Main Topics Raised by the Financial Services Agency (FSA) at a Dialogue Meeting with the Industry Association

[Held on June 17, 2025 (with the Japan Securities Dealers Association (JSDA))]

1. Response to unauthorized accesses and transactions in Internet transactions

○ Regarding the cases of unauthorized access and transactions in Internet transactions for securities accounts, the FSA has recently announced on its website the damage situation as of the end of May 2025. Although the amount of unauthorized trading decreased slightly in May compared to April, the number of securities companies, including regional ones, involved in unauthorized transactions increased to 16, indicating that the damage is not yet under control.

○ We are aware that each securities company is currently sequentially taking measures to make multi-factor authentication mandatory for login. However, we would like to request that management continue to recognize that security measures are their responsibility and take all possible measures to prevent customer damage and to prevent the spread of damage.

○ In addition, we would like each securities company to sincerely respond to inquiries from and consultations with customers who have been affected by transactions that they do not know about owing to unauthorized accesses in an effort to alleviate their concerns, and to take sincere measures for damage restoration.

○ With regard to compensation, we recognize that some securities companies have already commenced procedures for recovery. We ask that securities companies fully recognize the magnitude of the anxiety caused by the incidents to their customers, and consequently to the securities industry as a whole, and take sincere measures to rebuild an environment in which customers can make investments with peace of mind.

○ We recognize that it may take a certain amount of time for compensation procedures, from notification of specific compensation details to completion of compensation. However, we would like securities companies to ensure that there is no delay in contacting affected customers so that they do not spend time in a state of anxiety without receiving any communication at all.

○ We have received reports that the call centers of securities companies are currently receiving many inquiries about compensation and other unauthorized transactions as well as about enhanced authentication functions such as multi-factor authentication. We understand that each securities company is working to strengthen its consultation system. We would like to request that each securities company continues to take all possible measures to respond to customers' inquiries and concerns in a timely manner.

○ We also understand that the Japan Securities Dealers Association (JSDA) is currently discussing a fundamental review of its "the Guideline for Preventing Unauthorized Accesses in Internet Transactions." We request that the JSDA and securities companies work together to review the guidelines to ensure that they are effective, taking into account the incidents and the increasing sophistication of cybercrime tactics in recent years.

2. Results of monitoring of securities business, etc. for PY2024

(Major securities companies)

Customer orientation, etc.

○ Each securities company has established a framework for product structuring, sales, and management that contributes to the best interests of its customers. We hope that securities companies will continue to provide high-quality financial products and services through appropriate monitoring and thorough quality control under the leadership of management.

○ It is requested that the issues identified through dialogue with the FSA concerning the handling of structured loans be appropriately addressed.

○ In addition, we would like to request that appropriate efforts be made to prevent recurrence of employee misconduct, such as by ensuring that all employees are familiar with the Code of Conduct, implementing various predictive detection and other measures, and continuing effective efforts based on these measures.

Group global governance

○ Major securities companies have made progress in expanding their businesses globally, and have made corresponding progress in developing their governance and risk management systems.

○ On the other hand, with the expansion of cross-border business, there were also cases of unpleasant incidents arising from cross-border operations and lack of compliance. As each securities company is expected to continue to expand its business, we would like to request that each securities company continues to strive to develop effective governance and risk management systems commensurate with its business strategy in a unified group and global manner while also paying attention to compliance.

(Regional securities companies)

○ In the current program year, we held in-depth dialogues with top management, mainly from the perspective of building sustainable business models, on the management issues faced by securities companies and their efforts to resolve such issues.

○ As a result, many of them cited the following as important issues: maintenance and expansion of the customer base and difficulty in securing human resources due to the declining population, dwindling birthrate, and aging society; the necessity of shifting to an asset management business model from the perspective of securing stable earnings; and streamlining of middle and back office operations from the perspective of reducing costs.

○ We have found that based on the recognition of these issues, securities companies are taking steps to spread customer-oriented business operations, develop and secure human resources, expand their product lineup, and promote digital transformation. We will continue to monitor the status of each securities company's initiatives, etc. through in-depth dialogue.

3. Survey on NISA account usage

○ On May 8, 2025, the FSA released a survey on NISA account usage (as of the end of March 2025). The number of NISA accounts was about 26.47 million and the total purchase price was about 59.3 trillion yen. The government target is 34 million NISA accounts and 56 trillion yen in total purchase price as of the end of 2027. This means that the government target for total purchase price was achieved about three years ahead of schedule.

○ In this way, NISA is becoming established as an important means of asset building for citizens. In the future, we will examine the extent to which NISA actually contributes to the stable asset building of citizens and the policy effects thereof, taking into account the opinions of experts, and will consider further improvements such as the improvement of convenience, if necessary.

○ In addition, in order to promote customers' understanding of NISA's long-term, cumulative, and diversified investment methods, it will become increasingly important for financial institutions to have detailed communication with customers during daily transactions and market fluctuations, as well as to establish customer contact points. Financial institutions are requested to keep these points in mind and continue to pay attention to the situation of their customers and make improvements as necessary.

4. Request to strengthen measures against unauthorized access to customer accounts

○ These incidents pose a serious threat not only to the securities industry but also to the trust in the financial sector as a whole. It is therefore imperative to promptly strengthen measures such as login authentication, countermeasures against spoofed websites and emails, detection of suspicious transactions, setting transaction limits, enhancing information sharing among financial institutions regarding attack methods and countermeasures, and raising customer awareness.

○ Not only is ID and password authentication alone vulnerable, but one-time passwords via email or SMS messages alone are not effective enough against phishing these days, so strong multi-factor authentication using pass keys and other methods must be made mandatory. In light of the fact that fraudulent methods are becoming increasingly sophisticated, it is necessary to keep a close watch on the technological trends of attack methods and countermeasures, on the assumption that even if countermeasures are taken, methods that surpass such countermeasures will emerge.

○ Given the vulnerabilities of ID and password-only authentication, and the limited effectiveness of one-time passwords sent via email or SMS against modern phishing attacks, it is essential to mandate robust multi-factor authentication methods, such as passkeys. As attack techniques continue to evolve, countermeasures must be

developed with the assumption that new methods will surpass existing defenses. Continuous monitoring of technological trends in both attack vectors and security solutions is necessary.

○ If adequate security cannot be ensured, financial institutions should consider suspending services proactively rather than reacting after damage occurs. Protecting customer assets is fundamental to customer-centric management, and we urge management to treat this as a critical issue requiring direct involvement.

5. Sending Password-Protected Files via Email

○ The procedure of sending a ZIP file with a password attached to an e-mail still persists in the financial industry. If a password is applied to a file attached to an e-mail, whether it is a ZIP file or non-ZIP file, the e-mail recipient is exposed to a security risk because the e-mail recipient cannot scan the file for security. Malware damage has occurred.

○ Therefore, sending password-protected files via email should generally be avoided. Instead, the email transmission path itself should be encrypted. If encryption is not possible and no alternative exists, secure online storage services should be used to ensure file safety. We urge management to do this as part of their basic cybersecurity measures.

Note on Password-Protected Files:

Sending password-protected files via email—especially when the password is sent through the same communication channel, even separately—poses a risk of interception. This method has been exploited in past malware outbreaks (e.g., Emotet).

Reference: JPCERT/CC Alert on Emotet Malware Resurgence

https://www.jpcert.or.jp/at/2022/at220006.html

Given these risks, financial institutions must consider alternative methods appropriate to each use case and implement corresponding security measures, such as encrypted email transmission.

○ The FSA intends to address this issue through inspections and monitoring.

6. Migration to post-quantum cryptography (PQC)

○ While the realization of practical quantum computers will bring societal benefits, it

also poses significant risks. Malicious actors may exploit quantum computing to break cryptographic algorithms used in internet banking and other services, compromising the confidentiality of customer information held by financial institutions. Such risks could undermine trust in the financial system.

○ To mitigate these risks, critical systems and services vulnerable to quantum computing must transition to cryptographic algorithms that are resistant to quantum attacks—known as Post-Quantum Cryptography (PQC).

○ Migrating to PQC requires substantial time, human resources, and investment, including coordination with IT vendors. Although the practical implementation of quantum computers is expected around 2035, major system upgrades typically occur only every few years, limiting opportunities for migration. Given the resources required, it is inappropriate to delay preparations; immediate action is necessary.

○ Specifically:

- Financial institutions should begin consultations with IT vendors and develop a roadmap for PQC migration. While the Financial ISAC is currently working on a roadmap template, institutions should not wait for its completion and should begin what they can immediately.

- To prioritize PQC migration efforts, institutions must comprehensively identify their information assets, create an inventory of the cryptographic algorithms used for each asset, and assess the associated risks—such as those posed by quantum computing or pre-quantum attacks like Harvest Now, Decrypt Later (HNDL). Evaluations of importance and urgency should also be conducted.

(Note) An attack in which a threat actor steals encrypted information today with the intention to decrypt it later when a practical quantum computer is available (so called HNDL attack: harvest-now, decrypt-later attack).

○ The FSA will continue to promote and monitor the progress of PQC migration across financial institutions and the industry through inspections and monitoring, also in collaboration with Financial ISAC and relevant industry associations.

(Reference) The FSA "Report of the Study Group on Deposit-Taking Institutions' Response to Post Quantum Cryptography" (published in November 2024)
https://www.fsa.go.jp/news/r6/singi/20241126.html

7. Working Group on Improving Internal Audits of Financial Institutions

○ In January 2025, the FSA established the Working Group on Improving Internal Audits of Financial Institutions to encourage financial institutions to upgrade their internal audits.

○ The Working Group held a total of five meetings to exchange opinions with financial industry associations and others on the level of internal audits and the attitude required of management. Based on these opinions, a report entitled "Report of the Working Group on Improving Internal Audits of Financial Institutions (2025)" was published (June 20, 2025). It is requested that management use this report as a reference to further enhance the sophistication of internal audits.

○ In view of changes in the environment surrounding internal audits of financial institutions, the FSA will continue to encourage financial institutions through inspection and monitoring to improve internal audits, and publish useful information such as monitoring results in the form of reports and other publications.

8. Results from the monitoring of customer-oriented business operations by companies selling and structuring risk-involving financial products

○ In PY2024, in addition to following up on improvements related to foreign currency denominated lump-sum payment insurance and structured deposits, issues that were pointed out in PY2023, the FSA monitored the product governance and sales and management systems of sales companies, etc. for a wide range of financial products such as foreign stocks, fund wraps, structured bonds, foreign currency bonds, and investment trusts.

○ The results of this monitoring were published as "Results of Monitoring of Customer-Oriented Business Operations by Companies Selling and Structuring Risk-Involving Financial Products" (July 1,2025).

○ Based on the results of dialogue with sales companies, etc. and qualitative and quantitative questionnaire surveys, this report summarizes the issues and innovations identified in sales companies, etc. with regard to their sales and management systems for financial products, as well as the basic concept and important elements of the PDCA cycle for customer-oriented sales of financial products.

○ It is requested that management exercise leadership in ensuring customer-oriented business operations by referring to the results of this monitoring, etc.

9. Results of dialogue on fostering a sound corporate culture and conduct risk management system

○ In PY2024, we held dialogues with major financial institutions on the theme of fostering a sound corporate culture and initiatives in conduct risk management.

○ Examples of initiatives identified through this dialogue were published in the "Report on the Results of the Dialogue on Fostering a Sound Corporate Culture and Conduct Risk Management System" (June 25,2025).

○ Amid the recent occurrence and discovery of multiple scandals in the financial industry, we would like management to reaffirm that it is necessary not only to strengthen the organizational structure and rules but also to encourage officers and employees to have a sense of norms in order to prevent the occurrence of scandals, and to use this report as a reference to exercise leadership to foster a sound corporate culture and properly manage conduct risks.

10. Establishment of AML/CFT Frameworks

○ The FSA requested that financial institutions complete the establishment of the basic framework required under the “Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism” by the end of March 2024. Almost all financial institutions reported that they had completed by the deadline.

○ However, some securities companies reported that they had not yet completed the establishment of the basic framework. It is requested that management of such securities companies take the lead in completing the framework establishment.

○ The FSA will consider taking administrative measures as necessary against securities companies that are deemed to be particularly fall behind, as it does with other types of businesses.

11. FSA AI Public-Private Forum

○ In March 2025, the FSA released the AI Discussion Paper (Version 1.0), thereby

announcing its policy to encourage the sound use of AI by financial institutions and others. We hope that efforts to improve customer convenience and operational efficiency will progress under the appropriate understanding and proactive involvement of management, while appropriately controlling risks under a risk-based approach. In order to ensure steady progress in such efforts, the FSA will strive to create an environment in which financial institutions can safely take on challenges using AI by sharing examples of AI initiatives and clarifying the applicability of regulations.

○ As part of these efforts, the FSA AI Public-Private Forum has been established and the first meeting will be held on June 18, 2025. In this forum, we plan to hold multifaceted discussions by inviting various stakeholders from the public and private sectors, including financial institutions, AI model developers, vendors, academia, and relevant ministries and agencies, to share examples of initiatives and to explore practical issues. The JSDA has also been invited to participate, and we would appreciate their active involvement in the process going forward.

- Website: https://www.fsa.go.jp/news/r6/singi/20250603.html

12. G7 Finance Ministers and Central Bank Governors Meeting in May 2025

○ The G7 Finance Ministers and Central Bank Governors Meeting was held in Banff, Canada from May 20 to 22, 2025. Major outcomes related to the financial sector in the Communiqué published after the meeting are outlined below.

- First, members reaffirmed that continued focus on financial stability and regulatory challenges remains essential to ensure the effective functioning of the financial system.
- On non-bank financial intermediation (NBFI), given its increasingly important role in financing the real economy, members agreed on the need to share knowledge and approaches to assess the availability, use and quality of non-bank data, as well as to monitor and assess potential risks.
- On AI, members expressed the need to monitor and assess the benefits of AI for the financial sector and the potential risks to financial stability as the adoption of AI further progresses.

- On cyber risk, members stated that the G7 will continue to further strengthen response capabilities and procedures in the event of a major cyber incident.
- Finally, the main finance-related contents of the Financial Crime Call to Action, adopted together with the Communiqué are as follows:
  - Members confirmed a commitment to support the effective implementation of risk-based anti-money laundering and other measures to promote economic development and financial inclusion.
  - Members expressed serious concerns that the theft of crypto assets by North Korea and other countries has reached an unprecedented level, and agreed to promote the investigation and exchange of information on new risks related to crypto assets and take necessary measures from the perspectives of cybersecurity, anti-money laundering, etc.
  - Members gave continued support the acceleration of the global implementation of the Financial Action Task Force (FATF) standards on crypto assets and the FATF's work on emerging risks including those that arise from misuse of stablecoins, peer-to-peer transactions and decentralized finance (DeFi) arrangements.
  - Members supported the ongoing work to strengthen FATF standards on Payment Transparency and the G20 roadmap for enhancing cross-border payments.

○ The FSA will continue to communicate with financial institutions and contribute to global discussions.

13. CDSC's Public Consultation on Draft Common Carbon Credit Data Model

○ The Climate Data Steering Committee (CDSC) was established in July 2022 to promote access to high-quality climate-related data from the private sector, which is essential for achieving net zero.

○ The G20 Sustainable Finance Working Group (SFWG) in 2025 is focusing on the issue of the lack of uniform standards for carbon credit data, which makes it difficult to compare carbon credits across markets and is developing a Common Carbon Credit Data Model to organize a minimum set of key data attributes that can be referenced

in the development of standards, along with voluntary guidance.

○ The CDSC s leading this initiative, with a newly established ad hoc working group tasked with preparing and publishing the data model and technical note.

○ The FSA is a member of the CDSC and participates in the working group, collaborating with the Ministry of Economy, Trade and Industry, the Ministry of the Environment, and others.

○ The data model presents a baseline that policymakers and market participants can voluntarily adopt to support data standardization and transparency in the carbon credit market.

○ A public consultation is scheduled to take place from July 4 to August 13, 2025, Financial institutions are invited to view it and provide comments as necessary.

14. IOSCO Annual Meeting

○ International Organization of Securities Commissions (IOSCO) held its annual meeting in Doha, Qatar from May 12 to 14, 2025. The IOSCO Board discussed various issues, including online harm, pre-hedging, and fintech. In particular, we would like to mention the "Statement on Combatting Online Harm and the Role of Platform Providers" released on May 21, 2025.

○ The statement urges platform providers to consider taking the following actions: (1) conducting due diligence to eliminate unregistered investment solicitations; (2) monitoring and swiftly removing investment scam content and advertisements, and (3) establishing proactive communication channels with authorities, including interactions related to suspected fraudulent activities.

○ In September 2024, we requested that the JSDA and securities companies broadly collect information and raise awareness on false advertisements, etc., and actively request the removal of false advertisements impersonating themselves. We ask that they continue to take such investor protection measures.

15. Asia Day

○ On October 22, 2025 during Japan Weeks, the FSA, jointly with the Asian Development Bank (ADB), the JSDA, and others, plans to hold an event called "Asia

Day," aimed at stimulating the circulation of financial resources in the Asian region.

○ The ADB President will be the keynote speaker at the event, to which high-level Asian authorities and stakeholders in Asian financial and capital markets are expected to be invited. The event information will be posted on the FSA website in the near future. We hope you will be interested and participate in the event.

(End)