data, the data processors shall conduct data security assessments, take necessary security protection measures, and have the same reported to the MIIT through the competent local industry and information technology departments (industrial field), telecommunications administrations (telecoms field), or radio regulatory authorities (radio services field). The MIIT will review the reported activities in accordance with relevant laws and regulations.

- Responding to user complaints: Article 29 of the Measures (0930) imposed mandatory obligations on data processors to "establish user complaint response mechanisms, providing the public with easy and effective access such as e-mail addresses, telephone numbers, fax numbers and online customer services, designating personnel to accept and handle data security-related complaints from users, and giving reply within 15 working days after receiving the complaint." The Measures (0210) replace these mandatory requirements with "encourage data processors in the field of industry and information technology to establish user complaint response mechanisms", easing data processors' compliance burden in responding to user complaints.

Coordinates data security reviews: adds flexibility for security assessments, cooperation with supervision, and other requirements

According to the Measures (0930), the State will implement data security supervision and administration through data security inspection, assessment, authentication, supervision, inspection and security reviews. Enterprises are obligated to conduct security assessments, assist with regulators' supervision and inspections, and pass data security reviews. The Measures (0210) make the following changes that would add flexibility in Article 5 (Data Security Monitoring, Authentication and Assessment) and Article 6 (Supervision and Inspection):

- Relaxing regulation on authentication institutions: Article 32 of the Measures (0930) required the MIIT and local regulatory departments to establish an institutional system for data security detection, assessment and authentication by means of setting institution accreditation standards and carrying out relevant work such as selecting and accrediting institutions, granting qualifications, daily management, and issuing institution catalogues. The Measures (0210) remove the above selection and accreditation obligations imposed on regulatory departments. Instead, the Measures (0210) stipulate that "the MIIT shall encourage and guide qualified institutions to carry out data security detection and authentication pursuant to relevant standards."

- Cancelling the self-assessment provision for general data processors: Article 33 of the Measures (0930) encouraged general data processors to conduct self-assessments. The Measures (0210) delete this provision and only require important and core data processors to conduct assessments on their own or entrust a third party to do so.

- Removing data processors' obligation to set aside an inspection interface: Under Article 34 of the Measures (0930), enterprises were obligated to cooperate with industry regulators in their supervision and inspections and to set aside an inspection interface for use. Accordingly, the major issues of concern for enterprises would have been the scope of inspection, technical standards of the inspection interface, and interface access conditions. However, the Measures (0210) remove this obligation to set aside an inspection interface and enterprises are only generally required to cooperate with regulators' inspections.

- The Measures (0930) provided at Article 35 that the MIIT will, under the coordinated working mechanism for national data security review, conduct data security reviews of processing of industrial and telecoms data that affect or may affect national security. On the other hand, on

January 4, 2022, 13 ministries and commissions, including the Cyberspace Administration of China and the China Securities Regulatory Commission, jointly promulgated the revised *Measures for Cybersecurity Review*, which subject data processing activities into the scope of review, stipulating that key factors for assessment include "the risk for core data, important data or large quantities of personal information to be stolen, leaked or destroyed, or illegally used or taken abroad." Therefore, under the Measures (0930), data processors would have faced two reviews pursuant to the MIIT's administrative measures and the CAC's *Measures for Cybersecurity Review*, respectively. However, under the Measures (0210), the MIIT is only required to carry out data security review work under the coordinated working mechanism for national data security review and is no longer obligated to "conduct data security reviews of industrial and telecoms data processing that affect or may affect national security." This change leaves flexibility for the MIIT and the CAC in their coordination of data security reviews.

Conclusion

Compared to the first draft, the Measures (0210) make quite a number of changes. In addition to the substantial compliance obligations mentioned above, the revised draft also makes changes in terms of wording and the assumption of legal liability (e.g., It removes the provision that incorporates data processors' data security liability into the credit management system and puts those who commit data security violations on the blacklist of dishonest subjects). The second draft coordinates the Measures with relevant laws and regulations, rectifies the wording of relevant concepts, and adds flexibility to supervision and compliance approaches. As the overarching regulatory design in the field of industry and information technology, the Measures set forth many specific compliance requirements to which enterprises in the industry and information technology field should pay great attention.

2. A Solid Step Toward Improving AML of Financial Institutions

Authors: Yin GE | Ellen MAO | Virginia QIAO | Aidan YU

Crowded release of new AML rules

With the continuous development of onshore financial markets and the ever-intensifying requirements globally for anti-money laundering ("**AML**"), it has become increasingly imperative for China to improve its AML legal and regulatory frameworks to give further play to the role of AML in building up the modern financial system and deepening the two-way opening-up of the financial industry. In 2021, the National People's Congress, the Ministry of Commerce, the People's Bank of China ("**PBoC**") and other legislative and regulatory bodies introduced a series of AML-related laws and regulations that have a significant impact on AML regulatory supervision. These laws and regulations aim to strengthen and improve China's AML frameworks and control measures from the perspectives of cross-border business, risk assessment, due diligence and so on.

The crowded release of AML-related laws and regulations in 2021 reflects a general trend in the approach to AML from "rule-based" regulation to "risk-based" regulation, such that "*pro forma*" compliance can no longer meet existing regulatory requirements. In short, the AML laws and regulations (including consultation drafts) issued in 2021 mainly include:

1. the *Guidelines for the Self-Assessment of Money Laundering and Terrorist Financing Risks by Corporate Financial Institutions* (《法人金融机构洗钱和恐怖融资风险自评估指引》), promulgated by PBoC and effective as of 15 January 2021;

2. the *Guidelines for Anti-Money Laundering and Counter-Terrorist Financing in Cross-Border Services of Banks (for Trial Implementation)* (《银行跨境业务反洗钱和反恐怖融资工作指引(试行)》), jointly promulgated by PBoC and the State Administration of Foreign Exchange on 19 January 2021 and effective as of 18 February 2021;

3. the *Measures for Administration of Client Due Diligence and Maintenance of Clients' Identity Information and Transaction Records by Financial Institutions (Revision Draft for Comment)* (《金融机构客户尽职调查和客户身份资料及交易记录保存管理办法（修订草案征求意见稿)》) (the "**2021 Consultation Draft**") jointly issued on 31 March 2021 for public comments by PBoC, the China Banking and Insurance Regulatory Commission ("**CBIRC**") and the China Securities Regulatory Commission ("**CSRC**");

4. the *Anti-Money Laundering Law of the People's Republic of China (Revision Draft for Comment)* (《中华人民共和国反洗钱法(修订草案公开征求意见稿)》) released by PBoC on 1 June 2021 to solicit public comments; and

5. the *Measures for the Supervision and Administration of Anti-Money Laundering and Counter-Terrorist Financing of Financial Institutions* (《金融机构反洗钱和反恐怖融资监督管理办法》) promulgated by PBoC on 15 April 2021 and effective as of 1 August 2021.

In addition, the *Measures for Administration of Client Due Diligence and Maintenance of Clients' Identity*

Information and Transaction Records by Financial Institutions (《金融机构客户尽职调查和客户身份资料及交易记录保存管理办法》) (the "**2022 Measures**") were jointly promulgated by PBoC, CBIRC and CSRC, to be effective as of 1 March 2022. Once effective, the 2022 Measures will replace the existing *Measures for Administration of Distinguishing Clients' Identities and Preserving Data on Clients' Identities and Transaction Records by Financial Institutions* (《金融机构客户身份识别和客户身份资料及交易记录保存管理办法》) (the "**2007 Measures**"). Further, the 2022 Measures will take precedence over any other inconsistent regulatory provisions promulgated prior to the effective date of the 2022 Measures with respect to client due diligence and maintenance of clients' identity information and transaction records.

Interpretation of the key provisions of the 2022 Measures

Financial institutions serve on the front lines of monitoring and combating money laundering activities. Therefore, improving AML of financial institutions is a core issue in ensuring the steady operation of the financial system and safeguarding a fair and just market order, which is also of great significance in combating illegal activities and crimes and maintaining social stability. Under the increasingly severe context of money laundering crimes, stricter domestic and international AML standards and the strengthening of AML regulatory supervision and penalties, a particular flashpoint for AML within the financial sector is establishing AML internal control systems that are compatible with the business characteristics of banking, securities, futures and mutual funds industries. In light of this, we analyze key provisions of the 2022 Measures, which specify the AML obligations to be performed by commercial banks, securities firms, futures firms and fund management companies ("**FMCs**").

I Applicable scope of the 2022 Measures

In light of the development of the financial sector and the diversification of business types, Article 2 of the 2022 Measures expands the applicable scope of financial institutions to cover development financial institutions, consumer finance companies, lending companies, wealth management companies, non-banking payment institutions, bank card clearing institutions and other applicable bodies, and further refines the hierarchy for the application of rules. However, the 2022 Measures do not specify whether subsidiaries of securities firms, futures companies and FMCs are included in this applicable scope. We understand the subsidiaries of securities firms will be subject to the 2022 Measures by referring to the *Official Reply of PBoC in Seeking Public Comments on the Measures for the Supervision and Administration of Anti-Money Laundering and Counter-Terrorist Financing of Financial Institutions (Revision Draft for Comment)* (《中国人民银行关于<金融机构反洗钱和反恐怖融资监督管理办法(征求意见稿)>公开征求意见的反馈》) (the "**PBoC Reply**"), because "securities firms" licensed by CSRC by definition include the subsidiaries of securities firms. However, the 2022 Measures may not apply to the subsidiaries of futures companies because their main business is not specifically considered "financial" in nature. In addition, according to the PBoC Reply, FMCs will be required to undertake AML obligations for their subsidiaries; however, PBoC may study further the AML system, the allocation of administrative resources and other issues relating to FMC subsidiaries, and then decide at a later stage whether these subsidiaries will be separately included as AML obligors. Based on the PBoC Reply, FMC subsidiaries may be classified as "other institutions engaging in financial business as determined and announced by PBoC" as stipulated in the 2022 Measures. The

requirements under the 2022 Measures will still apply by reference to FMC subsidiaries during the routine performance of their AML obligations.

Notably, the applicable scope of the 2022 Measures does not cover private fund managers (including institutions such as PFM WFOE, QDLP, QDIE and QFLP). According to the PBoC Reply, private fund managers are not included because: (i) the current definition and scope of "private fund manager" remain vague and may need further clarification from regulators; and (ii) in light of their large numbers, complex classification and limited administrative resources, it would be difficult from a practical perspective to unify regulatory requirements and substantially carry out AML work for private fund managers. PBoC intends to further study the potential money laundering risks of private fund products in conjunction with the relevant competent authorities.

II Supervision of offshore branches and subsidiaries

Profound and complicated changes have taken place in the domestic and international AML regulatory environment in recent years, in which the focus of AML has shifted from policy formulation to effectiveness, and the international consensus has become to place equal emphasis on effectiveness and compliance. The 2022 Measures in principle apply to offshore branches and certain subsidiaries of financial institutions subject to AML obligations and further specify rules relating to the concurrent application of laws in the country (or region) in which foreign branches and subsidiaries are located. The applicable provisions of relevant laws and regulations regarding client due diligence and maintenance of clients' identity information and transaction records by financial institutions and their offshore subsidiaries are as follows:

1. in principle, the relevant requirements of the 2022 Measures apply to financial institutions and certain offshore subsidiaries which are subject to AML obligations under the 2022 Measures;

2. if the country (or region) where such subsidiaries are located have more stringent requirements, such requirements must be complied with; and

3. if the requirements of the 2022 Measures are more stringent than those of the country (or region) where such subsidiaries are located, but the laws of such country (or region) prohibit or restrict the implementation of the 2022 Measures by such offshore subsidiaries, the financial institutions setting up such subsidiaries must take appropriate measures to address the money laundering and terrorist financing risks and report to PBoC.

In respect of the newly added requirement that "financial institutions should take appropriate measures to address the money laundering and terrorist financing risks", the 2022 Measures raise higher requirements for financial institutions and their offshore subsidiaries with respect to their AML capabilities under Scenario (3) above.

III Establishment of information sharing policies and procedures

In order to improve the efficiency of the AML work of financial institutions and to facilitate the unified management of AML risks by financial institutions, the 2022 Measures impose higher requirements for the synchronization and sharing of AML information:

"*A financial institution shall, at the head office level, make unified deployment or arrangement for the client due diligence and the maintenance of clients' identity materials and transaction records and formulate information sharing policies and procedures for anti-money laundering and counter-terrorist financing, so as to ensure the effective performance of client due diligence and management of money laundering and terrorist financing risks. A financial institution shall supervise and manage the implementation by its branches for policies and procedures of client due diligence and maintenance of clients' identity materials and transaction records.*"

In light of the above provision, when undertaking AML work, the shareholders of financial institutions, financial institutions themselves and their branches and certain subsidiaries (subject to AML obligations under the 2022 Measures) need to formulate corresponding joint working mechanisms, such as establishing unified standards for AML client due diligence, classified maintenance of client identity materials and transaction records, emergency plans, blacklist databases, etc.

As is common in the mutual funds industry, there remains room for improvement in actual business operation processes for relevant fund distributors in respect of the transmission of client identity information due to limitations in their systems, data transmission interfaces, information confidentiality requirements or other reasons. Such requirements provide a strong basis for the comprehensive transmission of client information where the FMC's shareholder acts as the distributor for the fund products issued by the FMC.

However, the 2022 Measures do not specify whether the above-mentioned "unified deployment or arrangement at the head office level" and "information sharing" cover the cross-border transfer of AML information to a head office located offshore, which is a key concern in the practice of many foreign-invested financial institutions. Interpreting from the context and based on our practical experience, it is advisable for foreign-invested financial institutions to communicate with competent authorities, such as PBoC, CBIRC, CSRC, etc., to be timely informed of the permissible/prohibitive scope of AML information for cross-border transmission because PRC laws and regulations do not currently set out explicit requirements on cross-border transfer of AML information.

IV Client due diligence

1. The 2022 Measures replace the previous concept of "client identity identification" in the 2007 Measures with "client due diligence", remove concepts such as the initial client identification, ongoing client identification, re-identification, etc., and highlight the principle of "focusing on substantial risks". Financial institutions must determine the extent and detailed methods for client due diligence measures per different risk levels and must not take due diligence measures that are obviously inconsistent with the risk characteristics. Financial institutions must therefore strike a balance between risk management and service optimization.

2. The 2022 Measures set out the client due diligence requirements under two separate sections of "general requirements" and "other requirements", specifying client due diligence requirements under general and special scenarios. Among the above, for high-risk scenarios or clients, the 2022 Measures further stipulate enhanced due diligence measures from pre-investigations to ex-post restrictions. For low-risk scenarios and clients, the 2022 Measures provide simplified due diligence

measures and further clarify the identification measures that should be adopted when applying simplified due diligence measures by reference to the *Guidelines for Risk Assessment of Money Laundering and Terrorist Financing and Classified Client Management by Financial Institutions* (《金融机构洗钱和恐怖融资风险评估及客户分类管理指引》). Compared with the 2021 Consultation Draft, the 2022 Measures emphasize "adjusting the service scope and business functions per risk levels" and allow for the batch processing of clients and businesses of the same type.

3. The continuous development of information technology has given rise to the era of big data, requiring diversified measures to be taken to verify client identity information. The 2022 Measures specify methods to verify client identity information, including one or a combination of the following methods:

   - verifying client identity through information obtained from the authorities in charge of public security, market regulation, civil affairs, taxation and immigration or through other public channels of the government;
   - verifying client identity through information certified by a foreign government or an international organization, etc.;
   - supplementation of other identity materials or evidence by the client; and
   - other sources of information recognized by PBoC.

   Where a bank is obliged to verify the second-generation ID card of a natural person when performing client due diligence obligations pursuant to laws, administrative regulations and departmental rules, the bank is required to conduct the verification through the Online Verification System for Citizen Identity Information (联网核查公民身份信息系统) established by PBoC. Compared with the 2007 Measures, the 2022 Measures provide certain changes on client due diligence requirements of commercial banks. For example, the 2022 Measures expand the business types that must undergo the client due diligence process (including the establishment of any business relationships with the clients by signing up an agreement). In respect of a single cash deposit or withdrawal transaction involving more than RMB50,000 or USD10,000, or its equivalent value in any foreign currencies, the 2022 Measures will now require learning about and registering the source or purpose of the funds. Nevertheless, based on PBoC's interpretation on 9 February 2022 regarding the application of the 2022 Measures, the responsible official of PBoC indicated that this new requirement will not adversely affect the normal cash deposit and withdrawal transactions of individual clients. As the next step, PBoC will guide financial institutions to formulate implementing rules to learn about and register the client information in the principle of "least and necessary" when performing AML obligations, without adding on material burdens to clients.

   In respect of securities firms, futures companies, FMCs and other institutions engaged in fund sales business, the 2022 Measures re-classify the businesses that must undergo client due diligence by specific business types (such as brokerage business, asset management business, margin trading and securities lending, stock pledge, repurchase arrangements and other credit trading business), which are different from the specific business classification standards in the 2007 Measures (such as opening, closure or change of a capital account, deposit or withdrawal of funds or other transactions).

As the classification standards between the 2007 Measures and the 2022 Measures may overlap, securities firms, futures companies, FMCs and other institutions engaged in fund sales business need to re-examine the business types that must undergo client due diligence in accordance with the 2022 Measures. In addition, by re-classifying business types, the 2022 Measures may require client due diligence to be adopted during the entire relationship with a business rather than only for certain processes under the 2007 Measures.

Currently, distributors generally carry out the verification of client identity information for clients of FMCs from distribution channels; however, for clients of FMCs from direct sales channels (including over-the-counter direct sales and online direct sales), most FMCs have established online verification mechanisms for client identity information, usually via systems provided by E-Capital Transfer Co. Ltd (证通股份有限公司) and GZT Technology Co., Ltd. (国政通科技有限公司). Such arrangements may satisfy the requirements of the 2022 Measures, i.e., "when a financial institution establishes a non-face-to-face business relationship with clients or provides clients with financial services in accordance with laws via the internet, mobile communications and other information technologies, it should establish an effective client identity verification mechanism and take effective measures to determine and verify clients' identities."

V Identification of beneficial owners

According to Article 22 of the 2022 Measures, during client due diligence, if the client is a legal person or an unincorporated organization, the financial institution must determine and verify the identity of the client, understand the client's business nature, ownership and control structure, and determine and take reasonable measures to verify the client's beneficial owner(s), i.e., one or more natural persons ultimately owning or actually controlling the legal person or the unincorporated organization identified via the following means:

1. natural person(s) directly or indirectly owning 25% or more of the equity or partnership interests in the legal person or the unincorporated organization;
2. natural person(s) independently or jointly exercising actual control over the legal person or the unincorporated organization, including but not limited to exercising control through agreement, kinship, etc., such as deciding on the appointment or dismissal of directors or senior management personnel, deciding on the formulation or implementation of major business operation or management decisions, deciding on financial revenues and expenditures, and dominating the use of material assets or major funds for a long period of time; or
3. natural person(s) directly or indirectly owning 25% or more of the rights to the profits of the legal person or the unincorporated organization.

Financial institutions must determine and verify the beneficial owner(s) of the client through a combination of the aforesaid three methods and determine the senior management personnel of the legal person or the unincorporated organization when the beneficial owner(s) is/are unable to be identified through any of the aforesaid methods.

The requirements of the 2022 Measures for the identification of beneficial owners follow a series of

similar PBoC's regulatory provisions, e.g., Article 13 of the *Measures for Administration of Due Diligence of Tax-Related Information of Non-Residents' Financial Accounts* (《非居民金融账户涉税信息尽职调查管理办法》), Article 1(iii) of the *Notice of PBoC on Work Related to Strengthening Client Identification for Anti-Money Laundering* (《中国人民银行关于加强反洗钱客户身份识别有关工作的通知》) and Article 3(i) of the *Notice of PBoC on Further Improving the Identification of Beneficial Owners* (《中国人民银行关于进一步做好受益所有人身份识别工作有关问题的通知》).

There were many obstacles in practice previously with respect to the identification of "controlling party" under PBoC's regulatory provisions. For instance, financial institutions and their clients may have different understandings as to the meaning and application of a provision; in addition, there were also cases where financial institutions and their clients had reached a consensus on the understanding and application of a provision but encountered difficulties in actual implementation. Therefore, in the actual identification of "beneficial owners" according to the 2022 Measures in the future, financial institutions need to formulate detailed identification plans internally based on their business profiles and conduct communications with their clients in advance.

VI Application in the event of business suspension

According to Article 22 of the 2022 Measures, where the term of validity of the ID card or other identity documents previously submitted by the client to a financial institution has expired, and the client fails to update within a reasonable period without giving a reasonable cause after the financial institution has performed the necessary notification procedures, the financial institution must suspend its services to the client.

Compared with the 2007 Measures, the 2022 Measures add the "necessary notification procedure" as a precondition. Financial institutions are required, during actual business operations, to make corresponding arrangements in advance in respect of the design and implementation of necessary notification procedures, communications with clients and other processes so as to achieve an effective balance between the performance of AML obligations and the prevention of client complaints.

VII Dynamic assessment of client risk ratings

The 2022 Measures specify due diligence "risk-based" and "risk tracking" principles, requiring that continuous attention be paid to the relevant information of clients and corresponding measures be taken such as the timely adjustments of risk levels, etc. Financial institutions should pay continuous attention to the changes in their clients' risk statuses, transaction profiles and identity information, and timely adjust the risk levels of clients for money laundering and terrorist financing. Based on this dynamic assessment of client risk levels, the 2022 Measures reduce the frequency of regular review of clients with the highest risk levels in money laundering or terrorist financing from at least once every six months to at least once a year.

VIII Re-examination of client due diligence

Compared with the 2007 Measures, the 2022 Measures optimize circumstances where client due diligence is required to be re-examined, including where:

1. the risk status of the client has changed;
2. the client has changed its business scope or beneficial owner;
3. the term of validity of the ID card or other identity documents previously submitted by the client has expired; and
4. other circumstances.

Although the above-mentioned rules largely mirror the relevant requirements under the *Provisions on Anti-Money Laundering by Financial Institutions* (《金融机构反洗钱规定》), the *Guidelines for the Management of Money Laundering and Terrorist Financing Risks by Corporate Financial Institutions (for Trial Implementation)* (《法人金融机构洗钱和恐怖融资风险管理指引(试行)》), the *Guidelines for Fund Management Companies on Client Risk Rating Standards for Anti-Money Laundering (for Trial Implementation)* (《基金管理公司反洗钱客户风险等级划分标准指引(试行)》) and the *Circular of PBoC on Strict Implementation of Anti-Money Laundering Provisions and Prevention of Money Laundering Risks by Financial Institutions in Securities and Futures Industries and Insurance Industries* (《中国人民银行关于证券期货业和保险业金融机构严格执行反洗钱规定防范洗钱风险的通知》), the 2022 Measures further clarify relevant issues and provide useful guidance for financial institutions to carry out their daily AML work.

IX Electronic management of clients' identity information

In light of the overall trend of systematization, integration and standardization of AML work, Article 45 of the 2022 Measures requires the electronic management of AML information.

Financial institutions must take necessary management and technical measures to gradually realize the complete and accurate maintenance of client identity materials and transaction information via electronic means, and prevent the loss, damage and leakage of client identity materials and transaction records.

Financial institution maintenance methods and management mechanisms for clients' identity materials and transaction records must be sufficient to reproduce and trace each and every transaction so as to facilitate AML work of the financial institution as well as related AML investigation, supervision and management.

Financial institutions must maintain clients' identity materials and transaction information in an auditable and traceable manner, with strong backup and leak-proof measures. In addition, the 2022 Measures strengthen the "protection of personal information and trade secrets" in accordance with relevant provisions on personal information and AML information protection in the *Personal Information Protection Law of the People's Republic of China* (《中华人民共和国个人信息保护法》) and the *Anti-Money Laundering Law of the People's Republic of China* (《中华人民共和国反洗钱法》).

X Elements of clients' basic identity information

In accordance with the current requirement of the "three certificates in one" registration system, the 2022 Measures adjust the original elements of the "clients' basic identity information" as previously set

out in the 2007 Measures, including deleting the organization code and tax registration certificate number for non-natural-person clients, etc. In addition, the original expressions of "controlling shareholder" and "actual controller" are replaced by the term "beneficial owner", consistent with other expressions in the 2022 Measures.

Compared with the 2021 Consultation Draft, the 2022 Measures delete the element of "workplace" from the information of natural-person clients, consistent with the elements of the "basic identity information" of natural-person clients in the 2007 Measures.

XI Client due diligence involving overseas institutions

With respect to the business types conducted by financial institutions with overseas financial institutions that should undergo client due diligence, in addition to the establishment of an agency relationship or a similar business relationship with an overseas financial institution stipulated in the 2007 Measures, the 2022 Measures further add the circumstance where a financial institution accepts appointments to provide domestic securities and futures trading for an overseas broker or its clients. The 2022 Measures stipulate that the financial institution may not establish an agency or similar business relationship with a shell bank and must ensure that the agency does not provide any account for the shell bank to use. In addition, the financial institution must continuously pay attention to and examine the supervision received by the overseas institution for AML and counter-terrorist financing, as well as the risk status of money laundering and terrorist financing of the country or region where the overseas institution is located, assess the risk level of the overseas institution and implement dynamic management. Financial institutions may not conduct client due diligence by relying on a third party from a high-risk country or region.

Key areas to be strengthened in the future

In recent years, in order to effectively respond to the assessments of China's AML and counter-terrorist financing efforts carried out by the Financial Action Task Force on Money Laundering (FATF) and strengthen AML regulation in the financial sector, various market participants are faced with the significant task of AML risk control. In the process of fulfilling AML obligations, there are a series of issues being discussed frequently within the industry that need to be continuously improved and optimized, including (a) inadequate money laundering risk prevention and control systems, insufficient money laundering risk assessments for businesses and products, and the failure to allocate AML resources in a risk-oriented manner; (b) lagging staffing and system set-ups; (c) insufficient client due diligence and incomplete client information; (d) lack of means for suspicious transaction monitoring and analysis; and (e) failure to establish a substantive review mechanism for the source of large-sum subscription funds, etc.

As the next step, in view of the above issues and the relevant requirements of the 2022 Measures, financial institutions should pay attention to the following key areas and make enhancements accordingly.

I Formulating a classified client due diligence mechanism

According to Article 7 of the 2022 Measures, where a financial institution, at the time of establishing a business relationship with a client, processes a one-off transaction above the stipulated amount or, throughout the lifecycle of the business relationship, suspects that the client and its transactions are

involved in money laundering or terrorist financing or has any doubts about the authenticity, validity or completeness of the client's identity information obtained previously, it must conduct due diligence on the client and take the following due diligence measures:

1. determining the client's identity and verifying the identity through supporting materials, data or information from reliable and independent sources;

2. understanding the purpose and nature of the business relationship and transactions established by the client and obtaining relevant information based on the risk status;

3. understanding the source and purpose of the client's funds and taking enhanced due diligence measures based on the risk status for circumstances that present a high risk of money laundering or terrorist financing;

4. carrying out ongoing due diligence on the client throughout the lifecycle of the business relationship, reviewing and examining the client's status and transaction profile so as to confirm that the various services and transactions provided to the client are consistent with the financial institution's understanding of the client's identity and background, business needs, risk status, as well as the source and purpose of the client's funds; and

5. determining and taking reasonable measures to verify the beneficial owner of the client if the client is a legal person or unincorporated organization.

The financial institution should determine the extent and specific methods of due diligence measures based on the differentiation of risk status and should not take due diligence measures that are obviously inconsistent with the risk status, so as to achieve a balance between risk prevention and service optimization.

To fulfill these requirements, financial institutions should establish a classified client due diligence working mechanism and proceed to work in a step-by-step approach. For instance, financial institutions can (a) verify the ID cards of individual clients from direct sales channels via the systems of E-Capital Transfer Co. Ltd and GZT Technology Co., Ltd.; (b) verify the identities of institutional clients from direct sales channels through websites such as the National Enterprise Credit Information Publicity System (国家企业信用信息公示系统); (c) analyze the purpose of clients' transactions through questionnaires in conjunction with reviews on clients' identity; (d) conduct continuous screening by establishing a suspicious transaction monitoring model, and conduct manual screening of suspicious transactions in conjunction with reviews of clients' historical transaction information; and (e) create a document list requesting the clients to provide articles of association and relevant supporting documents, etc.

II Formulating working mechanism for ex-post identity verification

According to Article 25 of the 2022 Measures, financial institutions must verify the identity of a client and its beneficial owner at the time of establishing a business relationship or processing a one-time transaction. Under the circumstance of effective management of money laundering and terrorist financing risks, for a normal transaction which is difficult to be interrupted, the financial institution may

complete the verification of the identity of the client and its beneficial owner as soon as possible after establishing a business relationship. Where a financial institution handles any businesses for the client before completing the verification on the identities of the client and its beneficial owner, it is required to take appropriate risk management measures.

In respect of financial institutions, the ex-post identity verification could improve the efficiency of daily business activities. In other words, for normal transactions that are difficult to interrupt, ID card verification could be completed at the end of each day in a joint manner and the identity verification via the systems of E-Capital Transfer Co. Ltd, GZT Technology Co., Ltd. and through websites such as the National Enterprise Credit Information Publicity System could be conditionally delayed as appropriate. However, financial institutions should establish risk management measures for the ex-post identity verification, such as restrictions on subsequent transactions in the event of incorrect identity verification, blacklist screening mismatches and other circumstances, cancellation of trading qualifications with ex-post identity verification and other related measures, etc.

III Formulating systems for enhanced due diligence measures

According to Article 29 of the 2022 Measures, at the time of establishing a business relationship with a client or throughout the lifecycle of such business relationship, financial institutions should comprehensively take into account the client's characteristics, business relationship, nature and purpose of the transaction, source and purpose of funds and other factors. Enhanced due diligence measures should be adopted based on risk status where the client presents a high risk for money laundering or terrorist financing, or the client is a person investigated or announced by national judicial organs, law enforcement and supervisory authorities for suspected money laundering, terrorist financing and related crimes.

According to Article 30 of the 2022 Measures, for clients with high risk for money laundering or terrorist financing and other high-risk clients, financial institutions should adopt one or a combination of the following enhanced due diligence measures corresponding to the perceived risk status:

1. obtaining the relevant information regarding the business relationship, purpose and nature of transactions and source and purpose of funds, and requiring clients to provide supporting materials for verification where necessary;
2. understanding the clients' economic status or business status through onsite inspections, etc.;
3. strengthening monitoring and analysis of clients and their transactions;
4. increasing the frequency of information review and update of clients and their beneficial owners; and
5. obtaining approval from senior management for the establishment and maintenance of business relationships with clients or the handling of business for clients.

Upon adoption of enhanced due diligence measures, where a financial institution deems that there is a need to carry out risk management for money laundering or terrorist financing risks of its clients, it should implement reasonable restrictions on the mode, scale, frequency, etc. of the clients' transactions; where the financial institution deems that the money laundering or terrorist financing risks

of the clients exceed the risk management capacity of the financial institution, it must refuse the transaction or terminate the established business relationship.

Financial institutions should further refine the specific conditions applicable to clients subject to enhanced due diligence measures mentioned in the 2022 Measures, i.e., those applicable to "persons with high risk for money laundering or terrorist financing", "persons investigated by the national judicial organs, law enforcement and supervisory authorities for suspected money laundering, terrorist financing and related crimes" or "persons announced by the national judicial organs, law enforcement and supervisory authorities for suspected money laundering, terrorist financing and related crimes".

In light of the above, it is advisable for a financial institution to establish a full set of evaluation systems and working plans to assess the clients' risk profiles for AML and counter-terrorist financing after adopting enhanced due diligence measures, and to standardize the multi-level restrictive measures over the clients' business activities under different risk scenarios.

IV Establishing the simplified due diligence measures system

According to Article 31 of the 2022 Measures, a financial institution may adopt the corresponding simplified due diligence measures where the financial institution determines a low risk of money laundering or terrorist financing for certain types of clients, business relationships or transactions upon assessment and with adequate reasons, by referring to the following information while taking into account the client's characteristics and the purpose and nature of the business relationship or transactions:

1. national money laundering risk assessment reports;
2. relevant provisions and guidelines on AML, counter-terrorist financing and account management, risk warnings, analysis reports on money laundering types and risk assessment reports promulgated by PBoC; and
3. other relevant provisions stipulated by laws and administrative regulations.

When adopting simplified due diligence measures, financial institutions should at least determine and verify the identity of the client, register the client's name, contact information, and the type, number and validity period of his/her valid ID card or other identity documents, and retain the identity materials as necessary for the client due diligence. For clients, business relationships or transactions for which simplified due diligence measures are adopted, the financial institution should examine their risk status on a regular basis and adjust the scope of services and business functions provided based on their risk levels. Financial institutions may not adopt simplified due diligence measures where any clients, business relationships or transactions are suspected of money laundering or terrorist financing or are considered of high risk.

The creation of simplified due diligence measures aims to reduce the burdens on financial institutions and other financial institutions in carrying out daily AML work. Financial institutions should establish a classified AML management program for clients accordingly. Given that financial institutions retain certain discretion in adopting simplified due diligence measures, corresponding assessment standards

and subsequent identification and review methods for simplified due diligence could be established accordingly. At the same time, this provision poses a challenge for financial institutions to apply simplified due diligence measures in the future due to the developing working mechanism for financial institutions to carry out classified client identification in fulfilling their due diligence obligations.

V Sorting out third-party cooperation mechanisms

According to Article 39 of the 2022 Measures, the third parties are required to perform the corresponding client due diligence obligations in strict accordance with laws and contractual agreements, and must provide necessary client identity information to the financial institution; where the financial institution has any doubts as to the authenticity, accuracy or completeness of a client's identity information, or suspects that a client is involved in money laundering or terrorist financing activities, the third party must cooperate with the financial institution in client conducting due diligence. Third parties are subject to liability for failure to cooperate with financial institutions in performing client due diligence obligations.

In the current AML work of FMCs, there are common problems within the industry such as incomplete client information from distribution channels, the urgent need to supplement and improve the information of existing clients and the slow progress of the system upgrades due to monopolies by individual suppliers of core FMC systems. As for the incompleteness of client information from distribution channels, the limited available approach for FMCs is to cooperate with distributors on optimizing the method of client information provision through active communications. With respect to the problem with urgent need to be solved within the industry, i.e., "ineffective clients' basic identity information verification and client risk classification due to poor transmission mechanisms for client information through distribution channels", the 2022 Measures add that "if the third party fails to cooperate with the financial institution in performing client due diligence obligations, it should assume the corresponding liabilities". FMCs may review the agreements, system interfaces and daily business cooperation arrangements with the distributors to proceed more smoothly with work in the future.

VI Client due diligence checks

According to Article 51 of the 2022 Measures, for existing clients with whom a financial institution has established a business relationship or conducted transactions prior to the implementation of the 2022 Measures without meeting the relevant due diligence requirements, the financial institution must complete the due diligence on those existing clients with a relatively high-risk level or above within one year from the implementation date of the 2022 Measures and complete the due diligence on all existing clients within two years from the implementation date of the 2022 Measures.

Therefore, financial institutions should conduct classified client management, determine client risk levels accordingly and arrange step-by-step due diligence planning for existing clients with different risk levels. This due diligence of all existing clients should be completed by 1 March 2024.

Comparison Table between the 2007 Measures and the 2022 Measures

Please click here to open the comparison table between the 2007 Measures and the 2022 Measures.

Important Announcement

This Newsletter has been prepared for clients and professional associates of Han Kun Law Offices. Whilst every effort has been made to ensure accuracy, no responsibility can be accepted for errors and omissions, however caused. The information contained in this publication should not be relied on as legal advice and should not be regarded as a substitute for detailed advice in individual cases.

If you have any questions regarding this publication, please contact:

Beijing	**Wenyu JIN**	**Attorney-at-law**
	Tel:	+86 10 8525 5557
	Email:	wenyu.jin@hankunlaw.com
Shanghai	**Yinshi CAO**	**Attorney-at-law**
	Tel:	+86 21 6080 0980
	Email:	yinshi.cao@hankunlaw.com
Shenzhen	**Jason WANG**	**Attorney-at-law**
	Tel:	+86 755 3680 6518
	Email:	jason.wang@hankunlaw.com
Hong Kong	**Dafei CHEN**	**Attorney-at-law**
	Tel:	+852 2820 5616
	Email:	dafei.chen@hankunlaw.com