22 April 2024

National Financial Regulatory Administration
Jia No.15 Financial Street
Xi Cheng District
Beijing 100033

To the National Financial Regulatory Administration

Administrative Measures Data Security of Banking and Insurance Institutions (Consultation Draft)

On behalf of its members, the Asia Securities Industry & Financial Markets Association ("**ASIFMA**")[1] ("**we**", "**our**" or "**us**") are pleased to submit this letter to the National Financial Regulatory Administration ("**NFRA**"). We seek to convey industry's views on the *Administrative Measures for Data Security of Banking and Insurance Institutions (Consultation Draft) (《银行保险机构数据安全管理办法》(征求意见稿))* ("**Draft Measures**"), and offer constructive ideas on how the Draft Measures can be refined to encourage foreign investment into the People's Republic of China ("**PRC**" or "**China**"), enhance risk management and facilitate compliance by market participants with robust standards and obligations aligned with those of other jurisdictions that are considered integral to world markets.

Our detailed considerations and suggestions in relation to the Draft Measures are highlighted in the schedule to this letter. We very much appreciate the opportunity to respond to the Draft Measures and look forward to engaging in further communication with the NFRA and any other relevant bodies as may be helpful.

[1] ASIFMA is an independent, regional trade association with over 160 member firms comprising a diverse range of leading FIs from both the buy and sell side, including banks, asset managers, law firms, and market infrastructure service providers. Together, we harness the shared interests of the financial industry to promote the development of liquid, deep, and broad capital markets in Asia. ASIFMA advocates stable, innovative, competitive, and efficient Asian capital markets that are necessary to support the region's economic growth. We drive consensus, advocate solutions and effect change around key issues through the collective strength and clarity of one industry voice. Our many initiatives include consultations with regulators and exchanges, development of uniform industry standards, advocacy for enhanced markets through policy papers, and lowering the cost of doing business in the region. Through the GFMA alliance with SIFMA in the United States and AFME in Europe, ASIFMA also provides insights on global best practices and standards to benefit the region.

ASIFMA - Unit 3603, Tower 2 Lippo Centre
89 Queensway Admiralty, Hong Kong

Should you have any questions in relation to this letter or would like to obtain further industry input, please contact Diana Parusheva, Managing Director at ASIFMA, Head of Public Policy and Sustainable Finance at dparusheva@asifma.org.

In the meantime, to facilitate dialogue, we will also share a copy of our submission with [the People's Bank of China ("**PBOC**"), the China Security Regulatory Commission ("**CSRC**"), and the Cybersecurity Administration of China ("**CAC**")], given the potential overlapping areas of regulation.

This submission was prepared with the assistance of the law firm Fangda Partners, based on feedback from the wider ASIFMA membership.

Yours faithfully

Diana Parusheva

Managing Director

Head of Public Policy and Sustainable Finance

Asia Securities Industry & Financial Markets Association (ASIFMA)

www.asifma.org

Schedule – ASIFMA Comments and Suggestions

1. Scope of Application

(1) Imposing uniform requirements across a wide range of institutions without considering business size and characteristics as appropriate

Article 2 outlines the scope of application, which encompasses a wide range of institutions, including not only large financial institutions such as commercial banks and insurance companies, but also smaller-scale institutions like financial leasing companies, auto finance companies, consumer finance companies, money brokers and wealth management companies.

Article 80 of the Draft Measures provides that it shall apply by reference to branches of foreign banks, other financial institutions, and financial holding companies that are established upon approval by the NFRA as well as the agencies subject to the administration of the NFRA. The Draft Measures shall apply by reference to financial organizations established upon approval by local financial regulatory authorities. However, it lacks clarity on what constitutes "by reference," leading to confusion among affected entities.

Further, throughout the Draft Measures, numerous obligations are stipulated, primarily targeting "banking and insurance institutions." Nevertheless, the term lacks a clear definition. We are also aware that under different existing NFRA rules, the scope of institutions this term covers may be different.

While ensuring comprehensive coverage of the Draft Measures is essential, we kindly request the NFRA to consider the potential implications for various types of financial institutions. For example:

- Following several previous data security rules targeting banks and/or insurance companies, such as the *Guidelines for Data Governance of Banking Financial Institutions (《银行业金融机构数据治理指引》,* "**NFRA Banking Data Governance Guidelines**"*),* the *Regulatory Measures on the Information Technology Outsourcing Risks of Banking and Insurance Institutions (《银行保险机构信息科技外包风险监管办法》)* and the *Risk Management Guidelines for Third-Party of Banking Financial Institutions (《银行业金融机构外包风险管理指引》)* (the foregoing two rules, "**NFRA Banking IT TPRM Guidelines***"*), many large commercial banks may have gradually established comprehensive information technology systems and data security management policies. For these banks, the requirements under the Draft Measures represent further refinement and improvement. However, for smaller institutions that have not been required to fully implement past rules, the requirements under the Draft Measures imply starting from scratch, possibly even overturning many existing operational practices, which could burden them excessively.
- The Draft Measures appear to include certain existing regulatory mechanisms that are applicable only to large institutions. For example, Articles 26 and 31 refer to information technology outsourcing management exclusive to banks and certain other institutions. However, these existing provisions do not extend to other institutions, potentially rendering them unable to comply with such requirements under the Draft Measures.

- Furthermore, for some institutions that heavily rely on group support, such as foreign bank branches, fully implementing the Draft Measures would impose a significant burden. They may lack the authority and resources to establish the full set of governance bodies as specified in Chapter II, develop a data asset inventory as required by Article 21, build a data “firewall” between their parent banks as required by Article 29, and fully comply with other provisions regarding data management under the Draft Measures.
- Many foreign-invested institutions primarily engage in wholesale business, and even when they serve individual clients, their overall client base is significantly smaller. For them, the resources required to meet all stringent compliance standards far outweigh their business scale.

ASIFMA Suggestions:

In light of the above, we sincerely hope the NFRA may consider:

- Under Article 2,
  - Clearly defining "banking and insurance institutions" to encompass large financial entities only, such as commercial banks and insurance companies; and
  - Excluding entities with a small-scale client base or those exclusively serving institutional clients from the scope of application of the Draft Measures; alternatively, NFRA can create a de minimis standard or business scenario-based carve-outs.
- Regarding Article 31,
  - It is recommended that the scope of data entrusted processing under information technology outsourcing management should be consistent with the NFRA Banking IT TPRM Guidelines.
- Regarding Article 80,
  - Removing this entire article, ideally, or
  - Clarifying other institutions (including foreign bank branches) may reference the Draft Measures based on their specific circumstances.
- Alternatively, considering the implementation of differentiated compliance requirements tailored to the size and type of institution across the Draft Measures.

(2) Dual oversight by multiple financial regulators may confuse institutions seeking to comply

Depending on the specific types and businesses, the data management of institutions covered by the Draft Measures may also be regulated by other financial regulators, such as the PBOC and the CSRC. It is inevitable that the requirements of different regulators may overlap or even conflict, which presents a significant challenge in determining how to apply these sets of rules.

For example, the PBOC has issued several rules and standards regarding data security management that may be applicable to the institutions subject to the Draft Measures,

including the *Draft Measures for the Management of Data Security in People's Bank of China Business Areas (《中国人民银行业务领域数据安全管理办法（征求意见稿）》,* "**PBOC Draft Measures**"*)*, the *Guidelines for Financial Data Security - Data Security Grading" (《金融数据安全 数据安全分级指南》, JR/T 0197-2020)*, the *Technical Specifications for Personal Financial Information Protection (《个人金融信息保护技术规范》, JR/T0171-2020), Security Specifications for the Data Lifecycle of Financial Data Security (《金融数据安全数据生命周期安全规范》, JR/T 0223-2021).* In particular, the PBOC Draft Measures base their applicability on whether institutions engage in "PBOC business areas" activities such as anti-money laundering activities, cross-border RMB activities, interbank market transactions, comprehensive financial statistics, payment and clearing, and credit activities. These activities also cover typical business scenarios of NFRA-regulated institutions as well.

ASIFMA suggestions:

To address these conflicts and streamline compliance efforts, we recommend that the NFRA to

- Coordinate with other financial regulators, in particular the PBOC, to harmonize the different sets of rules and standards on data security management;
- Clearly address that if there is any inconsistency in the requirements of various regulators, the standards and regulations of a certain financial regulator shall be used as the benchmark;
- Provide clear guidance on whether rules and standards issued by the NFRA or the PBOC take precedence in cases of overlap; or alternatively,
- Grant institutions flexibility to choose the applicable rules and standards based on their specific circumstances.

2. Data Classification and Grading Rules

(1) New and multiple classification and grading requirements result in heavy operational burden

There are discrepancies between the data classification grading approaches outlined in the Draft Measures and those presented in rules issued by other relevant regulators. In particular, within the "core data, important data and general data" framework, the Draft Measures introduce a distinct subcategory "sensitive data" within the general data. To contrast, for example, the PBOC Draft Measures classify data as core data, important data, and general data, with further classification levels ranging from 1 to 5 based on specific criteria. Other regulatory documents concerning data classification and grading include the *Technical Rules for Data Security - Data Classification and Grading (Draft) (《数据安全技术 数据分类分级规则(报批稿)》*, GB/T 43697-2024) as well as the PBOC standards mentioned under Section 1 (2).

On one hand, it is encouraging that compared with the PBOC Draft Measures, the Draft Measures' requirements are more in line with global practice to require only one set of rules for data grading based on importance and sensitivity. On the other hand, the existence of multiple classification and grading methods and standards for the same financial activity,

such as anti-money laundering, creates confusion and implementation challenges for institutions, hindering the efficient implementation of data security management requirements.

ASIFMA Suggestions:

It is recommended that the NFRA considers:

- Collaborating with the PBOC and other industry standard-setting organizations to establish a unified data classification and grading framework for financial institutions; or
- Providing clear guidance on whether rules and standards issued by the NFRA and other regulators take precedence in cases of overlap; or alternatively,
- Granting institutions flexibility to choose the applicable rules and standards based on their specific circumstances.

(2) Challenges in Enforcing Compliance Obligations Related to Sensitive Data

The Draft Measures impose numerous additional data security management obligations specifically targeting sensitive level data or above. These obligations are outlined in Articles 22, 27, 28, 29, 34, 35, 37, 40, 41, 42, 43, 44, 45, 46, 48, 65 (IV), and 73. Considering the potentially large volume of sensitive data, these obligations have the potential to impose significant burdens on institutions.

For example:

- The Draft Measures require conducting a data security assessment prior to processing activities involving sensitive level data or above. This requirement differs from Article 30 of the *Data Security Law*, which only mandates periodic risk assessments for important data processing activities.
- Article 29 of the draft introduces authorization requirements for sharing sensitive level data within a corporate group. As sensitive data may encompass more types of data in addition to personal data, such as corporate client data, obtaining consent for all sensitive data would impose a substantially greater burden compared to the requirements under the *Personal Information Protection Law*.

ASIFMA Suggestions:

ASIFMA suggests that the NFRA:

- Consider adjusting the obligations in the Draft Measures concerning sensitive level data or above to specifically apply to important level data or above.
- Alternatively, consider clarifying that the existing obligations related to sensitive level data or above are not mandatory in nature, enabling institutions to evaluate their specific circumstances and determine whether to implement them accordingly.
- If the Draft Measures maintain the existing version, it is advisable to grant a grace period for institutions to implement the changes, taking into account the complexity and

resource requirements involved.

(3) Grading standards require further clarification

Article 18 provides broad definitions of core data, important data, and sensitive data. Further, according to Article 71, the NFRA will:

- formulate a catalogue of important data for the banking and insurance industry, and
- make suggestions for the catalogue of core data.

Meanwhile, other than a broad definition of sensitive data under Article 18, the Draft Measures remains silent on what constitutes sensitive data. The broad definition of sensitive data in the Draft Measures, coupled with the absence of a specific catalogue, poses challenges for institutions in accurately grading data.

Given the critical importance of these three levels of data for institutions in implementing the draft measures, we hope that the NFRA can provide more specific guidance for each level of data.

ASIFMA Suggestions:

- Sensitive data

  If the Draft Measures maintain the concept of sensitive data and associate it with various obligations, it is crucial to establish a clearer and more precise explanation or a specific catalogue of sensitive data. Furthermore, it is recommended to define the scope of sensitive data within the scope of "sensitive personal information" rather than expanding the scope of "sensitive data" to include data related to "organizations". This step is crucial to facilitate the smooth implementation of the Draft Measures by institutions.

- Important data

  The distinction between classifying data that may directly endanger national security (important data) and data that can significantly impact key areas of national security (core data) lacks clarity. Clearer guidance and clarification are recommended.

- Core data

  - It is recommended that the definition of "core data" be consistent with the definition of "core data" in the *Data Security Law*, that is, to be revised to "... once tampered with, destroyed, leaked or illegally obtained or illegally used, it may directly endanger national security, the lifeline of the national economy, important people's livelihood, major public interests, and other data", so as to avoid identification difficulties in practice.
  - It is recommended to clarify how the suggestions for the catalogue of core data would be given specifically, if being different from "formulation a catalogue".

- When providing guidance and formulating data catalogues for different data grades, it is advisable to consider the business scale of each financial institution and the international attributes of foreign-invested institutions.

3. Clarify the Specific NFRA Data Export Security Assessment Process

Article 36 stipulates that where a banking or insurance institution provides overseas parties with important data and personal information collected and generated through its business and operation within the territory of the PRC, it shall assume the primary responsibility for data security and conduct security assessment in accordance with the relevant national policies.

This provision remains too vague, as it does not clarify whether the NFRA is responsible for executing the data export security assessment for financial institutions, as well as the specific standards and procedures for implementation.

According to Article 2 of the *Provisions on Promoting and Regulating the Cross-Border Data Flows (《促进和规范数据跨境流动规定》)* issued by the CAC, which just came into effect on March 22, 2024, data processors do not need to undergo a data export security assessment if the data has not been informed or publicly disclosed by relevant departments or regions as important data.

In recent years, although the *Cyber Security Law* and the *Data Security Law* have mandated the requirement of data export security assessment for important data, the specific implementation mechanisms have not been fully established. Consequently, institutions struggle to clearly understand and comply with this regulatory requirement, leading to significant uncertainties in normal business operations. Our members are encouraged by the recent implementation of the CAC provisions, as it provides clearer guidance for foreign-invested institutions on understanding the data export security assessment of important data. Therefore, it is essential to pay closer attention to regulations set by industry regulators authorities, and regions.

Based on this, we hope that the NFRA will provide clearer mechanisms from the perspective of industry regulators for determining the applicability of the NFRA data export security assessment requirements in the Draft Measures.

ASIFMA Suggestions:

NFRA to consider:

- Clarifying that, either through a separate notice or in the Draft Measures, since the implementation of the Draft Measures, institutions regulated by the NFRA (regardless of whether they fall under the scope of application or not) do not need to submit a data export security assessment to the NFRA for data that has not been informed or publicly disclosed by the NFRA as important data.

- Explicitly outlining in the Draft Measures that if institutions regulated by the NFRA need to conduct the data export of important data, they should complete the NFRA's data export security assessment process. Additionally, provides specific guidelines on the data export security assessment of important data.

4. Alignment with other NFRA rules

We have noticed that some provisions in the Draft Measures overlap with existing NFRA rules concerning data security and third-party risk management such as the aforementioned NFRA Banking Data Governance Guidelines and the NFRA Banking IT TPRM Guidelines, but they are not entirely consistent. The Draft Measures do not specify whether the aforementioned rules will be invalidated upon the effectiveness of the new regulations, or how they will be applied in case of conflicts.

For example:

- Both the Draft Measures and the NFRA Banking Data Governance Guidelines involve requirements for data governance architecture. While the overall framework may be similar, there are still differences in specific details and responsibilities, such as the specific duties of the centralized management department for data security.
- Article 73 of the Draft Measures and the NFRA Banking IT TPRM Guidelines both include regulatory reporting requirements for specific entrusted data processing activities. We are unsure whether these reports can be consolidated for the same entrusted data processing activity or if they must be completed separately.
- Article 66 of the Draft Measures mandates an annual data security risk assessment, while Article 27 of the NFRA Banking Data Governance Guidelines also requires institutions to conduct an annual data governance assessment covering data security. We are unsure whether these assessments can be consolidated or if they must be completed separately.

Furthermore, the *Measures for Data Security of Banking and Insurance Institutions (《银行保险机构数据安全办法》)* mentioned in Article 81 of the Draft Measures have not been publicly released. Some institutions that have not received this document, or foreign-invested institutions planning to enter the Chinese market, may struggle to compare and understand the connection and differences between this regulation and the new rules.

ASIFMA Suggestions:

We earnestly request the NFRA to:

- Clearly specify that upon the effectiveness of the Draft Measures, relevant provisions in existing rules such as the NFRA Banking Data Governance Guidelines and the NFRA Banking IT TPRM Guidelines should be nullified, or prioritize the application of the Draft Measures in case of conflicts.
- Consider consolidating or nullifying original provisions related to similar reporting obligations and data security risk assessment reporting requirements, or explicitly state that redundant reporting is unnecessary.
- Publicly disclosing the *Measures for Data Security of Banking and Insurance Institutions* to facilitate broader understanding and learning among market institutions.

5. Grace period to provide sufficient time for FIs' implementation of the Draft Measures

The implementation of the Draft Measures is expected to have a significant impact on the relevant institutions and other data processors within the specified application scope.

We kindly urge the NFRA to consider instituting a reasonable grace period for compliance with the requirements outlined in the Draft Measures. This would provide the affected institutions and data processors with adequate time to adapt their data processing practices appropriately.

ASIFMA Suggestions:

In regard to Article 81, we suggest:

- Introduction of a grace period arrangement. For instance, a two-year grace period similar to that provided upon the launch of the European Union's General Data Protection Regulation – if two year is not possible, at least a seven-month period similar to that of Cyber Security Law of China.
- Granting different periods based on the varying types and scales of institutions to ensure fairness and facilitate a seamless transition to compliance.

6. Other Suggestions on Specific Articles

In addition to the comments raised in Sections 1-6, we set forth in the table below our comments and suggestions with respect to specific articles of the Draft Measures.

Article No.	Content under the Draft Measures	ASIFMA Comments	ASIFMA Suggestions
2, 80	Article 2 (Scope of Application) Article 80 (Reference Implementation)	• Please refer to our comments under Section 1.	\
3	Article 3 (Definition of Terms) … "data processing (处理)" refers to such activities as collection, storage, use, processing (加工), transmission, provision, sharing, transfer, disclosure, deletion and destruction of data.	• "data processing": The definition of "data processing" in the Draft Measures does not align with the definition provided in the *Data Security Law*. Specifically, the inclusion of "deletion and destruction" within the definition of data processing in the Draft Measures differs from the *Data Security Law*. Including "deletion and destruction" within the definition of "data processing" could potentially lead to semantic confusion. For example, "ceasing data processing" under Article 25 may be inappropriate if data processing includes deletion and destruction.	• "data processing": Consider keeping the definition of "data processing" consistent with that in the *Data Security Law* and revising it as below: *"data processing" refers to such activities as collection, storage, use, processing, transmission, provision, sharing, transfer, and disclosure of data.*
	… "data subjects" refers to natural persons or their guardians, enterprises, government agencies, public institutions, social groups, and other organizations identified by data.	• "data subjects": There are types of information which may not always allow for the identification of the "data subject". The Draft Measures include numerous requirements regarding "notifying the data subject" and "obtaining the consent of the data subject." However, in situations where the "data subject" cannot be	• "data subjects": It is recommended to define "data subject" within the scope of personal information.

Article No.	Content under the Draft Measures	ASIFMA Comments	ASIFMA Suggestions
	… "personal information" refers to all information relating to an identified or identifiable natural person recorded electronically or otherwise, excluding the information processed anonymously.	identified, practical challenges may arise. • "personal information": Special provisions are suggested to be made for the processing of personal information collected by institutions in the course of conducting corporate business and certain specific financial businesses (for example, personal information attached to underlying assets received during due diligence on asset securitization of non-performing loans).	• "personal information": the NFRA to consider including the following provisions: "personal information" refers to all information relating to an identified or identifiable natural person recorded electronically or otherwise, excluding the information processed anonymously *and:* *(i) Business contact information, such as an individual's name, title or position, business contact number, business address, business email, business fax number, and similar information; and* *(ii) Personal information involved in due diligence on packaging assets in financial business.*"
10	Article 10 (Data Security Responsibility System) Banking and insurance institutions shall establish a data security responsibility and accountability system, under which its Party committee and the board of directors shall assume the primary responsibility for the intuition's data security. The principal is the first person chiefly responsible for data security, and the leader in charge of data security is the person directly responsible in this regard. The responsibilities of the person-in-charge at each level shall be clarified, the circumstances of violations and accountability matters shall be specified, and the accountability and disposal mechanism shall be implemented.	• The term "leader" appears to be unclear. • According to Article 80, the Draft Measures shall apply by reference to foreign bank branches. Due to local experience, setting up a Party Committee is NOT a mandatory practice for foreign bank branches in mainland China. Instead, a local management committee would usually be set up to resume the function. • There is no clear indication whether the data security leader (officer) needs to sit within the regulated legal entity/foreign bank branch. In practice, many foreign	• NFRA to consider replacing the term "leader" with a more specific term, such as "senior management". • We would require NFRA to add in Article 10 the wording "or equivalent internal management committee" in addition to the Party committee, Board of Directors, to resume the main responsibility for the institution's data security. • We would suggest that the NFRA allows foreign bank branches the flexibility to designate internal staff or engage personnel from either domestic or foreign affiliates for

Article No.	Content under the Draft Measures	ASIFMA Comments	ASIFMA Suggestions
		bank branches follow global or regional best practices for data security management. Granting this flexibility would enable foreign bank branches to leverage their established practices and ensure effective data security management.	the position of data security leader (officer).
11	Article 11 (Centralized Management Department for Data Security) (数据安全归口管理部门) Banking and insurance institutions shall designate a centralized management department for data security as its primary department responsible for data security, with main responsibilities as follows: …	• The functions of data security are collaboratively undertaken and executed by various functional departments within an organization. It is challenging for a single department to solely assume the overall responsibility for data security.	• It is advisable to provide institutions with a certain level of flexibility by modifying the term "centralized management department" to "centralized management department, steering group, or internal management committee (归口管理部门、领导小组或内部管理委员会)".
14	Article 14 (Data Security Technology Protection Function) The data security technology protection function shall undertake the primary responsibility for the technical protection of data security, with main responsibilities as follows:…	• In the case of an onshore bank branch, there is no clear indication regarding whether the data security technology protection function should be set up within the onshore foreign bank branch. In practice, from best practice and cost efficiency perspectives, many foreign bank branches leverage global/regional resources to realize technology function, while remaining one IT officer seating within the branch.	• We would suggest that the NFRA allows flexibility for a foreign bank branch to decide by itself whether its security technology protection function needs to set up within the foreign branch or needs to be onshore.
16	Article 16 (General Requirements) Banking and insurance institutions shall formulate a data classification and grading protection policy, establish data catalog and classification and grading specifications,	• In addition to our comments regarding grading standards under Section 3, it's unclear if the NFRA will be issuing classification guidelines or institutions will be allowed to determine this based on	• NFRA to consider clarifying if it will be issuing classification guidelines or institutions will be allowed to determine this based on their internal criteria.

Article No.	Content under the Draft Measures	ASIFMA Comments	ASIFMA Suggestions
	dynamically manage and maintain data catalogs, and adopt differentiated security protection measures.	their internal criteria.	
Chapter III	Chapter III Data Classification and Grading	• Please refer to our comments under Section 2.	\
20	Article 20 (Management System) … Banking and insurance institutions shall formulate implementing policies for security management with respect to external input of data, cooperation to co-share and data outbound transfer.	• The terms external bringing-in (外部引入)" and " cooperation to co-share (合作共享)" are not clear.	• NFRA to consider clarifying "external bringing-in (外部引入)" and " cooperation to co-share (合作共享)".
22	Article 22 (Assessment of Data Security) When processing business activities with data at the sensitive level or above or carrying out activities with greater impact on data subjects such as data entrusted processing, joint processing, transfer, publicity, and sharing, a banking or insurance institution shall carry out prior data security assessment. Data security assessment shall, based on the purpose, nature, and scope of data processing and in accordance with laws, regulations, and ethical requirements, analyze data security risks and the impact on the rights and interests of data subjects, assess the necessity and compliance, and evaluate data security risks and the effectiveness of prevention and control measures.	• As mentioned under Section 2(2), the requirement of conducting a data security assessment prior to processing activities involving sensitive level data or above may impose a substantial burden on institutions. This requirement differs from Article 30 of the *Data Security Law*, which only mandates periodic risk assessments for important data processing activities. • At first glance, there is a potential for misinterpreting the term "Assessment of Data Security" in this context as referring to the requirement of submitting a data export security assessment to regulatory authorities.	• NFRA to consider adjusting the obligations in the Draft Measures concerning sensitive level data or above, including the assessment of data security under Article 22, to specifically apply to important level data or above. • Clarify that the assessment of data security is just an internal security assessment within the organization.
23	Article 23 (Management of Data Services)	• According to Article 23, institutions shall	• We suggest the NFRA allows foreign-

Article No.	Content under the Draft Measures	ASIFMA Comments	ASIFMA Suggestions
	Banking and insurance institutions shall establish an enterprise-level data service management system, formulate data service specifications, build a full-time data service team, coordinate internal and external data processing and analysis, and implement demand analysis, service development, service deployment, service monitoring and other activities for data services.	establish an enterprise-level data service management system, build a full-time data service team, etc. In practice, many foreign-invested institutions have already set up their global-level Enterprise Data Governance Management framework to comply with data requirements in variety of jurisdictions.	invested institutions to follow the existing global practice and leverage the current mechanism.
24	Article 24 (Data Collection) Banking and insurance institutions shall uphold the principles of "legality, legitimacy, necessity and good faith" for data collection, specify the purpose, method, scope, and rules of data collection and processing, and ensure the data security and traceability of data sources in the collection process. A banking or insurance institution shall not collect data from data subjects beyond the scope of consent, unless otherwise stipulated by laws and regulations.	• The Draft Measures cover corporate data and personal information. Therefore, according to this article, corporate data collection requires the consent of the data subject, except where otherwise provided by laws and regulations. At law level, the requirement to obtain consent from the data subject only appears in the *Personal Information Protection Law*. It would be burdensome to impose compliance obligations on institutions relating to collection of corporate data the same with personal information. Further, the other legal bases stipulated in Article 13 of the *Personal Information Protection Law*, such as "necessary for the conclusion and performance of a contract to which the individual is a party", are not mentioned, which will result in higher "authorization consent" execution requirements for corporate data processing than for personal information.	• NFRA to consider revising this article as follows: *"Banking and insurance institutions shall uphold the principles of "legality, legitimacy, necessity and good faith" for data collection, specify the purpose, method, scope, and rules of data collection and processing, and ensure the data security and traceability of data sources in the collection process. A banking or insurance institution shall not collect personal information from data subjects beyond the scope of consent, unless otherwise stipulated by laws and regulations."*
	The collection of industry data at or above the important level from other banking and	• This consent requirement appears to be burdensome in the case where cross-	• NFRA to consider not imposing this consent requirement, in particular when cross-border

Article No.	Content under the Draft Measures	ASIFMA Comments	ASIFMA Suggestions
	insurance institutions by a banking or insurance institution shall obtain consent from the NFRA.	border transfer of important data is not involved. Further, this consent appears to differ from the mechanism of data export security assessment. • It's unclear what constitutes "industry data at or above the important level"	transfer of important data is not involved. Additionally, NFRA to consider clarifying the specific mechanism of this consent and how it differs from data export security assessment. • NFRA to consider clarifying what constitutes "industry data at or above the important level", whether the NFRA will publish the industry-important levels and if this information is not public, how will we identify if the data is at or above the important level?
25	Article 25 (Data Collection) Banking and insurance institutions shall utilize information systems as the primary channel for data collection and restrict or reduce the collection of data from other channels and temporary data collection. Unless otherwise stipulated by laws and regulations, a banking or insurance institution shall, after ceasing financial business or services, forthwith cease relevant data collection or processing activities.	• We acknowledge the necessity of promptly halting data collection activities in this scenario. However, we believe that an immediate cessation of processing activities might be overly stringent and could impede institutions from fulfilling related compliance requirements, such as those concerning the retention period of business records. In addition, institutions may need to retain relevant data for litigation and other legitimate needs. • Additionally, while laws and administrative regulations are specified as exceptions, many departmental regulations, association rules, and specific requirements from regulatory authorities may also mandate institutions to retain business records for a certain period. Therefore, we recommend expanding the scope of exceptions appropriately to accommodate these scenarios.	NFRA to consider revising this article as follows: *"…Unless otherwise required by laws, regulations, or regulatory requirements or necessary for internal needs, a banking or insurance institution shall, after ceasing financial business or services, cease relevant data collection activities within a reasonable timeframe."*

Article No.	Content under the Draft Measures	ASIFMA Comments	ASIFMA Suggestions
26	Article 26 (External Data Procurement) Banking and insurance institutions shall formulate a centralized examination and approval management system for external data procurement and cooperative introduction, incorporate such system into its outsourcing risk management system for overall management, coordinate the establishment of a management mechanism for data demands, security assessment, collection and introduction, data operation and maintenance, registration, record-filing, and supervision and evaluation, investigate the authenticity and legality of data sources, assess the security guarantee capability of data providers and their data security risks, and specify the data security responsibilities and obligations of both parties.	• In practice, contracts commonly assign responsibility for verifying the authenticity and legality of data sources to data providers as the data recipients face practical challenges when tasked with investigating the authenticity and legality of the data. • Does "external data procurement" in this context exclusively pertain to client data? If institutions purchase integrated data, such as industry salary information from a consulting firm, does it still fall within the scope of external data procurement? Additionally, if institutions procure publicly available data, is it still necessary for the NFRA to manage it according to these requirements under this Article?	• NFRA to consider removing the requirement of investigating the authenticity and legality of the data. Alternatively, NFRA to consider amending this proposed mechanism into "dividing and constraining the responsibilities and duties of both parties through contractual arrangement". • Hopefully, the NFRA may clarify the scope of “external data procurement” and provide reasonable exceptions.
28, 30 and 43	\	• Should the “audit” referred in Articles 28, 30, and 43 means “log audit?	• NFRA to consider clarifying if “audit” referred in Articles 28, 30, and 43 should mean “log audit?
29	Article 29 (Data Sharing and Intra-group Sharing) …Banking and insurance institutions shall establish a "firewall" for data security isolation with its parent bank and insurance group or its parent company, subsidiaries, and branches, and take effective protection measures for shared data. Unless otherwise stipulated by laws and regulations, a banking or insurance institution intending to share the	• The term “firewall” appears to be unclear.	• NFRA to consider clarifying and expanding the definition of “firewall” to determine whether it refers solely to dedicated firewall devices or includes any control measures serving an isolating function.

Article No.	Content under the Draft Measures	ASIFMA Comments	ASIFMA Suggestions
	data at or above the sensitive level with its parent bank, group, or its branches or subsidiaries shall obtain the authorization and consent of the data subjects. Unless the data sharing is necessary for the provision of products or services, a banking or insurance institution shall not terminate or refuse the provision of financial services by a single branch or subsidiary on the ground that the data subjects refuse to consent to the sharing of sensitive data.		
29, 59, 60, 73	\	• The differences between the terms “sharing”, “transfer”, and “provisions to external parties” across several articles appear to be vague. • If data is stored in a third-party system due to the use of that system or its settings, does this arrangement fall under data sharing, transfer, or provision? If so, the associated compliance obligations may become unduly burdensome.	• We hope the NFRA may clarify the differences between the terms “sharing”, “transfer”, and “provisions to external parties”, or use consistent terminology provided no significant differences. • We hope the NFRA may clarify the data storage in a third-party system due to the use of that system or its settings does not constitute data sharing, transfer, or provision.
32	Article 32 (Co-processing of Data) When conducting joint data processing with a third party, a banking or insurance institution shall work out a plan under the principle of “authorization necessary for business” and take effective technical protection measures to ensure data security and shall specify the data security, responsibilities and obligations of both parties in the process of data processing in a contractual manner.	• The term “co-processing of data” appears to be unclear. Does it entail both parties jointly determining the processing objectives and methods, whereas "entrusted processing of data" suggests only one party making these decisions regarding the processing objectives and methods?	• NFRA to consider further clarifying “co-processing of data”.

Article No.	Content under the Draft Measures	ASIFMA Comments	ASIFMA Suggestions
34	Article 34 (Data Transfer) Unless otherwise stipulated by laws and regulations, where a banking or insurance institution provides external parties with data at or above the sensitive level, it shall obtain the consent of the data subjects. Except for the performance of duties by the State organs according to the law, the cross-subject flow of the core data of banking or insurance institutions shall pass the risk assessment and security review in accordance with the relevant national policies.	• It's unclear if "cross-subject flow of core data of banking and insurance institutions" is identical to "provides external parties with core data". If yes, suggest using consistent terminology. • It remains unclear how to complete the "risk assessment and security review in accordance with the relevant national policies". The term "national relevant policies" is too broad.	It is recommended to • Unify the terminology if "cross-subject flow of core data of banking and insurance institutions" and "provides external parties with core data" refer to the same activities. • Clarify the specific requirements and process of "risk assessment and security review in accordance with the relevant national policies".
36	Article 36 (Cross Border Data Transfer) Where a banking or insurance institution provides overseas parties with important data and personal information collected and generated through its business and operation within the territory of the PRC, it shall assume the primary responsibility for data security and conduct security assessment in accordance with the relevant national policies.	• Requirements to "assume the primary responsibility for data security and conduct security assessment" for cross border transfer of core data are not clarified here. • When it comes to cross border transfer of core data, it is unclear whether the security assessment requirement under this Article 36 and the "risk assessment and security review" requirement under Article 34 can be consolidated or if they must be completed separately.	• It is recommended to clarify the specific requirements to "assume the primary responsibility for data security and conduct security assessment", making sure no duplication or conflict with the assessment requirements stated in Article 34.
37	Article 37 (Data Backup) Banking and insurance institutions shall take technical measures to strengthen the focused protection of the data at or above the sensitive level. It shall strengthen data backup, formulate a backup strategy, isolate backup	• It may be unclear how to implement the "isolate" and "separate" requirements.	• It is suggested to specifically clarify the "isolate" and "separate" requirements.

Article No.	Content under the Draft Measures	ASIFMA Comments	ASIFMA Suggestions
	data from production data, keep backup data and production data separately, and strictly manage the access authority for backup data. It shall also have a backup verification plan to ensure that the backup data are complete and valid, and the business is recoverable.		
38	Article 38 (Data Deletion and Destruction) Banking and insurance institutions shall develop a data destruction management system and delete or anonymize data in accordance with the relevant national and industrial regulations and agreements with data subjects. When suspending the entrusted data processing, a banking or insurance institution shall require the service provider to promptly delete the data and take effective supervision measures such as on-site inspection to ensure that the data are destroyed and irrecoverable.	• In certain cases of outsourced data processing, banking and insurance institutions retain full ownership and control over the data. For example, when using a public cloud service, they have complete authority to delete or destroy the data in their cloud accounts after discontinuing the service. • Furthermore, "to promptly delete the data" may potentially violate existing provisions of laws, regulations and other regulatory requirements. For example, after data is promptly deleted, it may not be possible to meet the requirements of relevant laws and regulations for investigation and evidence collection.	• NFRA to consider revising this article as follows: *"Banking and insurance institutions shall develop a data destruction management system and delete or anonymize data in accordance with the relevant national and industrial regulations and agreements with data subjects. When suspending the entrusted data processing in the case that a banking and insurance institution does not have a direct control of the data, the banking or insurance institution shall require the service provider to promptly delete the data and take effective supervision measures such as on-site inspection to ensure that the data are destroyed and irrecoverable, except as otherwise provided by law, regulation, and regulatory requirements."*
41	**Article 41** (Protection of Cyber Security and Data Security) Banking and insurance institutions shall incorporate data into the multi-level protection scheme for cyber security. It shall, based on the grade of data security, divide network logical security domains, establish baselines for data security protection by region, implement effective security control, including	• It seems ambiguous regarding the implementation of the requirement to "incorporate data into the multi-level protection scheme for cyber security". Current multi-level protection scheme is conducted based on applications, and the assessment rules are made by relevant authorities.	It is suggested to specifically clarify • The requirement to "incorporate data into the multi-level protection scheme for cyber security". Whether it refers to adding a risk factor on applications security level with regard to protecting data? Since the multi-level protection scheme assessment rules are published by relevant authorities, it is suggested not to impose the requirements on

Article No.	Content under the Draft Measures	ASIFMA Comments	ASIFMA Suggestions
	content filtering, access control and security monitoring, etc., and ensure that the relevant measures meet the requirements of the cyber security policy and the data security protection policy for processing and storing the data at the highest level. Computer rooms and networks storing or transmitting data at or above the sensitive level shall be given priority in protection, and physical security protection areas shall be established to conduct security monitoring and auditing for network boundaries and important network nodes.	• Regarding the requirement to "based on the grade of data security, divide network logical security domains", is it a mandatory requirement to enforce logical isolation for data of different levels, or is it sufficient to meet the network security and data protection policy requirements for processing and storing data of the highest level?	financial institutions, but rather to suggest to relevant authorities to revise their assessment rules on multi-level protection schemes. • The requirement to "based on the grade of data security, divide network logical security domains".
42	Article 42 (Baseline of Data Security Protection – Protection of Information System) Banking and insurance institutions shall incorporate the data at or above the sensitive level into its information system for protection. It shall take effective access control management measures within the whole life cycle of data and implement security protection measures of the same level for the data circulated and shared in different areas. After the convergence and centralization of data from multiple sources at the sensitive level or above, security measures should be taken that are enhanced or not lower than the intensity of the data protection of the highest level before the convergence and concentration.	• We wonder whether "share folder (access control mechanism in place), cloud storage, local disk, and any other non-application based storage" could be included into the scope of "information system".	• We would like to get further clarification on the definition of "information system". Please further clarify whether "share folder (access control mechanism in place), cloud storage, local disk, and any other non-application based storage" could be included into the scope of "information system". If not, we would suggest that NFRA should allow foreign-invested institutions to self-prove that non-application based information storage is well under protection by complying with foreign-invested institutions existing internal data security governance mechanism.
43	Article 43 (Baseline of Data Security Protection – Data Access Control)	• The PBOC Draft Measures require a retention period of at least 3 years for all	• It is recommended that the NFRA collaborate with the PBOC to align the retention period

Article No.	Content under the Draft Measures	ASIFMA Comments	ASIFMA Suggestions
	Banking and insurance institutions shall strictly manage the data at the sensitive level or above, formulate strategies for users' access to data, take effective technical measures for user authentication and access control, and standardize data operations. Users' access to data shall meet the necessary requirements of business development and match the grade of data security. The operation on the data at or above the sensitive level shall be recorded in log, including the operation time, user ID, and type of behavior etc. The operation log and the backup data for core data shall be kept for not less than three years, the operation log and the backup data for important data and sensitive data shall be kept for not less than one year, and the operation log and the backup data for data involving entrusted processing or joint processing shall be kept for not less than three years. Data operation activities shall be audited on a regular basis with an audit cycle not exceeding six months.	different types of data records. We welcome the NFRA to shorten the record retention period for important and sensitive data to no less than 1 year. We would suggest that financial regulator's may align the relevant requirements with each other for record retention at different levels.	time, ensuring consistency with the approaches proposed in the Draft Measures.
47	Article 47 (Infrastructure for Data Security) Banking and insurance institutions shall carry out the construction of technical infrastructure for data security, support the componentization and service-orientation of user identity management, data anonymization, behavioral monitoring, log audit, data virtualization, and other functions, and ensure the consistency of the implementation of security standards in the information system.	• It seems ambiguous regarding the implementation of the requirement to support "data virtualization".	• Hopefully, the NFRA may clarify the specific requirements of data virtualization.
52	Article 52 (Data Processing)	• The specific requirements of "explanation"	• We would like to get further clarification on

Article No.	Content under the Draft Measures	ASIFMA Comments	ASIFMA Suggestions
	When using artificial intelligence technologies for business, a banking or insurance institution shall explain and disclose the impact of data on the decision-making results, monitor the results of automatic processing and system operation in real time, and establish risk mitigation measures for artificial intelligence applications, including developing alternative plans for exiting artificial intelligence applications, and develop incident plans for security threats and carry out drills.	and "information disclosure" regarding the impact of data on the decision-making results are unclear.	the scenarios for "explanation" and "information disclosure" regarding the impact of data on the decision-making results when foreign-invested institutions conduct AI technology related business. Should the "explanation" and "information disclosure" provide to related clients, regulators, or public?
Chapter 6	Chapter VI Personal Information Protection	• Since the *Personal Information Protection Law* and relevant regulations of the cyber security and informatization departments have already made very specific provisions on personal information protection, it is recommended that the relevant requirements should not be repeated in the Draft Measures to avoid inconsistencies, omissions, or failure to coordinate and adjust in a timely manner when other laws and regulations change. It is recommended that the Draft Measures focus on stipulating provisions for special circumstances of personal information processing activities of banking and insurance institutions.	• It is recommended that the Draft Measures refer to the *Personal Information Protection Law* and the regulations of the CAC, for example, "banking and insurance institutions should handle personal information in accordance with the provisions of the *Personal Information Protection Law* and relevant laws and regulations" instead of restating relevant provisions.
		• Further, for the individual information protection part, suggest differentiating the treatment of individual information obtained for personal business relationship and corporate business	• It is recommended to give full consideration to the actual situation of the foreign-invested institutions' business operations and the types of clients they face, and give differentiated treatment or provide more

Article No.	Content under the Draft Measures	ASIFMA Comments	ASIFMA Suggestions
		relationship. For corporate business, the information of relevant individuals such as board directors, legal representative and authorized signer will be provided to financial institutions for the financial service to corporate client, relevant treatment of such individual information is subject to the authorization from corporate, and no need to separately obtain the individual's consent.	operational guidance to corporate businesses in terms of difficulties in fulfilling various obligations such as the "obligation of notification" when handling personal information. Please refer to more detailed suggestions in this regard under our comments to Articles 56, 57, and 58 below.
54	Article 54 (Principles of Processing) Unless otherwise prescribed by laws and administrative regulations, a banking or insurance institution shall process personal information under the principle of "clear notification and authorized consent" and shall realize relevant functional control in the information system.	• Institutions utilize multiple channels to inform and obtain consent from individuals, including methods beyond information systems. A blanket requirement to "realize relevant functional control in the information system" may pose challenges in accommodating consent obtained through alternative channels such as paper signatures or recorded phone calls.	• NFRA to consider revising "realize relevant functional control in the information system", for example, to "retain relevant evidencing materials".
56, 57, and 58	Article 56 (Obligation of Notification) Prior to processing personal information, a banking or insurance institution shall inform the individual involved in a truthful, accurate, and complete manner of the processing of his/her personal information, type of personal information to be processed and storage period, application acceptance and handling procedures for the individual to exercise his/her right to information, and other matters that the individual shall be informed of as prescribed by laws and regulations. Banking and insurance institutions shall	• Further to our suggestion regarding the definition of "personal information" under Article 3 as well as our suggestion regarding personal information of corporate client under Chapter VI above, we would highlight again that in the case of a corporate client, the obligation of notification and obtaining consent from the individuals involved would be burdensome for institutions. In the public business of banking and insurance institutions, the counterparty of	• As mentioned in our suggestion under Chapter VI above, it is recommended to give full consideration to the actual situation of foreign-invested institutions' business operations and the types of clients they face, and give differentiated treatment or provide more operational guidance to corporate businesses in terms of difficulties in fulfilling the "obligation of notification" when handling personal information. • We are also aware that Article 17 (III) of the PBOC Draft Measures stipulates feasible

Article No.	Content under the Draft Measures	ASIFMA Comments	ASIFMA Suggestions
	develop rules for processing personal information. The rules for processing personal information shall be publicly displayed, readily accessible, specific, clear, and understandable. Article 57 (Obligation of Notification) Banking and insurance institutions shall not refuse to provide an individual with products or services on the grounds that the individual does not consent to the processing of his/her personal information or has withdrawn his/her consent, except that the processing of the personal information is necessary for providing products or services. Article 58 (Impact Assessment) When carrying out processing of personal information that has a significant impact on personal rights and interests, a banking or insurance institution shall carry out an impact assessment on the protection of personal information. The assessment shall cover the legitimacy and necessity of the processing of personal information, the impact on personal rights and interests and security risks, the legitimacy and effectiveness of the protection measures taken and whether the protection measures are appropriate to the risk degree. The impact assessment report on the protection of personal information and the handling record shall be kept for at least three years.	the legal relationship is the institutional client. The personal information of the relevant employees or other related persons of the institutional client is provided by the institutional client to the banking and insurance institution, and the banking and insurance institution does not directly face the relevant individuals. Regarding the requirement of "notifying individuals", whether there are differentiated regulatory requirements or guidance in the actual implementation of banking business operations, if the relevant individuals are informed or consent is obtained one by one and directly, it will bring great challenges and difficulties to the institutions in the implementation process.	and compliant operating methods for “non-direct collection of data from individuals or organizations”. It is recommended that this be used as a reference when implementing the regulatory provisions of this “duty of notification”. At the same time, it is recommended that regulators unify the provisions on such requirements as much as possible to facilitate institution management and implementation.
63	Article 63 (Personal Information Risk Report)	• We understand that this requirement	• It is recommended NFRA to refer to the

Article No.	Content under the Draft Measures	ASIFMA Comments	ASIFMA Suggestions
	Where personal information is or may be divulged, tampered with, or lost, a banking or insurance institution shall immediately take remedial measures, notify the individual involved at the same time of the case, and report the case to the NFRA or its local office. The notice shall include the following matters: (I) the type, cause, and possible harm of the information that is or may be divulged, tampered with, or lost; and (II) the remedial measures taken by the banking or insurance institution and the measures that can be taken by the individual involved to mitigate the harm. The banking or insurance institution may not notify the individual involved where the measures taken by it can effectively avoid harm caused by divulgence, tampering with or loss of the information. The regulatory authorities have the right to require the banking or insurance institution to notify the individual involved of the case if they deem that the case may cause harm.	corresponds to the requirement under Article 57 of the *Personal Information Protection Law*. However, in the course of daily operations, incidents such as loss of individual client information due to reasons like package mishandling by courier services may occur. Without establishing any reporting conditions, this situation can impose significant burdens both on institutions and regulators.	principles outlined in the *"Notice of the China Banking and Insurance Regulatory Commission on Issuing the Measures for Reporting Information on Incidents in the Banking and Insurance Industry" (《中国银保监会关于印发银行业保险业突发事件信息报告办法的通知》)* , which requires reporting of relatively significant incidents of personal information leakage, tampering, or loss. For example, to require reporting only when: (1) Involving personal information of more than 100 individuals; (2) Potentially or already resulting in financial losses exceeding 10 million RMB for banking or insurance institutions or their clients. • Alternatively, it is recommended to revise the requirement to aggregate and submit reports on a monthly basis on incidents involving a small number of clients or low-sensitivity personal information leakage, tampering, or loss.
65	Article 65 (Risk Monitoring) Banking and insurance institutions shall effectively monitor threats to data security, implement supervision and inspection, and take the initiative to assess risks, so as to prevent the occurrence of security incidents such as tampering with, destruction, leakage, and illegal use of data. The monitoring contents shall include: … (IV) abnormal flow of data at or above the	• The terms “different regions” and “abnormal” appear unclear.	• NFRA to consider clarifying “different regions” and “abnormal”.

Article No.	Content under the Draft Measures	ASIFMA Comments	ASIFMA Suggestions
	sensitive level in different regions; …		
68	Article 68 (Incident Response and Disposal) Banking and insurance institutions shall establish an incident management mechanism for data security incidents, establish an internal coordination linkage mechanism, set up a reporting mechanism for data security incidents with service providers and third-party partners, and timely dispose of potential risks and security incidents. …(IV) In the incident of a data security incident or a security defect or loophole of a network product or service used, conduct investigation and evaluation forthwith, and take remedial measures in a timely manner to prevent the expansion of the harm. Where a network product or service provider conceals its security defect or loophole, the banking or insurance institution shall order it to make corrections; if the product or service provider fails to make corrections as required or serious consequences are caused, the banking or insurance institution shall cancel the service qualification of the product or service provider, impose a penalty on the product or service provider under the relevant contract, and report the case to the NFRA or its local office.	• The management of security defects or loopholes associated with network products and services falls within the scope routine network information technology risk management for commercial banking institutions and may not be suitable for being included under this Draft Measures concerning data security.	• NFRA to consider revising Article 68 (IV) as follows: *"…(IV) In the incident of a data security incident, conduct investigation and evaluation forthwith, take remedial measures in a timely manner to prevent the expansion of the harm."*
69	Article 69 (Incident Supervision Report) A banking or insurance institution shall, within two hours after the occurrence of a data security incident, report the incident to the	• Under Article 67, data security incidents are classified into four levels. However, in the incident supervision reporting requirement outlined in Article 69, there is	• It is suggested that, considering the nature and severity of incidents, institutions should only be required to report significant and higher-level events.

Article No.	Content under the Draft Measures	ASIFMA Comments	ASIFMA Suggestions
	NFRA or its local office and submit an official written report within 24 hours after the occurrence of the incident. For an extremely serious data security incident, the banking or insurance institution shall forthwith take disposal measures, promptly notify users in accordance with the provisions, and report the incident to the local public security authority and financial regulator. The banking or insurance institution shall report the progress of disposal every two hours until the disposal is completed. After the completion of disposal of a data security incident, the banking or insurance institution shall, within five workdays, submit an assessment, summary, and improvement report on the incident and its disposal to the local regulatory authority. Where other laws and administrative regulations stipulate the incident disposal of data security incidents, the banking or insurance institution shall implement such provisions.	no differentiation based on the level of reported incidents. • There are various reporting requirements across multiple regulatory bodies, such as the CAC, the PBOC, the NFRA and the Public S*ecurity Bureau (PSB), which may be burdensome for institutions.* For example, the CAC's earlier released consultation on *the Administration Measures for Cyber Security Incident Reporting (《网络安全事件报告管理办法(征求意见稿)》)* in January 2024. This duplication could lead to confusion, inefficiency, and increased burdens on institutions, especially given the urgency of the reporting timeline mentioned under each regulatory mechanism. • After a data security incident occurs (regardless of the scope and extent of its impact), banking and insurance institutions are required to report it to the NFRA within 2 hours of the incident and submit an assessment, summary, and improvement report on the incident and its disposal within five working days after the disposal is completed, which may increase the operating costs of banks in practice. • For data security incidents, banks typically have an internal event identification process that requires a certain level of	• Ideally, we do hope that the NFRA could coordinate with other regulators such as the CAC, the PBOC, and the PSB to streamline incident reporting and avoid duplication. • For general security incidents that do not cause particularly serious, major, or significant impact on organizations and individuals, it is recommended to relax the time limit for reporting to the NFRA and allow appropriate flexibility to allow institutions to formulate assessment processes that are in line with their own business scale and comprehensively determine the standards for reporting to regulatory authorities based on the actual scope and degree of impact of the incident on individuals and organizations. • NFRA to consider the following suggestion regarding the timing:

Article No.	Content under the Draft Measures	ASIFMA Comments	ASIFMA Suggestions
		internal analysis and investigation to determine if the event constitutes a genuine data security incident. The two-hour reporting deadline after the occurrence of the event is excessively tight, making it challenging to implement. Taking reference from the regulations of other countries, for example, the Australian Prudential Regulation Authority's (APRA) CPS 234 on Information Security requires regulated entities to notify APRA as soon as possible and, in any case, no later than 72 hours, after becoming aware of an information security incident that has material impact. Similarly, the 24-hour requirement for written reporting is challenging as well. • Reporting progress of disposal every 2 hours is not in line with industry practice. In particular, reporting without progress within 2 hours will increase the burden on supervision and enterprises.	(i) Changing the requirement of reporting "within 2 hours after the occurrence of a data security incident" to "within 72 hours after confirming the occurrence of a data security incident". (ii) Extending the timeline to 7-day for institutions to collect all required information and formally submit written reports instead of 24-hour. • NFRA to consider changing "every two hours until the disposal is completed" to report the progress of disposal in a timely manner.
73	Article 73 (Reports by Institutions) Unless otherwise stipulated by laws and administrative regulations, for data sharing, entrusted processing, transfer transactions, and data transfer involving bulk data at or above the sensitive level, a banking or insurance institution shall report to the NFRA or its local offices 20 workdays prior to the processing and signing of relevant contracts.	• As discussed under Section 2 (2), this reporting requirement targeting sensitive level data or above is likely to increase the burden of regulatory reporting for foreign-invested institutions especially for low-risk transfers • The term "bulk" is unclear.	• We recommend that the NFRA creates exemptions for transfers of sensitive data for scenarios where there is low risk, e.g., transfer to the parent company. • NFRA to consider revising this requirement to be applicable to important level data or above.

Article No.	Content under the Draft Measures	ASIFMA Comments	ASIFMA Suggestions
		• The reporting content and format requirements are unclear.	• NFRA to consider clarifying what constitutes "bulk". • NFRA to consider clarifying the specific content and format requirements.