“Anti-Money Laundering, Counter Financing of Terrorism, and Counter-Proliferation Financing”

Current Status and Challenges

(As of March 2022)

April 2022

Financial Services Agency

Contents

Documentation

Introduction (Purpose of this Report)

With respect to Anti-Money Laundering ("AML"), Counter Financing of Terrorism ("CFT"), and Counter-Proliferation Financing ("CPF"), this paper summarizes and publishes changes in the risks surrounding financial institutions ("FIs") in Japan, the status of actions taken by businesses under the supervision of Financial Services Agency ("FSA") as of the end of March 2022, the results of the 4th round of Mutual Evaluation Report of Japan by the Financial Action Task Force (FATF), and FSA's initiatives.

Chapter 1. Risks Surrounding FIs in Japan

1. Risks Surrounding FIs in Japan

As advances in technology lead to the diversification of settlement methods, financial transactions are becoming more globalized and complex, while the risks faced by FIs in money laundering ("ML"), terrorist financing ("TF") and proliferation financing ("PF") are also changing. Furthermore, as ML/TF often take place across borders, it is necessary for countries to work together to develop proactive measures and control frameworks. As international AML/CFT/CPF is becoming increasingly important year by year, FIs are required to continuously improve their ML/TF risk control framework in response to changes in ML/TF risks. In other countries, the AML/CFT/CPF deficiencies of FIs have a bigger impact on their business, for example, large fines and other penalties were imposed on these FIs, their share prices declined, and even their managements were changed.

FIs must not be involved or used in crimes, including ML/TF. From the perspective of legal compliance and reputation, the establishment of a robust ML/TF risk control framework is an urgent task for FIs in Japan.

The global COVID-19 pandemic since 2020 has had a significant impact on day-to-day life and various businesses not only in Japan but also in many other countries. ML/TF risks are also changing, due to factors such as the expansion of non-face-to-face transactions.

In Japan, people have voluntarily refrained from going out and have worked from home, which resulted in the increase of non-face-to-face transactions. With non-

face-to-face transactions, it is easier to falsify customer identification information or impersonate someone else than with face-to-face transactions. Therefore, the National Risk Assessment ("NRA") published in December 2021 by the National Public Safety Commission categorized non-face-to-face transactions as high-risk transactions.

In addition, the COVID-19 pandemic highlighted that there have been swindles to obtain personal information, such as PIN, account numbers, and credit card information, by sending email messages or SMS (short message service) making such claims as "procedures are required for the transfer of Special Cash Payments" or "masks can be obtained free of charge," leading to phishing websites. There have also been new cases of fraud, in which the perpetrator pretends to be a national or municipal government official making a phone call asserting such claims as "acting for the application of Special Cash Payment," "subsidies are provided for COVID-19 measures," or "masks can be sent," leading the victim to an ATM to transfer money. It is necessary to note that the criminal methods used in the ML/TF environment are evolving with the changes of lifestyles and behavior in society.[1][2]

On August 30, 2021, the FATF, which sets international standards for AML/CFT/CPF, published the 4th round of Mutual Evaluation Report ("MER") of Japan on AML/CFT/CPF in light of its standards (such as the FATF Recommendations). The report says the Japanese AML/CFT framework was evaluated as having achieved better results in several areas by Japan's efforts than those of the 3rd FATF Mutual Evaluation Report of Japan in 2008, as described in Chapter 3. However, the 4th MER states that Japan needs to prioritize efforts in certain areas, including strengthening the supervision of FIs and designated non-financial businesses and professions ("DNFBPs") and enhancing the AML/CFT/CPF measures taken by FIs and DFNBPs (called specified business operators). Given the FATF MER of Japan, the Government of Japan published the "National AML/CFT/CPF

---

[1] FSA "Beware of Crime, etc. Caused by the COVID-19 Virus!"
https://www.fsa.go.jp/news/r1/ginkou/20200407/20200407.html

[2] In response to the global pandemic of COVID-19, the FATF issued a Chair's Statement titled "Measures to Address the COVID-19 Virus (COVID-19) and Associated Illicit Financial Flows" in April 2020 and "The Significance of Allocating Sufficient Resources to AML/CFT Regimes under the COVID-19 Pandemic" in October 2019. In May 2019, the FATF released a report that includes new threats and vulnerabilities, their impact on ML/TF risk management regimes in the public and private sectors, and recommended responses.
https://www.fsa.go.jp/inter/etc/20201030.html
http://www.fatf-gafi.org/publications/fatfgeneral/documents/covid-19-ml-tf.html

Action Plan" for the next three years to work steadily on necessary legislative actions. To achieve the goals of the Action Plan, it is necessary for both the public and private sectors to continue working together to enhance the AML/CFT/CPF regime.

2. Overview of money laundering crime in Japan and the perpetrators

Article 8 of the Act on Prevention of Transfer of Criminal Proceeds ("APTCP") requires specified business operators (excluding lawyers) to report suspicious transactions to competent authorities when they have identified suspicious transactions stemming from criminal proceeds or customers, etc. who are conducting ML in transactions related to specified business. According to the "Annual Report on Prevention of Transfer of Criminal Proceeds (2021)" published by the National Police Agency, the number of suspicious transaction reports has exceeded 400,000 for six consecutive years since 2016, and reached 530,150 in 2021. In the data, the banks accounted for 390,381 cases, 73.6% of all reports, a much larger proportion than Money Lending Business Operators (35,442 cases, or 6.7%) and Credit Card Operators (34,904 cases, or 6.6%).

The National Risk Assessment (December 2021) analyzes ML crime in Japan as follows.

There are various possible types of persons who conduct ML. In Japan, the main perpetrators of ML crime are members of *boryokudan*, specialized fraud crime groups, and crime groups consisting of foreign nationals in Japan.

Boryokudan continue to commit crimes repeatedly and skillfully in ML in order to gain economic benefits, and they pose a particularly serious threat in Japan. In concrete terms, it can be seen that members and associate members of *boryokudan* and other related persons are involved in a wide variety of crime, including fraud, hidden financial crime, gambling crime, and theft, and are boldly committing ML crime.

In recent years in Japan, there have been frequent occurrences of specialized fraud (including extortion to gain cash, etc. and opportunistic theft of cash cards, etc. [cash card fraud and theft]), in which the victims trust the perpetrators without face-to-face contact by calling or other means, and are swindled by one or more people into transferring money to designated savings accounts or other methods. The total amount of damage in 2020 was approximately 28.5 billion yen. The specialized fraud crime groups have been systematically working to commit fraud, and have been conducting ML crime by using bank accounts under fake names or other people's

names obtained through specialized fraud.

Crime involving foreign nationals is characterized by the fact that criminal groups consisting of foreign nationals visiting Japan carry out crimes under the direction of another criminal group located in the members' country of origin.

Crime involving foreign nationals tends to become sophisticated and latent as human networks and modes of crime are not complete within a single country and roles are shared across national borders. As organized ML crime committed by foreign nationals visiting Japan, there have been confirmed cases of ML crime related to illegal money transfer using internet banking committed by a Chinese group, shoplifting committed by a Vietnamese group, and international fraud committed by a Nigerian group. Over the past three years from 2018 to 2020, the number of solved cases of Act on Punishment of Organized Crimes and Control of Proceeds of Crime offenses involving foreign visitors to ML was highest for visitors from China and Vietnam, with the China accounting for nearly half of the total.[3] With regard to terrorist financing, FATF Recommendation 8 "Non-Profit Organisations" (NPOs) recommends that each country should review the adequacy of laws and regulations related to NPOs that the country has identified as being vulnerable to terrorist financing in such forms as pretending to be a legitimate organization, using a legitimate organization as a conduit for terrorist financing, or using funds for legitimate purposes to divert funds to terrorist organizations.

Regarding PF, FATF Recommendation 7 "Targeted financial sanctions related to proliferation" stipulates that each country should implement targeted financial sanctions in order to comply with the United Nations Security Council ("UNSC") Resolutions on the Prevention, Suppression, and Elimination of the Proliferation and Financing of Weapons of Mass Destruction. The FATF calls on member states to freeze without delay the funds and other assets held by any persons or entities designated by UNSC under Chapter VII of Charter of the United Nations and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of such persons or entities.

In addition to the analysis of products and services identified as being at risk in each business category, the National Risk Assessment (December 2021), identifies the following items as those considered to be high risk based on the analysis of these

[3] 2021 The NRA page 15

ML entities.

- Transaction types: non-face-to-face transactions, cash transactions, and foreign transactions.
- Countries and regions: North Korea, Iran
- Customers: Anti-social Forces (*boryokudan*, etc.), international terrorists (Islamic Extremists, etc.), non-residents, foreign politically exposed persons (foreign PEPs, etc.), and legal persons (legal persons without transparency of beneficial owner).

Although both the number of criminal acts and the amount of damage caused by illegal money transfers related to internet banking in 2021 decreased compared to the previous year, damage continued to occur. Most of these damages are believed to have been caused by SMS or e-mail disguised as FIs or home delivery companies used to lead people to phishing sites. There have also been confirmed cases of unauthorized access to memo applications that store information on the Internet, and theft of passwords and other stored information.

The threat posed by cyberspace continues to be extremely significant. For example, the damage caused by ransomware on Japanese companies and organizations has increased significantly, and there have been numerous cyberattacks on Japanese government agencies and research institutions.[4]

Regarding ransomware attacks, the proliferation of double extortion tactics and malware that could affect industrial control systems continues to be identified in Japan and overseas.

[4] National Police Agency, "Threats Surrounding Cyberspace in 2021 (Preliminary Version)"

3. Crime types and risks that should be noted in AML/CFT/CPF

(1) Money laundering, terrorist financing and proliferation financing using crypto-assets

In Japan, the Payment Services Act ("PSA") and the APTCP were amended in 2016 to develop legislation on crypto-assets (came into force in April 2017). As of April 2021, only 58 countries and regions have introduced legislation on crypto-assets (or explicitly prohibit crypto-assets by such laws and regulations).[5] Some overseas business operators conduct business such as selling crypto-assets to residents in Japan without registration, and FSA has issued warning letters.[6]

In addition, regarding crypto-assets, although the involvement of FIs is essential, as is the case with existing legal currencies in converting high-value crypto-assets into cash, transactions can generally be completed without intermediation or restrictions by FIs. Therefore, there is a possibility that terrorists and terrorist supporters, etc. are abusing crypto-assets as a means of avoiding economic sanctions,[7] and it is difficult to ascertain the actual size of these transactions. To this regard, there have been confirmed cases overseas in which people have provided a way to seek funding for ISIL (Islamic State of Iraq and the Levant) with crypto-assets without identifying themselves by name by making their crypto-asset wallet addresses known on Twitter,[8] and to provide financial assistance for travel to ISIL supporters who are planning to flee to Syria.[9]

In addition, a report by the Expert Panel of the North Korean Sanctions Committee in UNSC points out that North Korean attacks on crypto-assets exchange services providers ("CESPs") are continuing,[10] and the April 2020 US Federal Interagency Joint Report on North Korean Cyberattacks also calls attention to North Korea's illegal acquisition of U.S. dollar assets through cyberattacks on companies, FIs, central banks, and CESPs.[11]

---

[5] FATF Second 12-Month Review Report on the FATF Standards for Virtual Assets and Virtual asset Services Providers, page 10, https://www.fsa.go.jp/inter/etc/20210706/20210706.html
[6] Disclosed on the FSA website. June 2021 Case Study : "Issuance of Warning Letter to Binance Holdings limited" https://www.fsa.go.jp/policy/virtual_currency02/Binance2_keikokushilyo.pdf
[7] FATF Second 12-Month Review Report on the FATF Standards for Virtual Assets and Virtual asset Services Providers, page 22
[8] 2021 The NRA page 12
[9] 2021 The NRA page 58
[10] e.g.8 September 2021 S/2021/777 The midterm report of the 1718 Panel of Experts. Para 171
[11] DPRK Cyber Threat Advisory: Guidance on the North Korean Cyber Threat, The U.S. Departments of State, the Treasury, and Homeland Security, and the Federal Bureau of Investigation, April 15,2020

The October 2020 statement by the Minister of Finance of the G-7 Central Bank Governors Meeting[12] and the May 2021 Statement by the Leaders of the G-7 Cornwall Summit[13] also pointed out that increasing threat of ransomware, which demands a ransom for data recovery and other operations, and damage caused by ransomware infections. In the wake of a series of reports of major ransomware infections in Japan and abroad, there have been cases of people demanding payment in crypto-assets.[14,15] In addition, there have been cases outside of Japan where ransom attacks are believed to have been used to fund the activities of large-scale organized crime groups.[16]

Such attempts to obtain crypto-assets from victims through ransomware, fraud, or extortion have been identified by the FATF[17] as a new type of crime. Other examples of criminals' use of crypto-assets include the direct use of crypto-assets as a means of payment in order to illegally trade regulated items (including but not limited to firearms, child exploitation, and human trafficking), tax evasion, and economic sanction evasion, and the use of crypto-assets as a means of ML, such as the remittance, collection, and layering of criminal proceeds.

---

https://home.treasury.gov/system/files/126/dprk_cyber_threat_advisory_20200415.pdf

12 G7 Finance Ministers and Central Bank Governors' Statement on Digital Payments, https://www.fsa.go.jp/inter/etc/20201014/20201013_1.pdf and Ransomware Annex to G7 Statement

13 Carbis Bay G7 Summit Communiqué, https://www.mofa.go.jp/mofaj/files/100200009.pdf

14 Ransomware: The True Cost to Business, A Global Study on Ransomware Business Impact, Cybereason, June 2021. The U.S. Treasury Department's Office of Foreign Assets Control (OFAC) has identified and sanctioned VASPs involved in ransomware ransom transactions, and as of November 2021, two companies have been sanctioned.

15 Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021, Financial Crimes Enforcement Network, 15 Oct. 2021.
The U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN) introduced crime trends in this report published in October 2021. Specifically, the majority of ransom payments are in Bitcoin, but recently there has been an increase in requests for payment in highly anonymized coins (e.g., Monero). In order to evade tracking, criminals do not reuse the address of a wallet once used, but use a different wallet each time. They are also "chain-hopping" to evade tracing by using mixers and exchanging different virtual assets (especially highly anonymized coins). Furthermore, when using intermediaries, there is a tendency to use DeFi (Decentralised Finance) and offshore firms that are less subject to KYC regulations, etc.
In addition, FinCEN and OFAC published the advisory in October 2020, which lists as red flag indicators of suspicious transactions that financial institutions should be aware of: (1) customers who have no experience in crypto asset transactions suddenly attempting to purchase virtual assets in a hurry or in large amounts (the victim's symptom), and (2) a customer attempting to use a crypto asset exchange in a jurisdiction with less stringent money laundering regulations or attempting to send highly confidential coins to multiple wallets at once (the offender's symptom).

16 National Police Agency, "Threats in Cyberspace in 2021" (first half, Japanese Version)"

17 FATF Second 12-Month Review Report on the FATF Standards for Virtual Assets and Virtual asset Services Providers: page 22.
https://www.fsa.go.jp/inter/etc/20210706/20210706.html

Column [ML/TF risk trends in virtual assets]

The "SECOND 12-MONTH REVIEW OF THE REVISED FATF STANDARDS ON VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS"[18] published by the FATF in July 2021 identified ongoing trends in ML/TF risks associated with crypto-assets as "regulatory arbitrage" by uneven global implementation of the revised standards, with a large number of weakly compliant or noncompliant jurisdictions, "misuse of VASPs/CESPs that do not/weakly comply with regulations" and "misuse of tools and methods to increase anonymity. "

As for the status of global implementation of the FATF Standards related to virtual assets and virtual assets service providers, as of April 2021, 58 of the 128 jurisdictions that responded to the survey reported that they had taken some necessary legislative measures, including six of them prohibiting VASP' operations, but only 29 jurisdictions reported that they have conducted on- or off-site inspections and 18 jurisdictions mentioned that they have administrative sanctions in place. Some VASPs/CESPs have advanced to jurisdictions with weak regulatory and supervisory regimes, and furthermore, illicit actors are taking advantage of the weak AML/CFT environments in these VASPs/CESPs.

Furthermore, the following are tools and abuse methods to increase anonymity

- The use of tumblers and mixers (method that obscures the connection with the originator by mixing transactions with those of several others, aggregating them into one, and redistributing them to each beneficiary)
- Use of AECs (Anonymity Enhanced Coins) and Privacy Coins (crypto-assets in which anonymous technology is embedded in a blockchain platform)
- Use of a privacy wallet (a wallet that does not have an intermediary like a CESP, in which individuals manage their private keys and complete transactions themselves)
- Chain hopping (replacing crypto-assets with other crypto-assets; since blockchains differ by type, their history cannot be traced as a transaction of one crypto-asset)
- Dusting (transferring a small amount to random wallets in an attempt to hide the owner of funds; this technic is also known as part of the attacking or tracing technique, and used to identify such diversification called a "dusting attack."
- Use of DApps and DEX

Since around 2020, the method called CoinJoin, a method of hiding the relationship between the originator address and the beneficiary address by pooling coins and comingling multiple transactions into one to enhance anonymity, has increased significantly.[19]

[18] See Note 17

[19] See Study on Privacy and Traceability of Financial Transactions Using Blockchains, page 49, "Mixing" (2018, FSA).

We should be aware of the extent to which crypto-asset transactions will shift to transactions between individuals without the use of regulated intermediaries (P2P transactions) for the purpose of avoiding regulations. The FATF report presents quantitative market metrics on P2P transactions for the first time using data from seven blockchain analytics companies. While there remain challenges in understanding the actual state of P2P transactions, including technical limitations as the analysis results by the seven blockchain analytics companies vary, (1) P2P transactions are at a reasonably large scale (for bitcoins, five of the seven companies report that approximately 50% or more of the transaction amount is P2P transactions), and (2) the proportion of illicit transactions is higher for P2P transactions than for transactions via CESPs. However, the report concludes that there has been no significant increase in the proportion of P2P transactions since the finalization of the FATF Standards in 2019, and that changing the regulatory approach through regulation on intermediaries is not necessary at this point in time. Regarding crypto-assets, the report states that the early adoption the FATF Standards in each jurisdiction is the most effective way to address P2P risks, as the dissemination of crypto-assets is currently limited as a means of payment for goods and services and it is necessary for users to convert into fiat currency via CESPs.

However, if globally adopted stablecoins and other crypto-assets become widely adopted in the future, the current approach of reducing risk at on- and off- ramps to the traditional fiat economy will not work sufficiently, so the report underlines that close monitoring on this front will be necessary.

The FSA has long provided the red flag indicators related to the above-mentioned cases, and has received reports on the number of cases identified by the CESPs. It is important that the providers continue to take measures such as monitoring to ensure the detection of such cases.

(2) Risks involved in settlement of funds

The business models of Fund Transfer Service Providers vary. For example, there are businesses that provide remittance and settlement services using mobile phones for online sales of goods and services by individuals, small and medium-sized enterprises and sole proprietors, businesses that provide cross-border remittance services to the home country of foreign visitors to Japan, businesses that issue cards that enable shopping at member stores and withdrawal of local currency from ATMs when service users study abroad or go on business trips, and businesses that are in charge of refunds to a large number of users due to the returns of goods or cancellation of events commissioned by other businesses. In addition, since businesses vary in size and transaction type, the risks they face are also different.

Like deposit-taking FIs, Fund Transfer Service Providers need to deal with ML/TF risks associated with cross-border and domestic transactions. In other words, Fund Transfer Service Providers not only face risks of domestic fund flows, but also risks common to cross-border transactions, such as the transfer of criminal proceeds to foreign countries with different legal systems and trading systems, making it difficult to track them. Also, some money transfer operators may face potential ML/TF risks due to inadequate identification at their agents.

In addition, when a business operator providing cross-border remittance services conducts settlements by consolidating multiple small remittance transactions between its domestic and foreign locations (so-called bulk remittance transactions), there is a risk that information on individual senders and recipients included in the bulk remittance may become opaque from the perspective of banks that provide accounts to the Fund Transfer Service Providers, even though each small remittance is a cross-border fund settlement in nature. It is important for Fund Transfer Service Providers and banks providing accounts to take risk-based measures, such as checking each other's implementation of risk mitigation measures, to ensure that the services are not used for ML and that sanctioned persons are not contained in the users.

Furthermore, some collection agent service providers (*shunou daikou gyosha*) may also conduct cross-border fund settlements which may pose higher ML/TF risks. For example, some collection agents, in cooperation with overseas collection agents, provide domestic customers with a function similar to cross-border wire transfers in terms of economic effect by opening accounts with domestic and overseas banks that settle funds for overseas transactions using SWIFT, an international funds settlement network, and combine this with domestic payment infrastructure. It is important for banks that provide accounts with such providers to identify and assess risks in the flow of funds handled by collection agents, and to take measures to mitigate ML/TF risks related to cross-border wire transfers through risk-based customer due diligence (CDD).

(3) Risks in non-face-to-face transactions

Businesses that provide non-face-to-face remittance and settlement services via mobile phones face the risk of money launderers using IDs and passwords illegally obtained in some way to transfer or withdraw funds by impersonating the legitimate account owner.

One of the methods of verification at the time of transaction allowed by Fund

Transfer Service Providers is to verify that the customer account has already been opened at the bank. This is a method whereby a Fund Transfer Service Provider verifies that, for certain specified transactions settled by way of account transfer in a deposit/savings account, the business operator who has opened the account has verified the time of transaction with the customer or representative when concluding the deposit/savings contract and has preserved a record of such verification. It is used in Fund Transfer Service Providers as a method to link a bank deposit account held by a customer with an account in a Fund Transfer Service Provider and complete verification at the time of transaction.[20]

Under these circumstances, in 2020, there were multiple cases where a malicious third party, based on the depositor's account information obtained fraudulently in some way, opened a Fund Transfer Service Provider account in the name of the depositor, linked it to the victim's bank account, and then charged funds from the bank account to a Fund Transfer Service Provider account, thereby making fraudulent withdrawals.

In the abovementioned instance, the Fund Transfer Service Providers were vulnerable in that they used only the PIN number of the customer's bank card to confirm and authenticate the transaction when entering into an account transfer agreement (i.e. contract to initiate adding values from the customer's bank account to account with the Fund Transfer Service Provider).

In February 2021, FSA revised its Administrative Guidelines (Vol. 3: Financial Corporation 14: Fund Transfer Service Providers) to provide points to keep in mind for account coordination, including verification at the time of transactions using the above mentioned method. In November 2020, JBA also published the "Guidelines for Account Coordination with Fund Transfer Service Providers and Other Institutions,"[21] which summarizes points to be noted on the part of banks. This guideline shows the concept and examples of how banks should provide payment services in cooperation with fund transfer service providers, in response to several cases of unauthorized withdrawals from bank accounts by malicious third parties who have illegally obtained depositors' account information through fund transfer service providers that provide payment services linked to bank accounts.[22] In December 2020, Japan Payment Service Association also published "Guidelines for

[20] Article 13, Paragraph 1, Item 1 of the APTCP Enforcement Rules
[21] https://www.zenginkyo.or.jp/news/2020/n113001/
[22] Publication of JBA "Guidelines for Account Collaboration with Funds Transfer Service Providers, etc."(November 30, 2020)

Preventing Fraud in Connection with Bank Accounts, "which set out the measures that Fund Transfer Service Providers would take to prevent fraud in connection with bank accounts.

These Guidelines require that appropriate and effective fraud prevention measures be implemented for users of the funds transfer services, such as effective verification at the time of transactions through public personal authentication or other means, and verification of the identity of the users and their depositors by verifying the information of the users confirmed through personal identification documents with the information held by the collaborating entities, and that it is confirmed that the collaborating banks have introduced authentication methods, such as multi-factor authentication that combine effective elements.[23][24]

(4) Risks associated with digital verification methods (e-KYC)

e-KYC (electronic Know Your Customer) is a method to confirm customer identity that is completed online as confirmation at the time of transaction in the APTCP, which is a method prescribed in Article 6, Paragraph 1, Item 1, Sub-items (e) through (g), etc. of the Enforcement Rules of the APTCP.

In particular, in recent years, FIs have often used a method to receive from a customer an image of an identification document with a photo and an image of the person's appearance (Item (e)), and FIs often commission other companies to confirm the identity of a customer who has applied for e-KYC and to inspect the identification documents.

However, if FIs do not provide appropriate training or guidance to the outsourcee of e-KYC services, or if the business operator entrusted with part of the procedures for identifying customers of e-KYC does not perform appropriate verification, it is important that FIs take measures, such as monitoring, to ensure that verification procedures at the time of transaction are properly performed by the outsourcee, because there is a possibility that the outsourcee would not appropriately perform e-KYC services and would not appropriately perform verification at the time of transaction.

---

[23] Except in cases where a Public Personal Authentication is used, it is preferable to include not only the name, residence, and date of birth of the user, but also the phone number, etc.

[24] For example, in addition to user authentication using fixed IDs and passwords, methods using variable passwords using hardware tokens or software tokens, and methods using electronic certificates, such as public personal authentication, have been introduced.

(5) Cyber crime (phishing, ransomware)

In recent years, while digitalization is progressing and cyberspace is creating a new public space, in Japan, with the spread of cashless payments, the number of cleared cybercrimes reached a record high in 2021. In addition, the damage caused by ransomware (malicious programs that demand ransom) is increasing, and there are confirmed cases that have a significant impact on the lives of citizens. The threat surrounding cyberspace continues to be extremely serious, for example, it is found that information leaks by unauthorized access and state-backed cyberattack groups have actively worked.[25]

Regarding illegal money transfers related to internet banking in 2021, it is believed that most of the damage was "business email compromise," a method by which criminals use e-mail or SMS to disguise themselves as FIs or delivery companies and lead people to phishing sites.

In addition, there have been numerous incidents of attacks that exploit vulnerabilities in software and systems, as well as targeted email attacks that infect various types of ransomware. The seriousness of the damage caused by ransomware and the maliciousness of the methods have become a global problem. In Japan as well, there have been confirmed cases of victims of double extortion in which corporate systems have been infected with ransomware, resulting in the theft of personal information, encryption, and threats to pay ransom in exchange for not disclosing the information. The number of domestic ransomware cases reported to the National Police Agency in 2021 was 146, a steady increase from the previous year. The damage is widespread regardless of the size of companies and organizations and their type of business. In addition, as with the rapid increase in external connections to internal networks due to work from home, an increasing number of companies are introducing VPN devices as part of their security measures, and the majority of the damage is caused by the *modus operandi* in which the vulnerability of VPN devices is used to infiltrate networks within the organization and infect them with ransomware.[26]

[25] National Police Agency, "Threats in Cyberspace in 2021 (Preliminary Version)"; published in Japanese only, For English information, refer to their full report of year 2021.
[26] Ibid.

(6) Fraud cases such as specialized fraud

In recent years, there have been many cases of specialized fraud in Japan. Specialized fraud crime groups systematically commit fraud by skillfully misusing various tools, such as deposit and savings accounts, mobile phones, and cell forwarding services, with the ringleader playing a central role and assigning a role to each member, such as one-member cheats victims, another withdraws money, and the other procures tools to commit the crime. They also commit ML by using accounts in fictitious or other people‘s names for the transfer of fraudulent money. In addition, there are people who thoughtlessly sell accounts in their own name or accounts in fictitious or other people’s names opened by using falsified identifications for amusement or living expenses, making it even easier to commit ML.

The government has established procedures to pay benefits for damage recovery for victims under the Act on Damage Recovery Benefit Distributed from Funds in Bank Accounts Used for Crimes (“Criminal Accounts Damage Recovery Act”). In addition, each ministry and agency has been promoting various measures to eliminate specialized fraud, etc. in cooperation with local governments, various organizations, private business operators, etc., based on the “‘It’s me!’ phone call scam countermeasure plan” decided in 2019 as a comprehensive measure to protect the elderly from specialized fraud, etc. However, the damage continues.

In particular, although the amount of damage caused by specialized fraud in 2021 decreased from the previous year, the number of recognized cases increased, indicating that the amount of damage posed is still high, mainly among the elderly, and the situation is serious. In particular, there was an increase in the number of specialized fraud cases in which victims were made to use ATMs under the guise of overpayment of medical expenses and insurance premiums by pretending to be local government employees, etc., and were made to transfer cash to the criminals‘ account. Among them, medical expenses and health insurance and social insurance expenses have significantly increased. As in the previous year, the amount of damage caused by specialized fraud related to COVID-19 was around 110 million yen.

Cases of side business fraud other than specialized fraud have also been found. For example, there are cases of setting up a website for mediation of a side business

on the Internet, and having the person who applied for mediation of the side business pay money for the purported reason of necessary expenses, etc.

According to the Consumer Affairs Agency, there have been numerous consultations with Consumer Affairs Centers around Japan. For example, there are cases where, triggered by a message introducing a side business through a messaging app, consumers pay around 10,000 yen at the beginning to participate in the business, and then are persistently solicited over the phone to buy expensive information for commercial use that they cannot refuse. As a result of an investigation conducted by the Consumer Affairs Agency concerning these consultations, it was confirmed that several business operators acted in concert with each other, which was likely to unreasonably harm the interests of consumers (false advertisement, representation, and misstatement). In accordance with the provision of Article 38, Paragraph 1 of the Consumer Safety Act, the Consumer Affairs Agency publishes information that contributes to the prevention of occurrence or spread of harm to consumers and calls for consumers' attention.[27]

Banks, etc. are encouraged to impose restrictions on ATM withdrawals and transfers in accordance with the actual situation of damage, to address elderly people at places where ATMs are installed, and to promote efforts to convey the message, "Do not make or receive mobile phone calls at an ATM." Also banks, etc. are required to investigate and consider submitting suspicious transaction reports as necessary when unusual patterns of funds transfer, such as those described above, which are different from patterns of funds transfer in the past, are detected.

(7) Terrorist financing risk

The situation surrounding international terrorism continues to show no prospects for improvement, as terrorist incidents have occurred in many parts of the world, including in Western countries, and the Taliban declared the establishment of a government in Afghanistan in August 2021.

Japan is taking measures in accordance with various related laws, including the Act on Punishment of Organized Crime, and at this time, there are no Japanese nationals or residents of Japan who are subject to such measures as asset freezes in response to the UNSC resolution. In addition, no terrorist designated by the UNSC

[27] Consumer Affairs Agency, "Attention regarding the four business operators that first make consumers pay around 10,000 yen to purchase information for commercial use, and then make them purchase extremely expensive information materials through persistent telephone solicitation."(March 18, 2020)

has been confirmed in Japan. In the past, however, it has been revealed that people who were on an international wanted list through Interpol for crimes such as murder and attempted bombing terrorism repeatedly entered and departed from Japan illegally. This indicates that a network of Islamic extremist groups loosely connected through extremist ideology extends to Japan. In addition, there are persons in Japan who support ISIL and who sympathize with ISIL's propaganda, and persons suspected of having attempted to travel to Syria to join ISIL as combatants are identified.[28]

In addition, the FATF report[29] published in 2019 pointed out that "Nevertheless, in light of the cross-border nature of TF, a jurisdiction that faces a low terrorism risk may still face significant TF risks. A low terrorism risk implies that terrorist individuals and groups are not using funds domestically for terrorist attacks. However, actors may still exploit vulnerabilities to raise or store funds or other assets domestically, or to move funds or other assets through the jurisdiction." In Japan, it is also necessary to fully consider the risk of terrorist financing, and the use of funds via Japan for terrorist activities overseas should not be allowed.

In fact, the 2021 4th round of Mutual Evaluation Report of Japan issued by the FATF pointed out that Japan has not conducted targeted outreach to NPOs and that Japanese NPOs are at risk of being unwittingly involved in terrorist financing activities.

It is also important for FIs to routinely accumulate and analyze information on recent global developments and countries/regions and transactions with a high risk of terrorist financing. In cases where an NPO opens a bank account, it is important to identify and assess risks based on the region or entity that is conducting or supporting cross-border wire transfers, and to take continuous and preventive measures against terrorist financing risks.

As measures related to the financing of terrorism, in addition to the enforcement of the Act on Punishment of Financing to Offences of Public Intimidation, Japan has implemented measures, such as freezing the assets of parties related to the Taliban, ISIL, and Al-Qaida in accordance with the UNSC Resolution. These measures are implemented in accordance with the Foreign Exchange and Foreign Trade Act ("FEFTA") and the International Terrorist Asset Freeze Act.[30]

FSA's Guidelines for Anti-Money Laundering and Combating the Financing of

---

[28] 2021 The NRA page 54

[29] FATF Terrorist Financing Risk Assessment Guidance (July 2019)

[30] Amended Act on Special Measures Concerning Asset Freezing, etc. of International Terrorists Conducted by Japan Taking into Consideration UNSC Resolution 1267, etc.

Terrorism ("Guidelines"), in light of international standards, such as the FATF, requires a financial institution to update its sanctions list without delay and compare the names of customers, etc. with its sanctions list, even before the issuance of the Ministry of Foreign Affairs Notice pertaining to the designation of those subject to sanctions, if those subject to sanctions are added or if the information of those subject to sanctions is changed by the UNSC Resolution. In addition, the Guidelines require that, when a customer, etc. who falls under the sanctions list is recognized, appropriate and careful handling is required, such as conducting more rigorous CDD and determining whether the customer is a person with the same name as that on the list or not. Therefore, it is important to develop databases and systems, secure human resources, and secure funds necessary to ensure that such measures are implemented in accordance with the risks faced.

Column [Money Laundering related to illegal trade of wild fauna and flora]

Given the increasing global interest in the environment in recent years, the FATF published "Money Laundering and the Illegal Wildlife Trade" in June 2020 and "Money Laundering from Environmental Crime" in June 2021 with the aim of raising awareness of the flow of funds and laundering methods that encourage environmental crime.[31]

According to National Police Agency, although there have been no ML cases related to illegal wildlife trade in Japan, there have actually been cases related to the smuggling of wild animals and plants in Japan.

- A case in which a living Asian short-clawed otter was hidden in a Boston bag and imported from Thailand without obtaining necessary permission
- An attempt to export ivory, etc. to Laos by hiding it in a suitcase, etc. without obtaining necessary permission
- A case of marketing ivory stamps on an internet auction site without obtaining necessary registration and selling them to customers

In line with the discussion on the FATF and international society, it is necessary for Japan to recognize environmental crime as a risk and address it. It is also necessary to take ML risks into account when dealing with internationally scarce wild fauna and flora or their products. Similar to the precautions for dealing with remittances related to trade settlements, FIs should be aware of risk-based measures, such as identifying and assessing risks by checking the occupation and business of customers, the destination of remittances, whether there is anything unusual in the underlying commercial transactions, and whether

[31] These reports can be found below.
http://www.fatf-gafi.org/publications/environmentalcrime/environmental-crime.html?hf=10&b=0&s=desc(fatf_releasedate)

the goods traded are wild animals, rare animals, or ivory, and conducting further in-depth investigations depending on the risks when necessary.

(8) Geopolitical risks (including Proliferation Financing risks related to weapons of mass destruction)

In addition to ML/TF, it is also necessary to take adequate measures against risks related to PF, provision of funds for activities related to the production, acquisition, and transportation of nuclear weapons and other weapons of mass destruction). With regard to PF, economic sanctions, such as asset freeze, are being implemented against those who are involved in activities related to weapons of mass destruction as designated by the UNSC Resolutions as well as against terrorists. When a UNSC Notice is issued with respect to those subject to economic sanctions that are designated by the Sanctions Committee established by the Ministry of Foreign Affairs Resolution, it is necessary to immediately confirm that there are no transactions with those subject to economic sanctions, and if there are any transactions, it is necessary to take measures, such as freezing of assets.

As is the case with CFT, FIs need to ensure that they comply with economic sanctions related to PF, for example, by updating their sanctions lists without delay after their release and implementing stricter CDD.

On February 21, 2022, Russian President Putin signed a presidential decree authorizing the "independence" of the Donetsk People's Republic and the Luhansk People's Republic. On February 24, the Russian military commenced military operations against Ukraine. This invasion by the Russian military is a violation of the sovereignty and territorial integrity of Ukraine, a serious violation of international laws prohibiting the use of force, and a serious violation of the U.N. Charter. It also undermines the very foundation of the international order, which prohibits the unilateral change of the status quo by force. Japan has been taking various measures, including freezing of assets, since February 25 in order to respond in full solidarity with the G7 and other members of the international community.

Concerns about the invasion of Ukraine by the Russian military are not limited to G7 countries. On the last day of the FATF General Assembly held on March 1-4, 2022, the FATF Public Statement on the Situation in Ukraine was adopted and published.[32]

[32] On 4 March 2022, FATF Chairman's Summary: "FATF Members discussed the evolution of the tragic events and loss of life in Ukraine and issued a statement expressing the FATF's significant concerns about the risk situation regarding Money Laundering, terrorist financing

The key points of the statement are as follows:

- The FATF expresses its grave concern about the invasion's impact on the ML/TF/PF risk environment as well as the integrity of the financial system, the broader economy and safety and security.
- The FATF is reviewing Russia's role at the FATF and will consider what future steps are necessary to uphold these core values.
- The FATF further notes that malicious cyber activity targeting FIs and systems could jeopardize the ability of the private sector and competent authorities to implement and monitor core AML/CFT/CPF controls. The FATF reiterates the upmost importance of ensuring NPOs, and that all other humanitarian actors can provide the vital humanitarian assistance needed in the region and elsewhere, without delay, disruption or discouragement.
- The FATF calls on all jurisdictions' competent authorities to provide advice and facilitate information sharing with their private sectors on assessing and mitigating any emerging ML/TF/PF risks identified, including in relation to virtual assets, as well as other threats to international safety and security from the region. The FATF notes that all jurisdictions should be vigilant to the possibility of emerging risks from circumvention of measures taken in order to protect the international financial system from the ML/TF/PF risks resulting from Russia's aggression against Ukraine.

In Japan, financial sanctions, such as asset freeze, are implemented in accordance with FEFTA payment regulations and capital transaction regulations. In FEFTA, FIs are prohibited from making cross-border wire transfer, etc. of their customers until they have confirmed that such cross-border wire transfer, etc. does not fall under such regulations. In light of the current international situation surrounding the Russian invasion of Ukraine, based on a Cabinet understanding,[33] the Government

---

and Proliferation Financing, and the impact of the Russian invasion on the integrity of the financial system, the broader economy and security."
https://www.fatf-gafi.org/publications/fatfgeneral/documents/outcomes-fatf-plenary-march-2022.html

[33] The Cabinet Approval "On measures such as freezing of assets of persons related to the "Donetsk People's Republic" (self-proclaimed) and the "Luhansk People's Republic" (self-proclaimed) and designated banks of the Russian Federation, prohibition of imports and exports to and from the two "republics" (self-proclaimed), prohibition of issuance and circulation of new securities by the government and other government agencies of the Russian Federation, prohibition of issuance and circulation of securities in Japan by designated banks, and prohibition of export of items subject to the international export control regime to the Russian Federation" (dated February 26), etc.

of Japan requests that FIs comply with various obligations under the various economic sanctions under FEFTA. It is natural for FIs that conduct cross-border wire transfer, etc. by themselves or through other FIs to take necessary measures, such as checking with the sanction lists of related countries, etc., in accordance with the domestic and foreign laws and regulations on cross-border wire transfer, etc., such as FEFTA. As in AML/CFT/CPF, FIs need to ensure that they are prepared to respond to sanctions on a daily basis and to take necessary measures immediately in the event that sanctions are imposed.

FEFTA's payment regulations apply to all types of sanctioned persons, including crypto-assets. For the purpose of ensuring Crypto-asset Exchange Service's proper and reliable implementation, FSA and Ministry of Finance requested CESPs on March 14, 2022, to refrain from transferring crypto-assets if it determines that the address of a beneficiary designated by a customer is the address of a person subject to measures such as asset freeze, taking into account that FEFTA's payment permission obligations are imposed on the customer.

(Provisional translation)

Response to the current international situation concerning Ukraine (Request)

令和４年３月１４日

暗号資産交換業者 各位

金融庁総合政策局長
松尾　元信
財務省国際局長
三村　淳

ウクライナをめぐる現下の国際情勢を踏まえた対応について（要請）

○　我が国は、ウクライナをめぐる現下の国際情勢に鑑み、国際的な平和及び安全の維持を図るとともに、この問題の解決を目指す国際平和のための国際的な努力に我が国として寄与するため、主要国が講ずることとした措置の内容等を踏まえ、閣議了解(注1)を行い、これに基づき、外国為替及び外国貿易法（以下、「外為法」という。）による支払規制を含めた諸般の措置を実施している。

財務省は、令和２年10月20日、外為法の解釈運用通達を改正し、外為法第16条第１項に規定する支払等には、暗号資産の移転を含むことを明確化しており、外為法に基づく資産凍結等の措置の対象者として外務省告示により指定された者（以下、資産凍結等の措置の対象者という。）に対する暗号資産の移転に係る支払も支払規制の対象とされている。

（注１）　閣議了解「「ドネツク人民共和国」（自称）及び「ルハンスク人民共和国」（自称）関係者並びにロシア連邦の特定銀行に対する資産凍結等の措置、両「共和国」（自称）との間の輸出入の禁止措置、ロシア連邦の政府その他政府機関等による新規の証券の発行・流通等の禁止措置、特定銀行による我が国における証券の発行等の禁止措置並びに国際輸出管理レジームの対象品目のロシア連邦向け輸出の禁止等に関する措置について」（２月26日付）など

（財務省ホームページ）
https://www.mof.go.jp/policy/international_policy/gaitame_kawase/gaitame/economic_sanctions/recent.html#ukraine

○　暗号資産交換業者においては、この趣旨を踏まえ、暗号資産交換業の適正かつ確実な遂行を確保する観点から、以下の措置を実施していただきたい。なお、その実施に当たっては、別紙についても留意いただきたい。

記

①　顧客が指定する受取人のアドレスが資産凍結等の措置の対象者のアドレスであると判断した場合には、顧客に外為法の支払許可義務が課されていることを踏まえ、暗号資産の移転を行わないこと。顧客が指定する受取人のアドレスが資産凍結等の措置の対象者のアドレスである疑いがあると判断した場合には、資産凍結等の措置の対象者のアドレスでないことを確認した後でなければ、暗号資産の移転を行わないこと。

（注２）　暗号資産交換業者が取引の相手方として資産凍結等の措置の対象者と暗号資産の売買等の暗号資産に係る取引を行う場合、それに伴って暗号資産の移転や金銭の支払があれば、（帳簿残高の付替えであっても）当該移転は外為法上の支払に該当することに留意すること。

②　顧客から依頼を受けて暗号資産を移転した場合であって、暗号資産の移転先が資産凍結等の措置の対象者であることが判明したときは、金融庁、財務省等に速やかに報告すること。

③　上記①②の措置の実効性を高めるため、暗号資産に係る取引について、モニタリングを強化すること

（注３）　資産凍結等の措置の対象者を相手方とする取引でなくとも、資産凍結等の措置の対象者の関与が疑われる取引については、金融庁で公表している「疑わしい取引の参考事例（暗号資産交換業者）」を参照して、速やかに疑わしい取引の届出を行うこと。

以上

With regard to the situation in Ukraine, it is impossible to predict how it will develop in the future. FSA, however, continues to cooperate with the relevant authorities and industry associations to take risk-based measures, taking into account the impact on ML/TF risks.

Chapter 2. Current Status and Challenges of ML/TF Risk Management at FIs

1. Overall trends and issues common to all sectors (overall trends based on analysis of data reported by FIs)

Based on quantitative and qualitative information collected from FIs, FSA identifies and assesses the risks associated with the ML/TF of each sector and FIs. It then conducts monitoring through inspections and interviews of FIs in accordance with the risks.

Chapter 2 summarizes the current AML/CFT/CPF situation and challenges at FIs observed through these monitoring exercises.

As an overall trend common to all sectors, since the Guidelines were published by the FSA in February 2018, many FIs have begun to make an effort to upgrade their internal control, and progress has been seen in developing their verification system, including those at sales sites. In addition, FSA is promoting the use of transaction monitoring systems that use thresholds based on Ongoing CDD and risks, and transaction screening systems to verify lists of persons subject to sanctions, as well as the implementation of comprehensive and specific risk identification, and assessment and consideration of ongoing CDD based on those risks identified. In addition, regional banks, shinkin banks, and credit cooperatives are promoting the introduction of transaction monitoring/screening systems by the joint centers of their associations.

FSA revised the Guidelines for the second time in February 2021 and published Frequently Asked Questions Regarding the Guidelines[34] ("FAQ") in March of the same year to clarify the contents of "Required actions for a financial institution" of the Guidelines. Given that three years have passed since the formulation and publication of the Guidelines and that FIs are increasingly aware of the need to develop AML/CFT/CPF systems, in April 2021, the Government of Japan requested that the "Required actions for a financial institution" of the Guidelines be completed by the end of March 2024 and that AML/CFT/CPF systems be developed.

FIs have been gradually improving their risk management framework with a

[34] "Frequently Asked Questions Regarding "Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism"
https://www.fsa.go.jp/news/r2/2021_amlcft_faq/2021_amlcft_guidelines_FAQ.pdf

target of the end of March 2024, and its overall level is considered to be upgraded, however, some of them are lagging behind in their actual actions as it takes time to identify and assess comprehensive and concrete risks and to prepare action plans for enhancing their management framework. For example, the responses required by the Guidelines and FAQs are not reflected in the FIs' policies and procedures, including manuals, and some FIs are not adequately developing their control framework on a risk-based approach as not being systematically and continuously addressed.

Some FIs have outsourced verification at the time of transactions and part of CDD to agents. Even in such cases, the outsourcer FIs need to take actions in accordance with their legal obligations related to CDD. For example, it is necessary to be involved as an outsourcer through timely and appropriate verification of information necessary for CDD, and to manage CDD, record keeping, and other operations by agents. Although it is small number, however, there have been cases where outsourcer FIs do not take any action relying on an outsourcing contractor and the outsourcing contractor has not taken inadequate measures, either. Therefore, FSA requests improvements in individual inspections and interviews.

The analysis of quantitative and qualitative information collected from FIs has also revealed that a wide range of FIs are building and enhancing their AML/CFT/CPF framework.

It is also observed that FIs are identifying and assessing risks to a certain extent while referring to the NRA. This indicates that the financial sector as a whole is improving its risk understanding and other frameworks, regardless of sector type or size.

On the other hand, with regard to basic matters, such as the preparation of regulations, including risk assessment sheets and customer acceptance policies, implementation of customer risk assessments, and introduction of transaction monitoring and screening systems, even FIs that have established such basic matters are found to have insufficient control environments through actual inspections and interviews. For example, processes for risk identification and assessment have not been documented or specified by policies and procedures with internal approval. Therefore, further actions are required.

Through inspections and interviews, FSA will continue to examine the accuracy of the gap analysis for initiatives designated as "Required actions for a financial

institution" in the Guidelines and the progress of the Action Plan for completing the development of control framework by March 2024, in order to encourage FIs to enhance their risk-based initiatives.

2. Outline of risks and current status and issues by business sectors

(1) Deposit-taking financial institutions

A. Outline of the risks of the deposit-taking financial institution;

Deposit-taking Financial Institutions ("DFIs") provide a wide range of products and services, including cash transactions that are considered to have a high risk of being misused ML/TF; transactions of deposits that enable them to promptly and easily reserve or store funds on hand; exchange transactions that enable funds to be moved safely and promptly between remote areas or a large number of people; safe-deposit boxes that enable assets to be stored highly confidentially; and bills and checks that are highly liquid, transportable, and tradable, as well as other related services.

The ML/TF risk of DFIs as a type of FIs is relatively higher than that of other types of FIs given the ML/TF risk associated with the above mentioned characteristics of these products and services, the possibility that transactions may become more complex, the difficulty of tracking the flow of funds if they are combined, and the size of transactions in the sector as a whole.

B. Current Status and Challenges of DFIs[35]

(a) Risk Identification and Assessment

Risk identification is a process to identify ML/TF risks faced by a DFI through comprehensive and specific risk evaluation of the products and services offered, transaction types, countries and geographic areas of transactions, customer attributes, and other relevant factors, and is the starting point of a risk-based approach. It is necessary for FIs not only to comprehensively examine all the items listed in the NRA, but also to identify their own risks by examining each individual product and service one by one, taking into account the geographic attributes of its business area, business environment and management strategy,

[35] Excluding the three mega-bank groups described in Chapter 2. 2 (1) "Mega-Bank Group: Current Status and Issues" below.

and so forth (the same applies to transaction types, countries and geographic areas of transactions, customer attributes, and so forth.).

In addition, risk assessment is a process to evaluate the degree of impact of identified ML/TF risks on DFIs and form a foundation of specific countermeasures, such as mitigation measures, and is the basis for a risk-based approach. In conducting risk assessment, it is necessary to take into account the results of examination of transaction volume (value, number of transactions and so forth); probability and impact; and its own business environment, management strategy and risk profile. In addition, it is required to utilize the results of STR (suspicious transaction report) analysis not only for reviewing customer risk assessments but also for reviewing risk identification and assessment by categorizing and analyzing trends of STRs on the basis of factors such as products and services; transaction types; countries and geographic areas; customer attributes; reasons for reporting; and background of detection. From the perspective of comprehensive risk assessment, it is useful for DFIs which have customers who deal with foreign countries and foreign resident customers to prepare in advance a country risk assessment list for at least all countries and regions with which Japan has diplomatic relations.[36]

DFIs are required to take effective measures based on a risk-based approach in order to appropriately identify and assess ML/TF risks by themselves and to flexibly establish and develop a risk management framework that is commensurate with these risks by setting priorities. However, FSA found that some DFIs had not developed a basic risk management framework including internal rules, specifically "procedures for risk identification and assessment that form the basis of a risk-based approach have not been documented," "actions taken are mainly for compliance of laws and regulations and a system for taking mitigation measures commensurate with risks has not been developed" and "AML/CFT policies, procedures and programs, and the risk management framework based on them have not been reviewed periodically or on an ad hoc basis." In addition, the following cases were recognized:

[Cases where delays in actions were recognized]

[36] Country risk assessment may be based on information from the NRA, the FATF Grey List, the Corruption Index published by international NGOs and the Basel AML Index, as well as sanctioned countries by the U.S. Ministry of Finance and the EU, and past STR of FIs.

- Some DFIs use a template for risk assessment sheets provided by industry associations and only list the cases described in the NRA, and do not identify their own risks based on their size and characteristics, such as trends and analyses of STRs, analyses of accounts requested to be frozen from the police, and damage from financial crime.
- Some DFIs only refer to descriptions on a category of FI that they belong to in the NRA and do not consider descriptions on the risks of customers.
- Some DFIs do not identify or assess risks associated with products and services through non-face-to-face transactions, and do not comprehensively assess risks associated with all products and services.
- In some DFIs, despite being aware of the risks associated with some of the products and services it provides, it judged that these risks would not materialize, and it did not identify and assess the risks or consider risk-based response policies.
- Some DFIs do not assess risks taking into account their specific and concrete characteristics based on trend analysis of financial crime that targeted their customers, STRs and so forth.
- Some DFIs do not comprehensively identify "countries and regions" that may be directly or indirectly traded or countries with diplomatic relations with Japan and North Korea (196 countries).
- Some DFIs only update their existing risk assessment report and have not developed documented procedures for development of the report, such as who or what data or materials should be referred to, and how to identify and assess risks.

(b) Ongoing CDD

With respect to CDD, the core element of risk mitigation measures, ongoing risk-based CDD is especially important. As a series of ongoing CDD, DFIs are required to conduct customer risk assessment for all customers, review the customer risk assessment based on customer information updated with frequency commensurate with the risk, and then implement risk mitigation measures commensurate with the risk.

In implementing ongoing CDD, it is important for DFIs to develop medium-to long-term action plans based on risk assessment of all of their customers, and to steadily and carefully implement measures while managing the progress.

However, FSA recognizes that some FIs are lagging behind in their actions. In the revised FAQ published in March 2022, the FSA clarified points to note regarding the concept of "simplified due diligence" (SDD). In addition to inspections and supervision, FSA will continue to encourage FIs to develop an ongoing CDD framework including customer information update through various outreach activities, such as opinion exchanges and training/study sessions, and shares reference cases of risk-based CDD measures through industry associations.

[Cases where delays in actions were recognized]

- Some DFIs do not develop a plan for ongoing CDD including the frequency and specific methods of conducting surveys according to the level of customer risks.
- Regarding the ongoing CDD implementation plan, the start date of the project has been pushed back and it is not planned to be completed by the end of March 2024.
- Some DFIs manage customers on whom STRs were submitted as high-risk customers, but for other customers do not assess the risk of each individual customer and then do not manage them based on their risks.
- Regarding information update of existing customers, some DFIs consider only to send and collect questionnaires by postal mail and do not consider other methods, despite the low collection rate of postal mail.
- Some DFIs have not developed rules or documents on procedures of how to detect events that effect customers' risk and to review risk assessment, despite the fact that they have procedures to review risk assessment at a frequency commensurate with customer risk.

[Examples of advanced approaches taken]

- Regarding information update of existing customers, some DFIs assign provisional ratings to all customers based on attribute information already obtained, products and services used, transaction types and so forth. They have started to update information on high-risk customers and review their risks in the first place and are going to update information on medium-risk and low-risk customers in sequence.
- Regarding customers whose information is insufficient for customer

risk assessment, some DFIs have developed procedures for information collection, and identify and collect their information at a frequency commensurate with their risk. When collecting information, they consider and implement methods for information collection taking into account requests from FSA, such as referring to FAQs.

- When identifying actual situations of customers, some DFIs not only send questionnaires but also request cooperation from customers and collect information through multiple channels, such as asking customers when they visit the counter, visiting customers, displaying a notice on the internet banking screen, having call center representatives make phone calls, and printing a notice on bank statements when customers use ATMs.
- When identifying actual situations of customers, some DFIs identify customers to whom SDD will be applied by referring to the FAQs, and also efficiently review risk assessment by identifying customers with a very low risk of being used for ML/TF, such as customers whose accounts have not been active for more than a year and accounts linked to local governments.
- Some DFIs consider methods to identify the actual situation of customers when postal mail prohibited from being forwarded is returned (such as customers who have not submitted a notice of change of address despite moving from the address they declared for verification at the time of transaction), such as making a phone call, sending an e-mail, and so forth.
- Some DFIs request cooperation from customers and collect information at the counter, which is more reliable, in response to complaints from customers who suspect that questionnaires sent by postal mail are a new type of fraud.
- Some DFIs understand that identifying the actual situation of customers and KYC (Know Your Customer) literally mean to understand the actual situation of customers and understand that they should be conducted not only for AML/CFT/CPF but also as elementary actions of service business, and their management takes the lead in implementing ongoing CDD.
- Some DFIs have increased the response rate of questionnaires by enclosing a flyer prepared jointly by industry associations and FSA that

requests understanding of AML/CFT/CPF measures with the questionnaire for information update.

(c) Transaction monitoring and filtering

Transaction monitoring and filtering are ways to ensure the effectiveness of risk mitigation measures, focusing on the transactions to reduce risks through analysis of the actual transactions and the detection of unusual transactions and ones subject to sanctions. Transaction monitoring detects unusual transactions ex-post facto in order to submit STRs generally by employees or a system. It is important for the system detection to improve monitoring methods by verifying and analyzing the effectiveness of rules for pattern analysis and scenario, and to continuously identify more effective transaction patterns and monitoring methods, taking the false-positive rate into account. Also, DFIs should take note that transactions which should be detected may be missed when they adjust monitoring methods only intending to reduce the false-positive rate of the monitoring system. The important point is to review scenarios which frequently detect transactions which are obviously false-positives. It is also important for DFIs to enhance the detection abilities of employees of the 1st line who face customers by effectively notifying them of the "Reference Cases on Suspicious Transactions"[37] published by FSA in a timely manner and analyzing the STRs they submitted.

Transaction filtering is a way to detect prohibited transactions, such as transactions with sanctioned individuals, before executing transactions by employees or the system. For transaction monitoring, DFIs are required to adequately set ambiguous search features, take necessary measures without delay when economic sanctions are designated by the UNSC Resolutions (such as developing a framework to screen customers in 24 hours after the resolution) and so forth.

However, the following cases are recognized in some DFIs, and therefore, FSA periodically exchanges opinions with system vendors and encourages DFIs to develop a transaction monitoring/filtering framework through inspections and supervision as well as various outreach activities.

[37] https://www.fsa.go.jp/str/jirei/en_reference_cases.pdf

[Cases where delays in actions were recognized]

- Some DFIs have not changed scenarios or detection rules of transaction monitoring from the initial setting and do not review scenarios or set thresholds commensurate with their risks.
- Some DFIs have not developed procedures to report suspicious transactions to the division in charge, and decisions whether to submit STRs are left to the discretion of each office, despite suspicious transactions being detected by employees.
- Some DFIs do not analyze trends of crimes in the geographic areas in which they operate, STRs submitted and so forth.
- Some DFIs analyze trends of crime in geographic areas in which they operate, STRs submitted and so forth, but cannot sufficiently lead the results to improvement of the detection framework, such as reviewing monitoring methods of the transaction monitoring system and ensuring consistency of decisions on whether to submit STRs.
- Regarding legal entity customers with accounts, some DFIs do not screen their representatives or beneficial owners by transaction filtering when they do not have accounts.
- When malfunction of the transaction screening system occurred, some DFIs screened transactions by employees, but executed some transactions without screening.
- Some DFIs had prepared an alternative system in case of system trouble, but they could not activate it because they had not taken a dry run.
- When a sanction list was updated, some DFIs screened their existing customers by overnight batch processing but did not complete it 24 hours after the update.
- Some DFIs only check sanctioned countries and do not verify whether to correspond with major harbors or the address of offshore centers.
- Some DFIs do not adequately set the ambiguous search features to be able to detect multiple options by a transaction filtering system despite the multiple spellings of names of sanctioned individuals or geographical areas due to customs or conversion to the English alphabet from non-English names.
- Regarding the ambiguous search features of transaction screening, some DFIs leave the settings to their vendor and do not verify the

features.

(d) Suspicious transaction reporting

Regarding suspicious transaction reporting, it is important not only to fulfill the obligations set forth in the APTCP, but also to analyze the trends and status of the content of STRs and to make use of the results to strengthen DFIs' own ML/TF risk management. In particular, it is important for DFIs to understand the actual situations, commercial flows, and transaction types of customers according to their risks on a daily basis in order to promptly investigate, analyze and determine whether to submit STRs after detecting transactions as candidates for STRs by employees or the system. When analyzing transactions for which STRs have been submitted, it is important to extract information that can be reflected in DFIs' own risk assessment and verification of the appropriateness of scenarios and thresholds of transaction monitoring in addition to trend analysis, and to make use of them to improve the effectiveness of the risk management framework as necessary. It is also useful to examine the detected transactions for which an STR was not issued in internal audits in order to verify whether the decisions were appropriate.

FSA will continue to promote the development of a framework STR by holding training sessions jointly with National Police Agency and publishing and revising the "Reference Cases on Suspicious Transactions".

[Cases where delays in actions were recognized]

- Some DFIs determine not to submit STRs without sufficient consideration of the necessity of STRs because the factors to be taken into account and criteria for STRs are not specified in the internal rules.
- Some DFIs do not analyze the content and trends of STRs or make use of them to identify and assess the risks of customers and products/services, although they aggregate the number of submitted STRs by type.
- Some DFIs downgrade detections by employees and do not hold training for their employees on the "Reference Cases on Suspicious Transactions." Also, some DFIs determine not to submit transactions detected by employees as STRs at the branches and do not keep their records.

- It takes a long time to submit STRs in some DFIs due to a lack of time and data management from detection to decision and from decision to submission. Also, some DFIs submit STRs once a month rather than in each case.

[Examples of advanced approaches taken]

- Some DFIs reduce the false-positive rate to around 70% by making efforts to decrease the rate, such as periodic verification of monitoring system scenarios.
- Some DFIs make efforts at streamlining and improving the effectiveness of investigations by introducing supervised machine learning using past submissions as a training dataset or RPA.
- Some DFIs review the risk rating of customers for whom STRs have been submitted.
- Some DFIs periodically verify the effectiveness of the transaction monitoring system by outsourcing it to independent external consultants.
- Some DFIs take mitigation measures, such as the monitoring of accounts opened with only a small amount; the identification of whether funds are transferred during a specific period of time after account opening or registered mobile phone numbers are used; and notification, upon account opening, provided to customers stating that account selling is a crime, taking into account the analysis of STRs.
- Some DFIs analyze the "Reference Cases on Suspicious Transactions" published by JAFIC/FSA and the STRs they submitted, and report the trends of and controls for suspicious transactions to the board and the 1st line employees at the meetings with employees of branches and so forth, and then make use of the results in considerations and decision making when similar cases occur.
- Some DFIs keep records on transactions which were detected by employees or the system but were not submitted based on an investigation, and the internal audit divisions independently verify the effectiveness of their framework for STRs by sample investigation and analysis.

(e) Involvement and understanding of management

AML/CFT/CPF is regarded as a management issue. It is necessary to establish a cross-organizational framework under the responsibility of the board to strategically secure human resources, educate them, and allocate resources. In addition, it is necessary to establish a risk management framework by appropriately sharing necessary information with directors in charge in a timely manner and ensuring cooperation between management and divisions in charge.

However, while some DFIs are making efforts to improve their AML/CFT/CPF measures across their organizations under the strong leadership of the board, the following examples are recognized at some DFIs.

[Cases where leadership of management was not recognized]

- Management only receives reports on the status of AML/CFT/CPF measures taken from divisions in charge and does not sufficiently take leadership in establishing an AML/CFT/CPF risk management framework, for example the management does not order the development of an action plan to reduce the gap recognized from gap analysis.
- Management does not fully understand that the AML/CFT/CPF is an important management issue. In addition, management receives reports on the progress of the AML/CFT/CPF action plan quarterly, but does not order the division in charge to analyze the reasons why the plan did not go as planned and, therefore, the progress is not appropriately managed.
- Management does not appropriately implement allocation of human resources, which is the most expected leadership action of the board, for example, the board appoints persons who do not have sufficient knowledge both on the applicable laws, regulations and the Guidelines and on the internal procedures as managers of divisions in charge of AML/CFT/CPF or do not allocate sufficient employees.

C. Mega-Bank Group: Current Status and Issues

In May 2018, FSA issued a notice to the three mega-bank groups (“three mega-banks”) on actions required on a group/global basis for ML/FT risk

management ("benchmarks")[38] taking into account the roles expected of the G-SIBs. FSA asks for gap analysis between the benchmarks and the current status and formulation of concrete action plans to eliminate the gap, and monitors the progress through regular interviews. In addition, in February 2021, FSA published the revised Guidelines incorporating the benchmarks, and in March 2021, it published the FAQ. Since then, FSA has conducted interviews on the status of the development of the control framework in line with these as part of its year-round inspections.

The three mega-banks seems to have made progress in the development of their control frameworks regarding the "required actions" and "expected actions" of the Guidelines, as seen in the fact that they have implemented or that they are proceeding with their responses after formulating concrete action plans.

In addition to the above-mentioned efforts, the following examples of advanced approaches taken and issues that the three mega-banks need to steadily address are recognized.

(a) Risk Identification and Assessment

When assessing risks associated with new products and services, the Guidelines revised in February 2021 require comprehensive and specific evaluation of risks associated with such products and services, including the effectiveness of the risk control framework of alliance partners, collaboration partners, outsourcing contractor, and acquired companies. The three mega-banks have assessed risks associated with new products and services prior to their initiation, and now they are expanding their efforts to develop a framework to evaluate the risks of their alliance partners, collaboration partners, outsourcing contractor, and acquired companies. Information about business partnerships and M&As is highly confidential because it may affect stock prices and, therefore, discussions on them are usually conducted mainly by a planning division under the control of information within the organization, meanwhile, the risk control framework of counterparties may also affect business strategies after the alliance, fair price for acquisition and reputation risk, so it is desirable to evaluate risks of the alliance partners and so forth at the earliest possible

[38] The Guidelines are not limited to the items stipulated in the Guidelines, but are based on global standards regarding AML/CFT.

opportunity, giving sufficient consideration to confidentiality.

[Examples of advanced approaches taken]

- When planning new products and services, the division in charge of AML/CFT/CPF participates in the discussion at an early stage, and the ML/TF risks associated with new products and services, including the risk control framework of alliance partners, collaboration partners, outsourcing contractor are taken into account.
- When considering the acquisition of foreign FIs and so forth, the appropriateness of the acquisition is being considered in light of the AML/CTF framework of the acquiring entities.

In addition, when assessing the risk of customers who are expanding their import/export business and overseas operations and the risk of cross-border wire transfer associated with trade finance, it is necessary to assess the risks taking into account risks of the countries and geographic area with which direct and indirect transaction relationships are possible and risks of commercial flows of the customers. And also, regarding the foreign subsidiaries and so forth (including joint ventures with local companies) of the above-mentioned customers, it is necessary to consider risks of the countries and geographic areas where the subsidiaries and so forth are located as well as the main business areas of the subsidiaries as needed, because funds are usually transferred between the customers (in Japan) and foreign subsidiaries and so forth (abroad). In light of the above, the three mega-banks have already established or have been establishing a framework to investigate not only the commercial flows of customers but also the subsidiaries of customers according to the level risks.

[Examples of advanced approaches taken]

- They established a framework to investigate the countries and geographic areas where the subsidiaries and so forth of customers are located and the details of transactions of the subsidiaries and so forth, taking into account the business of customers and relations between the customers and the bank.
- They identify and assess risks by analyzing the cross-border wire

transfers of customers suspected of being transacted with sanctioned countries and clarifying industry peers which deal with the same products and services.

(b) Ongoing CDD

The three mega-banks have been identifying the actual situations of customers and updating their information while developing and improving the procedures and system to assess customers' risks, taking into account risks they face ahead of other FIs. Therefore, they have already updated information of some customers several times.

The three mega-banks have sent questionnaires by postal mail as the main approach of information updates; however, as the return rate of the questionnaires is not still high, they just started to take other approaches to increase replies from customers, such as the increase of channels and the adjustment of question items. In addition, it is expected that they would receive enormous inquiries from customers compared with other FIs because they have many customers from non-business individuals to small, medium and large sized entities. Therefore, they have taken measures to address the inquiries, such as a dedicated call center, because it is necessary to respond to these inquiries in a respectful manner, such as providing in-depth explanations of the need of the review to the customers.

The FSA has periodically interviewed the three mega-banks on the identification of actual situations of existing customers and the progress of review of the risk assessment as part of its year-round inspections. In addition, it considers approaches for the customers whom postal mail cannot reach, who do not update their information, whose contact information is not identified, and so forth.

Regarding ongoing CDD, the following examples are recognized at the three mega-banks:

[Examples of advanced approaches taken]

- Question items are reviewed taking into account the customers' opinions, and measures to increase customers' responses by increasing response channels, such as the internet banking screen, apps and phone calls, are considered and implemented.

- When outsourcing the sending of questionnaires and inquiry-response, it is ensured that in-depth explanations of the need of the review are provided to the customers by contributing manuals to the outsourcing contractors and holding training.

(c) Measures for economic sanctions

If measures for economic sanctions specified by a country are insufficient, it is at risk of assisting terrorism financing through sanctioned transactions and then being subject to a huge amount of financial penalties by the countries that designated the sanctions. In this point, it is necessary for the three mega-banks to avoid risks associated with economic sanctions by taking measures commensurate with risks, such as identifying the status of transaction stakeholders, countries and geographic areas related to the transactions, and commercial and financial flows of customers not only for ongoing CDD but also for individual transactions, such as cross-border wire transfers, because they trade a wide range of currencies and have relations with many countries and geographic areas because they offer several financial services for international trades, such as remittance to both domestic and foreign customers.

For example, it is necessary to determine whether the transactions are sanctioned by appropriately filtering SWIFT messages and trade documents as needed, identifying commercial flows of customers as needed, and asking their customers about the origin and final destination of traded goods and for information on the transaction parties, such as the address, before executing transactions.

In this point, the following examples are recognized at the three mega-banks:

[Examples of advanced approaches taken]

- With regard to so-called three-cornered trade (or triangular trade), in which commercial and financial flows pass through third countries in addition to exporters and importers, the collected and utilized information on indications of risks of violating various economic sanctions, such as the countries and geographic areas that are likely to be used as a transit point, commercial goods likely to be traded between Japan and sanctioned countries and geographic areas, and specialties of sanctioned countries and geographic areas for pre-transaction

verification.

- Employees of the 2nd line share information on indications of risks collected by employees of the 1st line, and then the effectiveness of verification before transaction executions, including in-depth investigations by staff to understand the status of customers and their transactions details, are improved. In addition, transactions are verified before execution as whether they are sanctioned by utilizing collected information and then improving the bank's own list and refining a pre-transaction checking sheet for remittance.
- Even if it is not clear from SWIFT messages whether a transaction is subject to economic sanctions, the framework to reject sanctioned transactions is improved by conducting in-depth investigations, such as obtaining and analyzing evidence according to risks.

[Areas required to be enhanced]

- With the increase of import/export transaction volume due to globalization and expansion of non-face-to-face and automated transactions, it is required to improve frameworks to continue to detect transactions for which additional verification is required before executing transactions by elaborating investigations for commercial flows of customers before executing and during transactions
- It is required to ensure a framework to appropriately verify transactions by an alternative system when trouble occurs, including when transaction data are not appropriately forwarded to the transaction monitoring system.

(d) Management of correspondent banks and outsourced FIs

The three mega-banks are connected to the international financial system through a large number of foreign entities/offices and a network of correspondent banking contracts. They are entrusted with cross-border wire transfers from regional FIs without correspondent banking contracts with foreign banks, and sometimes entrusted with a part of cross-border wire transfers from regional FIs with correspondent banking contracts with foreign banks, depending on the type of currency and destination of remittance.

When entrusting foreign exchange business with the three mega-banks, the

regional FIs that entrust the business are required to improve their control framework, and the three mega-banks are also required to monitor the AML/CFT/CPF risk control framework of the regional FIs while appropriately identifying the risks associated with being entrusted with foreign exchange business, and to strengthen the monitoring of each individual entrusted transaction by the system and so forth.

In this regard, the following examples are recognized at the three mega-banks:

[Examples of advanced approaches taken]

- They assess risks of the control frameworks of FIs that entrust cross-border wire transfers and so forth, monitor them according to the risks, and support their control framework development by holding outreach or training.
- Regarding monitoring of individual transactions, they are strengthening their framework to monitor cross-border wire transfer transactions whose originator or beneficiary is not their own customer, taking into account the details of past transactions and the transaction histories by collaborating with FIs that entrust cross-border wire transfers and utilizing the transaction monitoring system.
- They have developed a framework to detect high risk transactions and take necessary risk mitigation measures by accumulating information on individual transactions, even if the transactions are not originated by their own customers.
- For more sophisticated management of correspondent banks, they endeavor to identify normal transactions of correspondent banks by not only sending and receiving questionnaires but also investigating transactions executed using accounts in the name of correspondent banks periodically and on an ad hoc basis and asking correspondent banks.

(e) Financing and extending credit involving trade-based finance

Compared to domestic transactions, it is easy to abuse trade finance for illicit purposes due to the fact that it is more difficult to verify the actual location of import/export transactions, and to transfer the proceeds of crime by disguising

import/export transactions or paying an amount additional to or different from the actual transaction/unit price.

The three mega-banks are required to adequately identify, assess, and mitigate risks in light of the fact that the transaction volume of financing and extending credit involving trade-based finance is larger than that of other domestic FIs.

In this regard, the following examples are recognized at the three mega-banks:

[Examples of advanced approaches taken]

- They are establishing a framework to apply mitigation measures in accordance with the risks, taking into account the risks of products and services traded, contract terms, transportation routes (port of loading, port of call, port of discharge, final destination and so forth), name of vessel, port managers, final beneficiaries and so forth.
- They are establishing a framework to identify the beneficial owners of import/export transaction parties who are not customers in accordance with the risks.
- They are establishing a framework to obtain additional information where the contract price of goods differs unnaturally from the market price.
- They are establishing a framework to conduct further verification where the goods traded is unnatural from the products and services the customers usually trade.
- They are establishing a framework to verify whether the goods traded are dual-use goods.
- They are establishing a framework to perform further sanctions screening, including system screening where there is a significant time difference between the submission of trade documents and the inception of the transaction, and trade documents are amended.
- They are improving the effectiveness of settlement of trade transactions, remittance and trade finance business by collaborating with domestic and foreign vendors which provide digitalized trade transaction platforms, and they have started to improve an AML/CFT/CPF control framework by utilizing the system.

Reference Case [Initiatives to reduce risks pertaining to financing and extending credit involving trade-based finance utilizing systems]

In import/export transactions, a large amount and variety of documents are exchanged between the multiple parties involved. The contents of documents used in import/export transactions vary, depending on the type of transactions, and it is difficult to prepare data that can be matched with a list of economic sanctions by a transaction filtering system. Therefore, FIs manually scan information from such documents and perform necessary screening.

Under such circumstances, the three mega-banks have developed or are developing a system to enable documents on import/export transactions to be read by OCR (Optical Character Recognition) and automatically screened by a transaction filtering system.

By converting documents on import/export transactions and information on trade transactions into data, it is expected to become possible not only to confirm whether the persons involved in the transactions are sanctioned, but also to efficiently verify whether the goods traded are dual-use goods and the contract price is rational as well as monitor the routes of vessels transporting goods.

In addition, the three mega-banks are participating in a platform to digitize the exchange of documents on import/export transactions, and are taking steps to improve efficiency, such as reducing the administrative burden on those involved in import/export transactions and shortening document delivery times.

(f) Ship financing

The three mega-banks are working in cooperation with ship owners and operational companies to upgrade their framework for confirming transaction stakeholders, such as vessels subject to loans and operational companies, so that they are not subject to sanctions by the UNSC or other relevant countries.

In this regard, the following areas are expected to be enhanced at the three mega-banks:

[Areas expected to be enhanced]

- It is required to improve a framework to take measures according to the risk level, including screening of parties involved in ship financing and vessels themselves. In particular, in the case of ship financing for used vessels, it is required to verify whether the vessels have participated in ship-to-ship transfer in the past and vessels are sanctioned, although it

is not possible that vessels are sanctioned in the case of ship financing for new vessels.

- It is required to screen vessels when vessels are used for transportation of goods not only when executing ship financing but also when executing remittance or lending with trade documents as trade financing.
- It is required to take measures commensurate with risks by developing procedures for analyzing information predicting the potential danger of ship-to-ship transfers or calling at sanctioned countries/geographic areas, such as suspension of AIS (Automatic Identification System) and changes in routes.

(g) STR

When reporting suspicious transactions, the 2nd line, the control division, should properly analyze the content of the STRs and review the risk assessment for the customers for whom a STR was submitted and the same type of transactions.

In this regard, the following examples are recognized at the three mega-banks:

[Examples of advanced approaches taken]

- Since the number of transactions at the three mega-banks is considerable, they are continuing to consider improving the quality and streamlining of the system by reviewing scenarios, which improves the detection of its transaction monitoring system, which is the starting point for STRs.
- In order to reduce the workload from the detection of suspicious transactions to the submission of reports, a mechanism has been developed whereby necessary documents can be identified instantly by employees in charge using the IT system.
- They are developing a framework to reduce the burden for verification by identifying transactions that are more likely to be false-positives by utilizing the system in the event that suspicious transactions are detected.
- They are promoting the sophistication of STR related measures, such as

considering the establishment of a framework to enable detection of ordering customers, for whom a STR was submitted in the past, for outsourced foreign exchange remittances at the time of receiving a next transaction application, even if the ordering customers are not their own customers.

(h) IT system development and data governance

The proper operation of IT systems enables automatic detection of abnormal transactions, analyses of customer/transaction trends, and assessment of customer risks. It also facilitates the strengthening of the ML/TF risk control framework by setting and adding scenarios for detection and flexible changes to threshold. In addition to the effectiveness of the IT system itself, the data governance of IT systems is also essential.

In this regard, the following examples are recognized at the three mega-banks:

[Examples of advanced approaches taken]

- They are considering group/global-wide evaluation methods and the development of integrated databases, taking into account external experts' opinions, regarding the effectiveness of the transaction monitoring and filtering system and the appropriateness of data governance.
- They optimized their IT system to control risks, consistently taking into account individual customers and the characteristics of transactions of every office around the world.

(i) Group/global-wide management

The three mega-banks have many group entities and a worldwide office network. Therefore, it is necessary for them to develop group-wide/globally consistent policies, procedures and plans taking into account the differences in the business of individual entities and offices as well as the geographical, political and environmental conditions.

In addition, it is necessary for them to develop a framework to appropriately share necessary information between group entities and overseas

entities/offices taking into account the differences in laws and regulations on personal information.

In this regard, following examples are recognized at the three mega-banks:

[Examples of advanced approaches taken]

- They have developed a group-wide/globally consistent control framework, such as formulating policies, procedures, and plans on a group/global-wide basis, and have also been developing a system for sharing information on negative news within the group.
- As to the control framework at overseas entities/offices, the governance framework is being upgraded so that the status of compliance with local laws and regulations is appropriately monitored while supervised by local authorities, and management resources are invested as needed.
- The regional headquarters and the head office in Tokyo are working together to strengthen the AML/CFT/CPF measures of acquired foreign FIs, instead of leaving it to local operations.
- The regional headquarters and the head office in Tokyo are working together to fulfill the requests from local authorities for overseas entities/offices, instead of leaving it to local operations.

(2) CESPs

A. Location of Risks in CESPs

(a) CESPs

"Crypto-asset Exchange Service" refers to (I) the sale and purchase of crypto-assets or the exchange of crypto-assets with other crypto-assets, (ii) the intermediary, brokerage or agency service for the acts referred to in (I) above, (iii) the management of users' money in relation to the acts referred to in (I) above, (iv) the management of crypto-assets for others and the transfer of crypto-assets to a designated address based on the instructions of users without carrying out sale and purchase, etc. (except cases where there are special provisions in other laws on such management as a business), and (v) the business of initial coin offerings (ICOs).[39]

[39] Due to the amendment of the PSA (effective May 1, 2020), "virtual currency" has been

The revised PSA came into force in May 2020 (passed in May 2019), and it clarified that so-called crypto-asset custody business operators, as indicated in (iv) above, are subject to the regulations. There were some systematic improvements to ensure user protection and clarify the rules, including response to crypto asset margin trading and other margin trading, and measures to deal with ICOs.

(b) Characteristics of transactions on a blockchain

Many crypto assets, such as Bitcoin, are characterized by the fact that their transaction history is public on the blockchain and that transactions are traceable. However, in general, transactions are not easy to be traced and the technology for disrupting transaction tracing has been advanced, making it difficult for CESPs to identify the true users of crypto assets other than those that they manage for their customers.[40]

In addition, it is also suggested that as of 2020, there would still be more than 6,000 types of crypto assets in circulation worldwide.[41] Transactions in some of them are difficult to trace because their transaction records are not available even on blockchains, and some of them have vulnerabilities in the maintenance and renewal of transaction records. CESPs should reflect these characteristics in their risk assessments when evaluating ML/TF/PF and other risks of the crypto assets they deal in, and examine and implement the necessary mitigation measures.

(c) Transactions between CESPs and users

Most transactions between CESPs and users take place in a non-face-to-face setting. More specifically, after opening an account with a crypto asset exchanger, the user transfers funds to be deposited from a bank or other source, and uses

renamed "crypto assets" under the law, and the definition of crypto asset exchange business has also been changed.

[40] According to the report of the European Police Office, or "Europol"(INTERNET ORGANISED CRIME THREAT ASSESSMENT 2018), crypto-assets are used to buy and sell illegal drugs to pay for illegal services on the dark web because of their anonymity. In one of the cases where it was pointed out that crypto-assets enhanced anonymity and made it difficult for investigative authorities to trace them, WannaCry, ransomware that restricted the functions of infected computers and demanded crypto-assets in exchange for lifting the restrictions, infected the computers of companies and others around the world.

[41] Japan Virtual and Crypto assets Exchange Association, "Annual Report on Crypto-Asset Transactions (FY 2020)"

the funds to exchange transactions for crypto assets. In the event of a gain on the sale of a crypto asset, the funds are transferred to the user's personal account at the bank. However, all of these transactions are completed through online operations, and there are no opportunities for CESPs to confirm users themselves or the actual identification documents. Also in Japan, where identity verification is mandatory at the time of specified transactions, such as upon account opening with exchanges, such non-face-to-face nature is causing risks, such as identity theft. In some foreign countries, crypto asset ATMs have been installed to enable a form of non-face-to-face transaction with a cash transaction component.[42] There have been reports in other countries of crypto asset ATMs exchanging cash for crypto assets by using prepaid cell phones and falsified IDs to stagger transactions into small amounts (below the threshold value that requires identification at the time of the transaction). CESPs are thus required to adequately identify and assess the risks of transactions using crypto asset ATMs and implement mitigation measures prior to the launch of such services using crypto asset ATMs.

In addition to the risks involved in existing products and services, the rapidly changing environment surrounding crypto-asset transactions needs to be taken into account when identifying and assessing risks. There has been news on the launch of credit card payments directly using crypto assets (including so-called "stablecoins"). In addition, it has been reported that institutional investors have announced their intention to begin to include crypto assets in their portfolios. Therefore, it is necessary to pay attention to whether there are any changes in the risk environment in Japan as a result of the start of use of crypto assets by transaction channels and customer segments that have not had contact with crypto assets in the past. While the use of blockchain analysis tools to capture transaction histories is cited as one of risk mitigation measures, the FATF's guidance also points out challenges, including technical constraints.[43] In response to changes in the environment, there is a continuing need for research that combines multiple methods and consideration of risk mitigation measures; The fact that there are still jurisdictions that do not regulate the crypto asset

[42] Like bank ATMs, crypto asset ATMs are installed in general commercial facilities and usually exchange cash held by users for crypto assets.
[43] Explanatory note 44 and related paragraph in, https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html

exchange industry, as well as the existence of DeFi (decentralised finance) services for individuals worldwide that claim to have no central controller, are considered to be unique events that continue to increase the inherent risk of crypto assets being used for ML/TF, compared to other types of financial services.

B. Current situation and challenges in CESPs

(a) Identification and assessment of risks

As with deposit-taking financial institutions, risk identification in CESPs is to identify ML/TF risks they are facing by comprehensively and specifically examining risks, such as the products and services they provide, transaction types, countries and geographic areas involved in transactions, and customer attributes. This is the starting point of the risk-based approach.

CESPs should identify and assess the risks associated with, not only the crypto-asset products and services they provide, but also with the fiat currencies with which their products and services are closely interrelated, such as when users request yen transfers and withdrawals from their banks. The FSA requires that the establishment and enhancement of a framework commensurate with these risk factors be carried out in a flexible manner, while prioritizing the order of priority. Although there are some advanced cases among CESPs, the following cases are still observed.

[Cases where delays in actions were recognized]

- In some CESPs, their risk assessment reports were supposed to be reviewed each time new products and services are provided, but in reality they are updated only once a year. There are delays in reporting the latest risk awareness, mitigation measures, and residual risks to management and in the risk assessment document.

[Examples of advanced approaches taken]

- Some CESPs have identified and assessed the risks of not only key businesses, but also ancillary businesses.
- Some CESPs are sophisticating their risk assessment by incorporating risk scoring into their methodology.

- Some CESPs have established a framework to ensure the active involvement of not only the 2nd line of defense but also the 1st line of defense department in risk assessment of the products and services they provide, such as drafting of primary risk assessment and participation in risk assessment meetings, etc.
- Some CESPs proactively examine a wide range of quantitative data on products, services, and deposit/withdrawal channels offered by them to identify newly emerged risks and consider mitigation measures.

(b) Risk mitigation

① Verification at the time of transaction and customer due diligence

Some CESPs are taking steps to upgrade their level of risk control framework in light of their own businesses. On the other hand, there are significant differences in the implementation status of risk-based ongoing Customer Due Diligence measures depending on each CESP. In addition, as a result of the majority of the CESPs targeting retail customers in the business category as a whole, the level of depth of due diligence methods for institutional customers also ranged from one CESP to another.

[Examples of advanced approaches taken]

- With regard to Ongoing Customer Due Diligence measures, there are multiple cases in which CESPs actively update customer information and keep it up-to-date even though it has only been a short time since they started dealing with the customers, so that more information can be obtained and used for risk control.
- Identifying red flags related to suspicious transactions based on the results of analysis on past cases of fraudulent remittance and STRs by the firm, and use them to set the focal points for verification at the time of transactions.

[Cases where delays in actions were recognized]

- Some CESPs are considering risk-based Ongoing Customer Due Diligence measures in order to update customer information, nevertheless they pose a delay in the implementation of such measures.

- There is still room for improvement at CESPs in establishing an in-depth investigation when confirming the beneficial owners of their corporate clients and their business status, including the accumulation of insights regarding attributes of corporate clients.

② Utilization of IT systems and data management: data governance

With regard to IT systems, it is necessary to consider the introduction of IT systems and to update existing systems based on the risks faced in accordance with the scale and characteristics of their businesses and transaction types. In the crypto asset exchange business, which is connected closely to IT systems, it is recognized that it is relatively easy to introduce CDD using IT systems. Under these circumstances, a number of CESPs have been recording and retaining customer identification information on their systems since the inception of their businesses.

[Examples of advanced approaches taken]

- Given the risks associated with the transfer of crypto-assets, many CESPs make effective use of data, such as incorporating multiple data, including the beneficiary address of the transfer, into their use of monitoring systems.

[Cases where improvement is required]

- There has been a case where, in the scenario of the transaction monitoring system, a scenario for detecting high-value crypto-assets transactions in relation to customer attributes was missing. As a result, crypto-asset deposit/withdrawal transactions with high value against customer attributes could not be detected at all.
- Although the scenario of the transaction monitoring system itself was properly designed , it was neither implemented as designed in the system nor verified when the system was launched, which resulted in overlooking the fact that transactions that should be detected could not be detected.
- As there was no awareness of the need to investigate relationships

between customers, such as between relatives and interested parties, a search function that enabled this was not implemented. As a result, suspicious group-wide transactions that should be detected could not be identified in a timely manner.

(c) Business Management framework

In the initial stage when CESPs started registration based on the PSA, there were some providers that were concerned about the development of an internal control framework. However, there are several cases where management is reviewing personnel and systems commensurate with their business size and growth, and the internal control frameworks are becoming more sophisticated than in other sectors. Meanwhile, due to the relatively new nature of the business, some providers face the following challenges.

[Cases where delays in actions were recognized]

- The internal auditing division, which is the third line, has not fully had professional staff with expertise and capabilities to conduct AML/CFT/CPF audits of crypto-assets.
- Even in the risk management division, which is the second line, staff with expertise and capabilities in account opening, understanding of various regulations related to crypto-asset transactions, and consideration for the risk characteristics of crypto-assets have not been retained.

[Examples of advanced approaches taken]

- For the 2nd and 3rd line of staff, personnel with expertise in AML/CFT/CPF and internal auditing techniques are hired and retained.
- The providers are making progress in human resource development by encouraging all employees to obtain qualifications related to ML/TF/PF and other measures, thereby raising awareness of the issue throughout the organization.

In this regard, it is necessary to refer to the revised Guidance on Virtual Assets issued by the FATF in October 2021 in order to identify challenges in enhancing

the framework.[44] The public consultation for the revision of the guidance was held in March of the same year.[45] FSA explained the content of the draft Guidance to CESPs and stakeholders through the industry association and exchanged views on draft comments from Japan. The industry continues to work together with the public and private sectors to raise awareness and deepen understanding of the measures. It remains necessary for the industry to be mindful of the substance that the revised guidance addresses (see next section). In addition, the FATF has issued "Risk-Based Supervision Guidance,"[46] and the Bank for International Settlements' Financial Stability Institute has published "Supervising crypto-assets for anti-money laundering"[47] in its periodic report "FSI Insights." These include examples of good practices in Japanese CESPs and FSA, such as the opportunity for neutral multi-stakeholder dialogue and the dissemination of information by both the public and private sectors, and the establishment of a monitoring team with experts on Crypto-asset Exchange Service by the FSA.

C. Notification of information on the originator and beneficiary at the time of transfer of Crypto-Assets;

The FATF Standards were revised in June 2019, requiring the member jurisdictions to introduce and implement a regulation, such as so-called travel rules that require crypto-asset service providers used by the originator to obtain information on the originator and beneficiary upon the transfer of virtual assets and give notice of such information to the CESPs used by the beneficiary. So-called travel rules are stipulated in Recommendation 16 (wire transfer) and are common to banks and other FIs. In Japan, this is covered by the notification obligations pertaining to foreign exchange transactions under APTCP Article 10. In general, FIs are required to accurately add the information required when sending payment instructions through SWIFT or settlement systems (e.g., name, address, and account number of the originator and beneficiary).

On the other hand, given that transactions of crypto assets are processed and

[44] Updated Guidance for a risk-based approach to Virtual Assets and Virtual Asset Service Providers https://www.fsa.go.jp/inter/etc/20211101/20211101.html. For more information, see column [Revised "FATF Guidance on the Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers"] (page 94)

[45] https://www.fsa.go.jp/inter/etc/20210322.html

[46] https://www.fsa.go.jp/inter/etc/20210305.html

[47] https://www.bis.org/fsi/publ/insights31.htm

recorded on a blockchain that can be accessed by an unspecified number of people, it is impractical to post and broadcast the names and addresses of the originators and beneficiaries on the blockchain. Therefore, rather than directly applying Recommendation 16 (wire transfers), Recommendation 15 (new technology) was revised to include provisions for travel rules for crypto-assets in the Interpretive Note of Recommendation 15, which imposes an obligation to send and receive travel rule information separately from transaction data on the blockchain. In light of concerns raised by the private sector and government officials that there are no technical solutions to immediately fulfill this obligation, including the infrastructure for exchanging data, the FATF has established the Virtual Assets Contact Group "VACG"). Since the revision of the FATF Standards in 2019, the FATF has been monitoring the implementation of the FATF Standards by member jurisdictions, and the private sector's technological development on travel rules, conducting outreach activities, and contributing articles.

The FSA assumes the role of VACG co-chair, leading dialogues with local and international industry bodies and monitoring the industry's efforts to comply with the Standards.[48] In cooperation with Japan Virtual and Crypto assets Exchange Association (hereinafter referred to as "JVCEA"), FSA exchanged views on the status of action plans and action taken by CESPs and JVCEA in Japan. The JVCEA is considering the introduction of self-regulatory rules on travel rules. Prior to this, in March 2021, FSA requested the JVCEA to consider the appropriate implementation of the travel rules, resolve technical and operational issues, and establish a framework necessary to promptly implement the travel rules from the perspective of ensuring the proper and reliable business execution of Crypto-asset Exchange Service.[49]

D. International cooperation between supervisors

As a financial authority that introduced regulations for the crypto asset exchange industry and a registration system specifically for the crypto asset exchange industry at an early stage, the FSA is sometimes asked by financial authorities in Asia, Europe, and the United States to share its supervisory

[48] See Chapter 4.11 "Contributions to the FATF (Other Than Mutual Assessment)"

[49] Request for Notification of Originator and Beneficiary Information upon Crypto Assets Transfer (i.e. the travel rule) , https://www.fsa.go.jp/en/news/2021/20210331/20210331.html

experience and provide information on the process of introducing regulations. We are actively responding to such requests for supervisory information exchange.[50]

Reducing the number of jurisdictions that have not yet introduced regulations for the Crypto-asset Exchange Service industry will reduce the burden on Japanese CESPs and other pioneering players in the market who are complying with AML/CFT/CPF regulations; TA will also allow us to monitor the situation in emerging countries that will introduce regulations and enter the market in the future, as well as leading us to cooperation in dealing with overseas operators who conduct unregistered/unsilenced business and to understanding the situation of Japanese CESPs overseas. FSA shall continue to actively leverage opportunities for international cooperation among supervisory authorities.

(3) Fund Transfer Service Providers

A. Location of Risks in Fund Transfer Service Providers

The funds transfer service refers to the business of remittance transactions conducted by legal persons other than banks.

Fund Transfer Service Providers, like DFIs, face risks common to both domestic fund transfer and cross-border remittance transactions, and transfer of criminal proceeds to foreign countries with different legal frameworks and transaction systems, leading to decreased traceability.

(a) Establishment of new categories of fund transfer business

The Fund Transfer Service Providers previously were only allowed to conduct limited cross-border wire transfer transactions, which is an amount equivalent to 1 million yen or less. However, with the revision of the PSA in May 2021, the limitation on the amount of cross-border wire transfer transactions was removed, and has been classified into three categories based on the upper limit of transaction amounts, including new categories that allow handling of large remittances and handling of smaller remittances, in addition to the original business category.

The category classified as Type 1 Fund Transfer Service Providers can handle

[50] See Chapter 4.11, "Contributions to the FATF (Other Than Mutual Assessment) International Cooperation"

large remittances with no maximum transaction amount. In order for a Fund Transfer Service Provider to operate as a Type 1 Fund Transfer Service Provider, it is necessary to obtain approval for a business implementation plan. On the other hand, the original type is classified as Type 2 Fund Transfer Service Providers (where the maximum amount is not more than one million yen) and the type that handles small remittances (where the remittance is not more than 50,000 yen) are classified as Type 3 Fund Transfer Service Providers.

In light of the fact that Fund Transfer Service Providers transactions vary in terms of value, scale, and characteristics, and that the risks they face vary, depending on their size and characteristics, Fund Transfer Service Providers are required to identify and assess not only risks common to remittance transactions but also risks in accordance with the value, scale, and characteristics of each entity's transactions, and to implement necessary mitigation measures accordingly.

Reference [Revision of Administrative Guidelines and Management Framework Required for Type-1 Fund Transfer Service Providers]

In light of the revision of the PSA in May 2021, which newly created multiple categories of Fund Transfer Service Providers, FSA revised its Administrative Guidelines (Volume 3 : Financial Corporation-related 14 Fund Transfer Service Providers Matters) (hereinafter referred to as "Revised Administrative Guidelines").

The Revised Administrative Guidelines clearly state that a Type 1 Fund Transfer Service Provider is required to establish and maintain a more robust AML/CFT risk management framework than other types of Fund Transfer Service Providers because the AML/CFT is of greater importance to their risk control framework as they conduct cross-border wire transfer transactions exceeding one million yen. They also indicate points to note regarding risk identification and assessment, screening/filtering, customer risk assessment, ongoing CDD measures, and transaction monitoring.

The Revised Administrative Guidelines include not only the Type 1 Fund Transfer Service Providers but also the particular expectations common to the Type 2 and Type 3 Fund Transfer Service Providers. For example, the Revised Administrative Guidelines include new items, such as conducting risk assessments according to the period of stay of foreign customers, and timely verification of the accuracy and appropriateness of KYC records and transaction records.

(b) Occurrence of cases of fraudulent withdrawals using Fund Transfer Service Providers' settlement services

In 2020, it was revealed that there were multiple cases in which malicious third parties fraudulently obtained account information of a depositor, opened accounts with Fund Transfer Service Providers in the name of the depositor, linked it with the bank account, and then loaded funds from the bank account to Fund Transfer Service Providers' accounts.

In this case, the risk of fraudulent use associated with identity theft faced by Fund Transfer Service Providers was revealed due to vulnerabilities in the process of verification at the time of transaction by verifying that the customer account has already been opened at the bank and entering into an account transfer contract (i.e. agreement to load value from the specified user's bank account to account with Fund Transfer Service Providers); the verification by Fund Transfer Service Providers was completed only with a bank cash card PIN.

Reference Example [Response to a case of fraudulent withdrawals using Fund Transfer Service Providers settlement services that occurred in 2020]

In 2020, in response to the discovery of cases of fraudulent withdrawals using Fund Transfer Service Providers settlement services, the FSA issued warnings regarding fraudulent withdrawals using smartphone settlement services, and issued request letters to Financial Institutions and Fund Transfer Service Providers, respectively, and revised administrative guidelines. It is important for Fund Transfer Service Providers to build a framework to prevent ML/TF and unauthorized use based on these contents.

For example, it is required to assess risks of the services as a whole in cooperation with the collaboration partner, clarify the division of roles and responsibilities of each party, check information on users based on the results of risk assessment in cooperation with the collaboration partner, and implement appropriate and effective fraud prevention measures commensurate with risks. Specifically, when linking with account transfer services, it is important to implement appropriate and effective fraud prevention measures, such as effective verification at the time of transactions of the users of the funds transfer service by the Public Personal Authentication or other means, and verification of the identity of the users with their depositors by verifying the information of the users confirmed by personal identification documents, etc. with the information held by the collaboration partner, and detection (monitoring) of fraudulent transactions. These measures include effective verification at the time of transactions of the users of the funds transfer service and verification of the identity of the users with the depositors.

JBA has issued "Measures for Fraudulent Withdrawals in Fund Transfer Service Providers

Settlement Services," and Japan Payment Service Association has issued "Guidelines for Preventing Fraud in Linkage with Bank Accounts," in Japanese.

(c) Developments in Fund Transfer Service Providers

In addition, discussions are under way on the payment of wages to user account with Fund Transfer Service Providers (payroll) and the expansion of eligibility to participate in the Zengin system (nation-wide online network system for banks handling domestic funds transfers) to Fund Transfer Service Providers.

Fund Transfer Service Providers should keep a close eye on the status of these discussions and analyze and examine ML/TF risks in advance based on the possibility that the risks they face may change.

B. Current situation and challenges in Fund Transfer Service Providers

(a) Identification and assessment of risks

While many operators have comprehensively and concretely identified and assessed their own risks, such as products/services offered, transaction types, countries/regions, and customer attributes, the following instances have been observed in some Fund Transfer Service Providers. Challenges remain in identifying and assessing risks based on a comprehensive and concrete assessment of the risks in their size and characteristics.

[Cases where delays in efforts were recognized]

- As in the case of the fraudulent withdrawals using Fund Transfer Service Providers settlement services described in A (b) above, the Fund Transfer Service Providers only examined through interviews that the authentication method used by some of the partner banks involved only PIN numbers (one factor authentication), and did not examine risks based on the authentication method of the partner banks .
- As described in "(b) ①" below, due to the lack of accuracy of customer information resulting from inadequate Fund Transfer Service Providers verification at the time of transactions and non-implementation of ex-post analysis of records of verification at the time of transactions, it has

not been possible to comprehensively and concretely verify risks, such as customer attributes.

- Fund Transfer Service Providers did not conduct analysis of suspicious transaction reports and did not conduct risk assessment based on specific and objective grounds.

(b) Risk mitigation

① Appropriate verification at the time of transaction and preparation and preservation of verification records

As for verification at the time of transactions by verifying that the customer account has already been opened at a certain bank, as a result of the failure to require customers to declare accurate information and to verify the declared information, some business operators' customer records were found to contain an invalid description such as: occupations that are not ordinarily possible, inadequate answers like "(I) will not answer," and descriptions that include pictograms and symbols for "customer identification information (name, residence, and date of birth)," "occupation," and "purpose of transaction."

The accuracy of customer Information, such as "customer identification information" is a prerequisite for an ML/TF risk management framework. Without this information, it is impossible to identify and assess the risks faced by a business operator and to take mitigation measures commensurate with its own risks, such as ongoing CDD and transaction monitoring based on customer risk assessment. However, the following were observed at some Fund Transfer Service Providers.

[Cases where delays in efforts were recognized]

- As described above, the records of "customer identification information (name, residence, and date of birth)" "occupation" and "transaction purpose" confirmed by the verification at the time of transaction contain occupations that are usually impossible, invalid answers like "(I) do not answer" and descriptions that include pictograms and symbols.
- In cases where operations of verification at the time of transaction is

outsourced, the outsourcer does not adequately provide training or guidance to the outsourced party, or does not examine whether the outsourced party is performing its duties properly and reliably, and does not make improvements as necessary.

② CDD

Some operators did not develop effective plans for customer risk assessment and Ongoing CDD, while others did not adequately transform the control framework to manage the period of stay for foreign visitors to Japan. The challenge is to develop effective plans for customer risk assessment and Ongoing CDD and implement them before the required action deadline.

In addition to periodically grasping the actual situation according to risks, it is necessary to enhance the effectiveness of its risk-based approach, such as by confirming and examining customer information and transaction details and reviewing customer risk assessments when a trigger event that is expected to increase the ML/TF risk of a customer occurs (for example, when it encounters negative news through Timely Disclosure or news reporting).

③ Transaction monitoring and filtering

Regarding transaction monitoring, some operators were found to have not set alert criteria (scenarios and thresholds) that reflect their own risk assessment, and to have not sufficiently analyzed and examined them.

With regard to transaction screening, there were cases in which some operators did not establish frameworks for appropriate transformation and implementation of its control, for example, absence of fuzzy matching in screening logic.

④ Suspicious transaction notification

There were some cases where operators considered submitting suspicious transaction reporting only on the basis of the type of transaction, without considering customer attributes, such as occupation, purpose of transaction, nationality, age, etc.

In addition, there were some cases in which suspicious transactions were identified and no STR was submitted for more than one month, even after the

operator took measures to suspend the accounts. Also, there were cases in which one-month's amount of STRs were submitted at once, instead of immediate submission after the STR decision.

⑤ Agent management

There were some cases in which an operator did not confirm whether the agent was carrying out business appropriately despite the fact that it conducted transactions through the agent, and cases in which an operator only received reports on problems that had occurred at the agent and did not examine or analyze whether the agent management methods were effective.

The challenge for Fund Transfer Service Providers is to assess the risks of each agent and then monitor its control environment according to those risks.

Some of the global fund transfer service providers whose foreign affiliates have been subject to administrative sanctions by their home country authorities are taking steps to strengthen their agent management, such as reviewing agency management programs and auditing agencies.

(c) Business Management Framework

Some operators have been found to deprioritize the development of a risk control framework in general, including ML/TF, for example, by management promoting sales based on a business model that emphasizes speed and not allocating resources appropriately in line with the business model.

It was observed in some cases that second-line personnel at operators were under-staffed in light of the nature of their business and the number of transactions, and that they were forced to prioritize handling of incidents that occurred on a daily basis rather than developing a management framework.

Furthermore, there were cases where the third line audits were limited to compliance audits to ensure that procedures were carried out in accordance with the rules and regulations, and not audited in light of the ML/TF risks they face, in terms of scope, frequency, and methods.

[Cases where delays in efforts were recognized]

- The board has underdeveloped its risk control framework by, for example, promoting sales based on a business model that emphasizes

speed and not allocating appropriate resources to risk management in general, including ML/TF, commensurate with the business model.

(4) Insurance Companies

A. Location of risks in Insurance Companies

Although various reports state that the ML/TF risks of Insurance Companies are not higher than those of businesses that provide settlement services, they face risks that differ from those of DFIs, that immediately pay out deposits and savings to domestic and foreign customers and handle remittances and settlements, because of the set limitation in requirements for payment of insurance benefits.

Life insurance products are designed based on the premise of an ongoing relationship with policyholders whose claims can be paid only when certain events occur, such as death. On the other hand, as described in the NRA, products with savings characteristics allow for the voluntary withdrawal of all or part of the premium paid during the term of the contract. Therefore, ML/TF risks in the life insurance sector generally include the use of criminal proceeds to fund the purchase of life insurance products, as well as the use of funds obtained from life insurance contracts for the financing of terrorism, as with other financial products. Particularly for products with high savings characteristics, the occurrence of certain events is not a condition for benefits, and since refunds can be obtained through cancellation before maturity, criminal proceeds can be capitalized immediately or by being deferred. Considering that a relatively high surrender value can be paid even in the case of cancellation before maturity, ML/TF risks are particularly recognized when, for example, insurance premiums are paid at the time of contract conclusion and then promptly surrendered. Similarly, attention should be paid to cases where the amount allocated to insurance premiums is refunded due to cooling off.

However, the risks are considered to be limited, for example, with respect to the payment of maturity benefits, etc. for insurance contracts where no maturity benefits are paid, insurance contracts where the total refund amount is less than 80% of the total premium paid, qualified retirement pension contracts, and group insurance, etc.

As for non-life insurance products, which are mainly non-refundable,

although the possibility of ML/TF use of claims is small due to the unpredictability of the events of claim payment, attention should be paid as usual so that contracts for fraud in claims and cash repayments on loans to policyholders can be detected. Meanwhile, premiums may be used for ML/TF purposes in a manner similar to almost all commercial activities.

One example that could be used for ML/TF purposes is where premiums are paid or substantial overpayments are paid by proceeds of crime and a claim for full or equivalent of overpayment is made. From this perspective, it is necessary to grasp the actual situation of policyholders, etc. and screening them with あ targeted sanction list.

As marine insurance consists of cross-border transactions and vessels are also subject to sanctions, it is necessary to take risk-based measures and screen them with a targeted sanction list so as not to violate the sanctions of UNSC or other relevant countries.

Insurance companies, life insurance companies and non-life insurance companies alike, invest money and other assets received as insurance premiums through investments in securities or lending money. When examining ML/TF risks, it is necessary to take into account risks associated with investments and loans.

In addition, insurance products are sold through various channels. In particular most insurance contracts are sold through sales agents, including so-called independent agents. Therefore, it is necessary not only to confirm the beneficial owners of the sales agent, which are o61utsourcees, but also to confirm the control framework for managing the ML/TF risks of the agents. Furthermore, signing the insurance policies and various maintenance procedures are sometimes carried out in a non-face-to-face setting. It should be noted that, in general, compared to face-to-face transactions, it is more likely that customer identification information will be falsified or a fictitious person or other person will be impersonated due to the falsification or alteration of identification documents, etc..

B. Current status and challenges in Insurance Companies

(a) Risk identification and assessment

The Guidelines require insurance companies to comprehensively identify and

assess the risks they face with respect to their products and services, transaction types, countries and regions, customer attributes, etc., with reference to the NRA and the FATF Guidance. In order to comprehensively identify risks, insurance companies need to include management of securities investments and money lending, etc. with respect to money and other assets received as insurance premiums.

Under these circumstances, significant differences have emerged among companies in terms of specific initiatives, as described below.

[Cases of actions in progress]

- Based on the group policy formulated by the parent company in compliance with the Guidelines, business operators that form groups, such as holding companies, implement initiatives that are common in and outside Japan, and each company comprehensively and specifically identifies and assesses the risks faced by its business operation in terms of its products and services, transaction types, countries and regions, and customer attributes.
- In cases where an insurance company has outsourced KYC operations and/or been using agents, the insurance companies periodically examine risks and the business environment of the outsourcing contractor and/or agent from the viewpoint of whether the business environment for such AML/CFT/CPF is appropriately developed.

[Cases where delays in actions were recognized]

- There are cases where the NRA and its follow-up reports' descriptions are only formally described in their Risk Assessment Reports, and various transactions were counted, without comprehensive and specific risk identification and assessment taking into account the characteristics of the company and its business sector.
- As premium payments are becoming cashless, in some cases an insurance company allows exceptional administrative processes, such as accepting premium payments in cash at counters without confirming reasonable reasons and payment in cash through sales people, although there are internal policies and procedures prohibiting cash payments. In addition to ML/TF risks, there are various risks associated with cash

transactions, such as administrative burdens and accidents, so there are significant advantages in promoting cashless payments.

(b) Risk mitigation

① CDD

In order to implement ongoing CDD to mitigate risks, it is necessary to conduct a customer risk assessment that combines the products and services used by customers, transaction types, countries and regions, and customer attributes. Many insurance companies are making good use of existing mechanisms to respond to customer risk assessments.

With regard to risk assessment standards for customers, some insurance companies have developed group-wide risk assessment policies, etc., and then developed group-wide standard acceptance policies, etc., and are considering group-wide responses. It is also effective to rely on third-party validation to ensure consistency of those policies and actions taken, such as whether their control frameworks are being implemented at the same level.

[Cases of actions in progress]

- Comprehensive consideration is given to information such as products and services used by customers, transaction types, countries and regions, and customer attributes, conduct risk assessments for each customer category in which these elements are common, and take measures according to the risks of each customer group. Measures are taken according to the risks of each customer group, such as checking and updating information on customers and ultimate beneficial owners through visits once a year, etc., for customers deemed to be high risk.
- Established and implemented a validation framework to continuously confirm that related parties, including investee companies and ultimate beneficial owners, are not subject to sanctions or anti-social forces.

② Management of investments and loans

In order to comprehensively identify risks, it is necessary for insurance companies to include investment in securities and lending funding from insurance premiums; it is important for each company to take measures such

as establishing a system to continuously manage such risks. In doing so, for example, it is important to establish a validation framework to continuously confirm that the investee or counterparty or related parties are not subject to sanctions or anti-social forces, and to evaluate the risks from the perspective of whether the risk control framework pertaining to the outsourced AML/CFT/CPF is appropriately developed when such investment is outsourced.

[Cases of actions in progress]

- Among investment operations, management methods are distinguished into self-conducted and outsourced investment. For example, in the case of self-conducted investment and financing, it is necessary to confirm, based on the geographical factors and attributes of the investee, that the investee, beneficial owners, or other related parties do not include those subject to sanctions or high-risk targets.
- Periodically checks the beneficial owners based on risk, conducts screening, and if negative news is identified through publicly available information, such data is taken in investment decisions.
- In case of outsourced investment, checks and verifies the host country and investment target at the start of transactions and confirms that the parties concerned are not sanctioned or high-risk entities initially and on a regular and risk-based basis, taking into account whether the ML/TF risk control framework has been properly developed at the outsourced side.

③Transaction monitoring and filtering

It is required to establish a framework for the accurate detection, monitoring, and analysis of suspicious transactions, etc. by using IT systems and by humans according to the nature of its business and size. For example, in case of marine insurance, it is recognized that a framework to be developed according to risks so as not to violate the sanctions of UNSC or other countries concerned.

Multiple insurance companies are using transaction monitoring systems to detect unusual transactions, but some companies are still in the process of effectively reducing risk through the use of systems. It remains a challenge

for the industry as a whole to promote risk-based initiatives while taking into account each firm's situation.

[Cases of actions in progress]

- Actions are being made to screen vessels with marine insurance to check if they are not subject to sanctions, and to utilize systems and third-party data to appropriately manage routes and ports of call.

[Cases where delays in actions were recognized]

- Although there is a considerable number of cases where ASF is confirmed through transaction filtering, there are cases where scenarios are not yet designed to detect frequently repeated transactions, such as unusual exceptional operations by sales staff, transactions by cash, early cancellation / cooling off, etc., and the detection status of each scenario is not analyzed and reviewed in a timely manner

(c) Business Management Framework

In response to the findings by internal audits, some insurance companies have secured necessary personnel in their AML/CFT/CPF divisions and strengthened their AML/CFT/CPF control environments by, for example, increasing the sophistication of operational environments within the divisions and smoothly passing on skills and knowledge. However, some insurance companies have not established sufficient specialized units in the second line. Overall, the recruitment and development of highly skilled professional staff continues to be a challenge.

(d) Response to COVID-19

While the number of different types of non-face-to-face transactions is increasing in several industries, partly due to the impact of COVID-19, the life insurance industry has begun to actively adopt remote insurance sales and adopt chat functions and online interviews. It has been considered extremely difficult for life insurance companies to offer insurance policies without having direct contact with new customers due to characteristics that are

different from those of financial products such as deposits. However, some companies have been actively undertaking initiatives, such as transforming various processes that can be completed in non-face-to-face settings.

Future challenges include not only the adoption of ongoing CDD using an e-KYC on the occasion of online recruitment, and not only verification of negative news, but also consideration and sophistication of remote procedures for ongoing CDD in accordance with each company's circumstances, such as deepening questions according to the attributes and business purposes of a customer.

(5) Financial Instruments Business Operators, etc.

A. Location of risks in Financial Instruments Business Operators, etc.

With regard to transactions of financial instruments, the market itself in which financial instruments are traded may be used as a place where illicit funds are created by insider trading, market manipulation, or other predicate crimes, such as disguising legitimate transactions. Also, there may be cases where criminal proceeds, including those created in this way, are used for concealment by converting them into highly liquid financial instruments. In addition, if financial instruments, etc. have a complex structure or if there is a wide range of parties involved in transactions, the flow of funds becomes unclear and more difficult to trace, and there may be a risk that they may be used for concealment of criminal proceeds.

In addition, as transactions through the Internet and other non-face-to-face channels are increasing in securities transactions, there is a greater risk of transactions with fictitious persons or persons posing as others than in face-to-face transactions.

It is necessary to implement AML/CFT/CPF based on trading channels and transaction types, taking into account the characteristics and risks of such financial instruments and markets. In particular, it is important to coordinate between banks to which funds are deposited and withdrawn, and Financial Instruments Business Operators, etc. ("FIBOs"), as well as between the AML/CFT/CPF division within FIBOs, and the division that monitors and reviews unfair transactions.

In the asset management business, the inflow of criminal proceeds from

investors and the inflow of funds to companies in which those subject to economic sanctions are involved through investment activities in FIBOs are likely to occur. Therefore, FIBOs may take measures such as, for example, checking the director or beneficial owners of the investment target against the list of those subject to sanctions in the case of a direct investment target, or checking the AML/CFT/CPF management control framework of the investment manager who manages the investment target fund in the case of an investment through a fund of funds.

When outsourcing the sale of investment products (investment trusts, etc.), the risk of criminal proceeds flowing into investment products increases if the sales company's control framework for managing risks is weak. Therefore, it is important to identify and assess the risks of the products and services, including whether the control environment for managing the ML/TF risks of the outsourced sales company is appropriate in light of its own standards, and to implement ongoing management in accordance with the risks.

B. Current Status and Challenges of FIBOs

(a) Risk identification and assessment of FIBOs

In some cases, the significance of risk identification and assessment has permeated through various efforts, such as public-private partnerships through self-regulatory organizations and industry associations, and the methods and depth of analysis by FIBOs have improved. There were also cases in which the specific characteristics and risks of a FIBO's own operations have been analyzed and identified based on the status of STR and the results have been incorporated into its risk assessment report, and cases in which a company has collected information on economic sanctions imposed by foreign governments and assessed risks based on its own circumstances.

On the other hand, there were cases where there was room for improvement in the comprehensive and specific identification and examination of risks, such as products and services, transaction types, countries and regions, and customer attributes, in the examination of individual and specific characteristics that a company actually faces, such as the status of STR, as described below.

[Cases where delays in actions were recognized]

- In identifying the risks of products and services, risks are not examined after specifically identifying the products and services actually handled.
- In identifying transaction type risks, transactions through intermediaries or referrals are not examined.
- In assessing the residual risk of products and services, residual risks are estimated lower than actual risks, based on unimplemented risk mitigation measures.
- In identifying country and regional risks, reference is made to the APTCP Enforcement Ordinance, and only Iran and DPRK are subject to review.
- Risk assessments are conducted based solely on the NRA, without developing risk assessment criteria that take into account the scale and characteristics of the company.
- Only the conclusion of the assessment was described in the risk assessment report, and the basis for it was not understood.

(b) Risk mitigation

In risk mitigation, it is necessary to investigate the details of individual customers and transactions based on the risks identified and assessed by the company, and determine and implement effective mitigation measures that should be taken in light of the results of the risk assessment. It is also necessary to instill mitigation measures at branch offices and other locations, particularly through the guidance of the division in charge.

Under these circumstances, while there are good practices in FIBOs, such as examining the effectiveness of various risk mitigation measures with the perspective of third parties as necessary. On the other hand, there are still areas that remain as challenges.

① CDD

Due to the impact of COVID-19, there are constraints and challenges in the implementation of ongoing Customer Due Diligence and understanding of customers whose beneficial owners are unknown, there are good examples of efforts to mitigate ML/TF risks while giving consideration to the smooth execution of transactions, such as the introduction of simplified CDD according to risks.

[Cases of actions in progress]

- The company uses transaction balance reports to present the current registration information of all customers with assets in custody and to confirm whether information has been updated.
- Customers who have signed up for online trade services to update their registration information enter additional information through a dedicated screen within the service. The company also uses non-face-to face channels for information updates, such as to make it possible for each customer to manage records of access to information updates and additional entry screens
- Those who refuse to open accounts are registered in their own database, and a system is in place to prevent other branches from opening accounts.

② Transaction monitoring and filtering

It is necessary to appropriately prevent transactions with prohibited parties, such as anti-social forces and sanctioned persons, and to establish an appropriate control framework for transaction filtering in order to identify and manage customers who become prohibited parties after the commencement of transactions.

In addition, in order to detect transactions that may lead to the filing of an STR, companies are required to establish an appropriate control framework for transaction monitoring, such as setting criteria for extracting scenarios, thresholds, etc. that reflect their own risk assessments and improving the criteria for extracting transactions.

[Cases of actions in progress]

- The effectiveness of the identification criteria of the transaction monitoring system is reviewed and adjusted periodically.

[Cases where delays in actions were recognized]

- The frequency of screening the list of economic sanction persons against the names of existing customers is limited to a periodic basis, and screening is not conducted when updating the list.

③ Suspicious transaction reports

FIBOs are required to accurately detect suspicious customers and transactions, while taking into account various information held by them, and after filing STRs, it is necessary to analyze each report from various perspectives and use it to strengthen risk mitigation measures.

[Cases of actions in progress]

- In order to refine the analysis of suspicious transaction cases, reasons for filing are subdivided and the number of reported cases is classified and aggregated.
- STRs are analyzed according to transaction and customer attributes.

(c) Business Management Framework

When developing a risk management framework, it is necessary to implement the measures required by the Guidelines according to risks, even in cases where it is difficult to establish a specialized AML/CFT/CPF division due to restrictions on the size of the company, etc. However, if it can be reasonably determined that the risk is low as a result of risk identification and assessment, it may be possible to take risk mitigation measures according to risks. In any case, the involvement of the board is essential from the stage of risk identification and assessment. It is necessary to establish an internal framework in which the department in charge of AML/CFT/CPF shares information that contributes to appropriate recognition of the current situation and management decisions with the board and the board follows up appropriately.

Under these circumstances, the following good practices were recognized:

[Cases of actions in progress]

- For the purpose of reviewing the effectiveness of the AML/CFT/CPF, the management is working to establish testing procedures for the second line after selecting themes such as customer risk assessment and transaction monitoring.
- The FIBOs regularly report to the Executive Committee on the status of customer risk assessment, transaction monitoring and filtering alert processing, and the number of STRs by reason.

- The management in charge of AML/CFT/CPF communicate to branch offices a message regarding the risk-based approach and the significance of Ongoing Customer Due Diligence.
- Training is provided on the significance of a risk-based approach and points of focus of STRs for each level from directors to general employees.

(6) Trust Banks and Trust Companies

A. Location of risks in Trust Banks and Trust Companies

A trust is a system in which a trustor transfers the right of ownership, administration, and disposition of property related to money and land to the trustee (Trust Banks, Trust Companies, etc.) based on a trust agreement or will, etc., and the trustee administers and disposes of the property on behalf of the beneficiary in accordance with the purpose of the trust set by the trustor.

When Trust Banks and Trust Companies become a trustee, confirmation at the time of transaction is required under the APTCP, and there is no change in the fact that it is necessary to take measures against AML/CFT/CPF from the viewpoint of whether the trustee converts pre-trust assets into beneficial interests in Trust Banks and Trust Companies and transfers illicit profits to the beneficiaries.

B. Current status and challenges in Trust Banks and Trust Companies

A unique point of trust schemes is that the relationship between FIs and customers is a three party relationship that includes not only the initial owner of assets (trustor) and Trust Banks and Trust Companies (trustee), but also the person to whom the rights of assets are transferred (beneficiary). Trust Banks and Trust Companies, as a trustee, are required to conduct sufficient customer identification and risk assessment procedures for not only the trustor but also the beneficiary.

In particular, some of the products and services handled by Trust Companies are characteristic of individual business. Trust Companies are required not only to refer to the NRA and the guidance of FATF, but also to conduct comprehensive and specific risk identification and assessment of such products and services based on the characteristics of their own business. Under these circumstances,

the following actions were taken.

[Cases of actions in progress]

- After identifying the products and services they provide in a comprehensive and specific manner, they conduct risk assessments of those products and services in accordance with pre-defined risk assessment criteria.
- Risk assessment is conducted based on the review of possible customer attributes and utilized in customer risk assessment.
- Based on the products and services they provide, they conduct identification of parties involved in trust schemes and conduct screening.
- In case of investment of entrusted assets, relevant parties, including the investment target, are screened according to risks.
- When new products and services are provided, they are reviewed from the perspective of ML/TF risks, and the second line of staff instructs the department in charge for the products and services to implement the necessary risk mitigation measures.
- Management is actively commenting on the results of the risk assessment.

(7) Money Lending Business Operators

A. Location of Risks in Money Lending Business Operators

Money lending or money loan intermediation ("lending") by money lending business operators meets the various financial needs of consumers and businesses by providing highly convenient loan products and prompt screening. In the money lending business, partnerships with deposit-taking FIs and other FIs have led to the popularization of automated contract reception machines and automated teller machines, as well as the expansion of transactions over the Internet, which have further boosted the convenience of product usage.

Along with the increase in convenience, non-face-to-face transactions have become widespread in the money lending business. In addition, there have been cases of spoofing, such as making applications for loan contracts using forged personal identification documents of other persons. Therefore, the money

lending business, like other FIs, is required to strengthen its control framework for ML/TF risk.

The FSA monitors the development of a control framework in the money lending business, by requiring Money Lending Business Operators under its jurisdiction to report quantitative and qualitative information on the status of transactions and the implementation status of AML/CFT/CPF.

B. Current situation and challenges in Money Lending Business Operators

Money Lending Business Operators are characterized by restrictions on the amount of money that can be laundered at one time due to the regulations on total lending amount, and various investigations based on the Money Lending Business Act are conducted at the time of application and during the loan period. While some firms are using these existing mechanisms to establish and improve ML/TF management frameworks, there are differences in the status of their efforts.

[Examples of progress in initiatives]

- The skills of persons in charge are maintained and improved by concentrating their work at operational centers when conducting various surveys. In addition, operational centers, , where many contacts are made over the phone, check whether customer information has changed in order to keep the customer information up-to-date at the time of customer contact.
- Using existing systems, some money lending business operators have strengthened their monitoring, focusing on the similarities and suspicious nature of contracts, such as continuous use of the Money Lending Business Operators' cards at ATMs. In addition, some operators have also established a control framework in which similar incidents can be prevented before they occur by sharing them with related departments through internal cooperation systems.

[Cases where delays in efforts were recognized]

- In some cases, money lending business operators failed to identify and assess risks in a comprehensive and specific manner, taking into

account the NRA, guidelines, and the characteristics of their own business.

Chapter 3. FATF 4th round of Mutual Evaluation Report of Japan Results

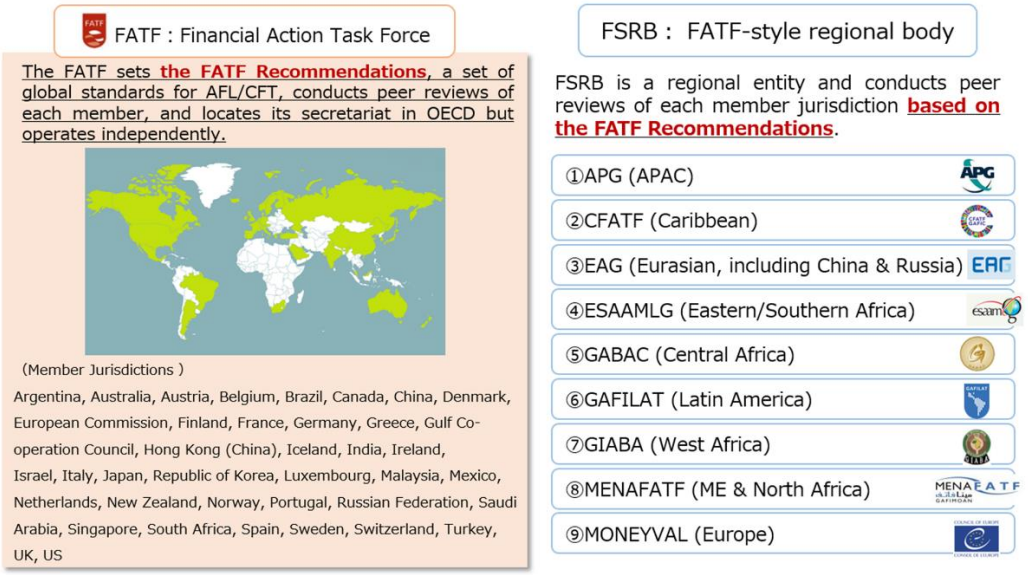
1. The FATF and the FATF 4th Mutual Review Mechanism

(1) FATF and its mechanisms

The FATF is an inter-governmental body established in response to the G7 Arche Summit Economic Declaration in 1989 to promote international efforts to fight money laundering. In 2001, the development of international standards in the fight against terrorist financing was added to the mission of the FATF; since then, the FATF has been promoting international measures and cooperation related to the financing of terrorism. In 2012, CPF measures related to weapons of mass destruction were added to the FATF Recommendations (i.e. Recommendation 7) in response to the nuclear weapon and other developments in North Korea and Iran.

The FATF has developed and reviewed the International Standards on AML/CFT/CPF (FATF Recommendations). Currently, more than 200 countries and regions around the world are working to strengthen their AML/CFT/CPF in line with the FATF Recommendations and other international standards. The FATF also conducts mutual evaluations of its member jurisdictions on their compliance with the FATF Recommendations. Based on the results of these evaluations, assessed jurisdictions are required to make progress on the area identified by the FATF as weak and to report the status of improvement (follow-up) to the FATF. If the results of mutual evaluations and follow-up assessments are extremely insufficient, they may be identified (listed) as a jurisdiction under increased monitoring in their AML/CTF/CPF regime, and foreign financial authorities and financial institutions may strengthen their monitoring of FIs and individual cross-border wire transfers in these jurisdictions. As a result, there is a possibility that the listed jurisdiction's import and export settlement procedures may be delayed and overall economic activities may be disrupted.

Overview of the FATF



(2) Results of the 3rd Mutual Evaluation of Japan and subsequent responses

At the third Mutual Evaluation of Japan in 2008, the FATF examined the status of the development of laws and regulations (TCs) in Japan in line with the FATF Recommendations. Out of 49 items consisting of 40 Recommendation and 9 special Recommendations (the 40 Recommendations and 9 special Recommendations were combined in 2012), a review of Japan was conducted in which the 25 items were rated as “need for improvement (non-compliance or partial compliance),” and CDD measures, which was one of the important Recommendations, were also rated as “non-compliance.” In June 2014, the FATF released a statement calling on Japan to promptly remedy the AML/CFT deficiencies identified by the FATF in 2008. Subsequently, the development of related laws and regulations proceeded in light of the FATF’s international discussions, financial crime in Japan and overseas, and terrorist acts overseas.

Japan's response after the third Mutual Evaluation

Date		Contents
2008	**October**	**Adopted 3rd Mutual Evaluation Report of Japan**（resulted in Regular Follow-up） ＜Major deficiencies＞ 1 Material support to terrorists is not criminalized 2 There is no asset freeze system for transactions between residents 3 Customer due diligence is inadequate 4 Has not signed the Palermo Convention
2014	**June**	**FATF Public Statement (Noted that Japan should be encouraged to address deficiencies promptly.)**
	December	Enforcement of Amended Act on Punishment of Financing to Offences of Public Intimidation (Respond to 1 above)
2015	**October**	Enforcement of International Terrorist Asset-Freezing Act (TAFA)(Respond to 2)
2016	**October**	Full Enforcement of Amended Act on Prevention of Transfer of Criminal Proceeds (Respond to 3) **Completion of the Follow-up Process for 3rd mutual evaluation Japan**
2017	**April**	**Enforcement of Amended Payment Services Act and Act on Prevention of Transfer of Criminal Proceeds**
	July	**Enforcement of Amended Act on Punishment of Organized Crimes and Control of Proceeds of Crime** **Conclusion of the Palermo Treaty (Respond to 4)**
		Publication of Collection of Defects Pointed out in Foreign Exchange Inspections (MOF)
2018	**February**	**Publication of the Guideline for financial institutions (FSA)**

Source: Ministry of Finance, June 14, 2019, Council on Customs, Tariff, Foreign Exchange and Other Transactions, 41st Subcouncil on Foreign Exchange and Other Transactions.

Japan's Action after the public statement by FATF in the 3rd round of Mutual Evaluation

① **Enforcement of Amended Act on Punishment of Financing to Offences of Public Intimidation : Enforcement on December 11, 2014**
- In addition to financial support for terrorist acts, material support such as providing hideouts is also criminalized.
- Criminalizing the collection and indirect provision of funds by terrorist collaborators.

② **Enforcement of Amended Act on Special Measures Concerning Asset Freezing, etc. of International Terrorists Conducted by Japan Taking into Consideration United Nations Security Council Resolution 1267, etc. : Enforcement on October 5, 2015**
- Restrictions on domestic transactions by international terrorists.

  Note : Foreign transactions of international terrorists are regulated by the Foreign Exchange Law.

③ **Enforcement of Amended Act on Prevention of Transfer of Criminal Proceeds : Enforcement on October 1, 2016**
- Define the verification of high-risk transactions at the time of transaction and the determination of suspicious transactions.
- Make it mandatory to check whether the counterparty bank overseas is appropriately implementing AML/CFT measures when signing a correspondent contract.
- Formulating internal rules for the implementation of CDD measures and stipulating ongoing CDD, in addition to providing education and training for employees.

④ **Enforcement of Amended Act on Punishment of Organized Crimes and Control of Proceeds of Crime : Enforcement on July 7, 2017**
- New penal provisions for planning to commit certain crimes related to organized criminal groups (Planning to Commit Terrorism and Other Serious Crimes)
- Predicate crimes for criminal proceeds should be punished in the same manner as crimes that are punishable by the death penalty, life imprisonment, or imprisonment with or without work for more than four years.

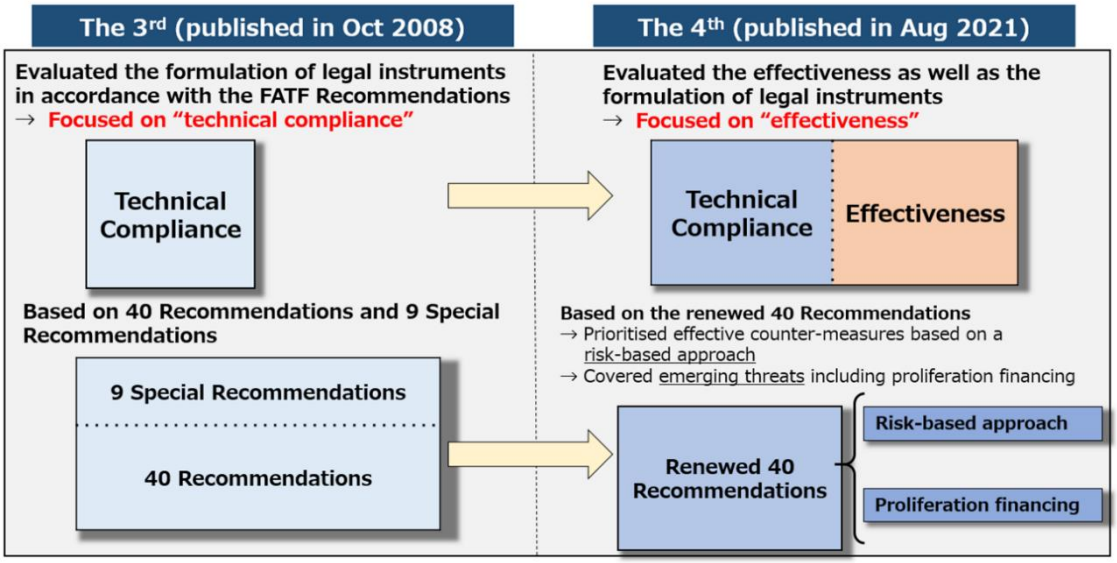
  Note : This Act has made it possible to conclude the Palermo Convention.

Source : June 14, 2019, Council on Customs, Tariff, Foreign Exchange and Other Transactions, 41st Subcouncil on Foreign Exchange and Other Transactions, MOF

(3) 4th round of Mutual Evaluation Report of Japan Structure

In the 4th round of Mutual Evaluation Report of Japan, the FATF reviews not only the level of technical compliance (TC) with the FATF standards but also the level of effectiveness of countries' AML/CFT/CPF framework. There are eleven categories (immediate outcomes (IOs)) to evaluate effectiveness, and the IO. 3 examines how effectively FSA and other supervisory authorities are conducting appropriate regulation and supervision of the AML/CFT/CPF measures of FIs and DNFBPs. IO. 4 examines how FIs are conducting appropriate AML/CFT/CPF measures (risk assessment, CDD, record keeping, suspicious transaction reporting, etc.) according to risks.

Table 3 Comparison between the 3rd round of Mutual Evaluation and 4th round of Mutual Evaluation



Each FATF Mutual Evaluation Report is comprised of an executive summary, a main document (results of IOs assessment), and a TC Annex (results of TCs assessment). In the mutual evaluation process, the FATF evaluates the effectiveness and especially core issues, described in the FATF's Procedures for the FATF 4th Round of AML/CFT Mutual Evaluations,[51] and asks assessed countries questions about the level of understanding and implementation, such as "how they understand

[51] FATF Methodology for assessing compliance with the FATF Recommendations and the effectiveness of AML/CFT systems
https://www.fatf-gafi.org/publications/mutualevaluations/documents/fatf-methodology.html

and how they are implemented." In the main body of the report, the items evaluated based on these viewpoints by the FATF are summarized as "Key Findings," "Recommended Actions," and main document, followed by "Overall Conclusions," which consist of four grade ratings.

A. Rating criteria for the 4th Mutual Evaluations

(a) Ratings of Technical Compliance

The rating of Technical Compliance has four stages: C (Compliant), LC (Largely compliant), PC Partially compliant), and NC (Non-compliant) for each of the 40 Recommendations.

Evaluation		Reasons
Compliant	C	No shortcomings
Largely compliant	LC	Only minor shortcomings
Partially compliant	PC	Moderate shortcomings
Non-compliant	NC	Significant shortcomings
Not applicable	NA	A requirement does not apply, due to the structural, legal or institutional features of a country

List of FATF 40 Recommendations

40 Recommendations					
1	Assessing risks and applying a risk-based approach	15	New technologies	29	Financial intelligence units
2	National Cooperation and Coordination	16	Wire transfers	30	Responsibilities of law enforcement and investigative authorities
3	Money laundering offence	17	Reliance on third parties	31	Powers of law enforcement and investigative authorities
4	Confiscation and provisional measures	18	Internal controls and foreign branches and subsidiaries	32	Cash Couriers
5	Terrorist financing offence	19	Higher-risk countries	33	Statistics
6	Targeted financial sanctions related to terrorism and terrorist financing	20	Reporting of suspicious transaction	34	Guidance and feedback
7	Targeted financial sanctions related to proliferation	21	Tipping-off and confidentiality	35	Sanctions
8	Non-profit organisations	22	DNFBPs: Customer due diligence	36	International instruments
9	Financial institution secrecy laws	23	DNFBPs: Other measures	37	Mutual legal assistance
10	Customer due diligence	24	Transparency and beneficial ownership of legal persons	38	Mutual legal assistance: freezing and confiscation
11	Record-keeping	25	Transparency and beneficial ownership of legal arrangements	39	Extradition
12	Politically exposed persons	26	Regulation and supervision of financial institutions	40	Other forms of international cooperation
13	Correspondent banking	27	Powers of supervisors		
14	Money or value transfer services	28	Regulation and supervision of DNFBPs		

DNFBPs : Designated Non-Financial Businesses and Professions

Source: Publications of FATF

(b) Rating of the effectiveness

The rating of the Immediate Outcomes has a four grade scale; High, Substantial, Moderate, and Low for each of 11 IO items.

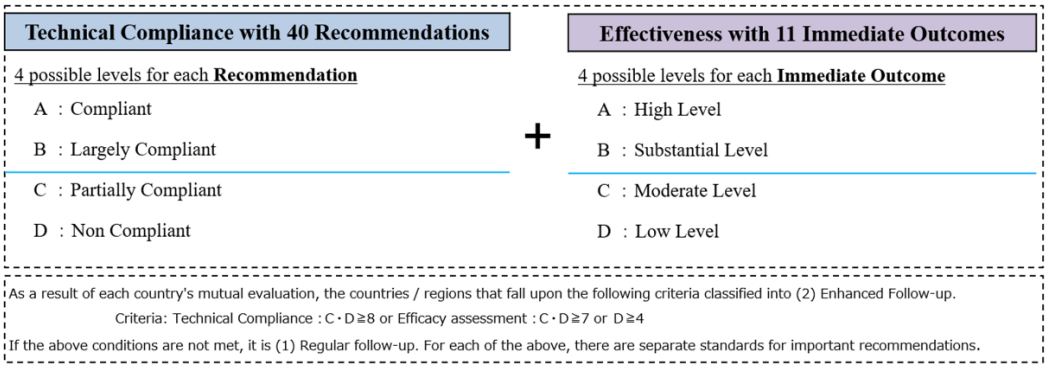
Table. List of Immediate Outcomes

High-Level Objective			
Financial systems and the broader economy are protected from the threats of money laundering and the financing of terrorism and proliferation, thereby strengthening financial sector integrity and contributing to safety and security.			
Intermediate Outcomes		**Immediate Outcome**	
1	Policy, coordination and cooperation mitigate the money laundering and financing of terrorism risks.	1	Money laundering and terrorist financing risks are Understood and, where appropriate, actions coordinated domestically to combat money laundering and the financing of terrorism and proliferation.
		2	International cooperation delivers appropriate information, financial intelligence, and evidence, and facilitates action against criminals and their assets.
2	Proceeds of crime and funds in support of terrorism are prevented from entering the financial and other sectors or are detected and reported by these sectors.	3	**Supervisors appropriately supervise, monitor and regulate financial institutions, DNFBPs and VASPs for compliance with AML/CFT requirements commensurate with their risks.**
		4	**Financial institutions, DNFBPs and VASPs adequately apply AML/CFT preventive measures commensurate with their risks, and report suspicious transactions.**
		5	Legal persons and arrangements are prevented from misuse for money laundering or terrorist financing, and information on their beneficial ownership is available to competent authorities without impediments.
3	Money laundering threats are detected and disrupted, and criminals are sanctioned and deprived of illicit proceeds. Terrorist financing threats are detected and disrupted, terrorists are deprived of resources, and those who finance terrorism are sanctioned, thereby contributing to the prevention of terrorist acts.	6	Financial intelligence and all other relevant information are appropriately used by competent authorities for money laundering and terrorist financing investigations.
		7	Money laundering offences and activities are investigated and offenders are prosecuted and subject to effective, proportionate and dissuasive sanctions.
		8	Proceeds and instrumentalities of crime are confiscated.
		9	Terrorist financing offences and activities are investigated and persons who finance terrorism are prosecuted and subject to effective, proportionate and dissuasive sanctions.
		10	Terrorists, terrorist organisations and terrorist financiers are prevented from raising, moving and using funds, and from abusing the NPO sector.
		11	Persons and entities involved in the proliferation of weapons of mass destruction are prevented from raising, moving and using funds, consistent with the relevant UNSCRs.

Source: Publications of FATF

(c) Final assessment decision and follow-up process

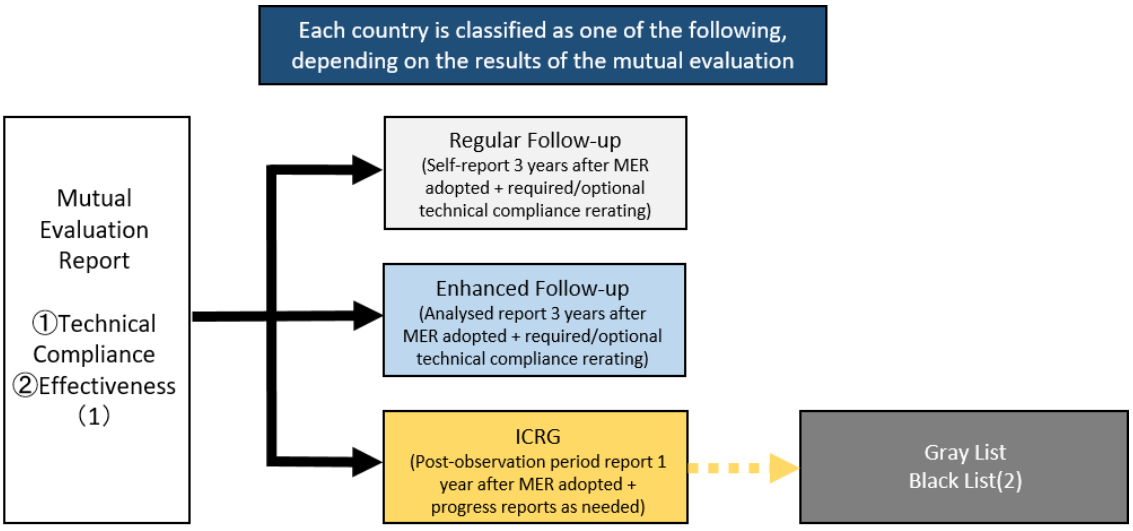
Adding all scores of the 40 Recommendations (TCs) and 11 IOs, the assessed countries are reviewed as either (1) regular follow-up or (2) enhanced follow-up. Once the Mutual Evaluation Report is published, a follow-up process will start for each category.



Source : ・Annual Report on Prevention of Transfer of Criminal Proceeds (2018), NPA
・June 14, 2019, Council on Customs, Tariff, Foreign Exchange and Other Transactions, 41st Subcouncil on Foreign Exchange and Other Transactions, MOF

B. Results of the 4th Mutual Evaluation

Depending on the results of the FATF mutual assessment, countries can be classified into one of the three categories: regular follow-up, enhanced follow-up, and countries under increased monitoring.



(1) The 4th round of mutual evaluation is conducted on ①TC and ②IO.
(2) North Korea and Iran are the only countries designated as being in the Black List.

If the assessment results are below certain conditions, the FATF will re-examine the deficiencies in the countries/regions after the one year follow-up period. The FATF will publish the name of the Enhanced follow-up/regions that have not made progress on the list as "Jurisdictions with strategic deficiencies." [52]

[52] As a result of each country's mutual evaluation, the countries/regions that fall under the following criteria enter the ICRG process.
Criteria: Technical Compliance : C / D ≥ 20 or Efficacy assessment : (C / D ≥ 9 and D ≥ 2) or D ≥ 6

List of high-risk countries and countries/regions subject to monitoring

Jurisdictions with strategic deficiencies	Source countries as of March 2022
Countries that are politically committed to make an improvement but have strategic shortcomings and are encouraged to take actions. (Jurisdictions Subject to Enhanced Monitoring Grey List)	Albania, Barbados, Burkina Faso, Cambodia, Cayman Islands, Haiti, Jamaica, Jordan, Mali, Malta, Morocco, Myanmar, Nicaragua, Pakistan, Panama, Philippines, Senegal, South Sudan, Syria, Turkey, Uganda, United Arab Emirates, Yemen.
High-Risk Jurisdictions subject to a Call for Action (High-risk Blacklist Countries)	North Korea, Iran

When the FATF announces high-risk jurisdictions and jurisdictions under increased monitoring, financial authorities of FATF member jurisdictions will instruct their FIs to strengthen AML/CFT/CPF in transactions with FIs of the announced country on the grounds that AML/CFT/CPF in the country is insufficient, in accordance with Recommendation 19 (Higher-risk countries).

For high-risk jurisdictions in particular, FIs that have been instructed to do so will be required to tighten screening procedures for transactions with FIs in those high risk countries. For example, FIs in the high risk countries will be required to provide detailed explanations on AML/CFT/CPF operations and information on the status of their control framework.

As a result, there is a possibility that FIs in high-risk countries and countries subject to monitoring may delay transactions or that FIs may be avoided by foreign FIs when making a transactions, which could have an impact on the real economy and trade transactions of the countries listed by the FATF.

Reference FATF Recommendation 19 (Higher-risk countries)

- Financial institutions should apply enhanced due diligence measures to business relationships and transactions with natural and legal persons, and financial institutions, from countries for which this is called for by the FATF. The type of enhanced due diligence measures applied should be effective and proportionate to the risks.
- Countries should be able to apply appropriate countermeasures[53] when called upon by the FATF. Countries should also be able to apply countermeasures independently of any call by the FATF to do so. Such countermeasures should be effective and proportionate to the risks.

2. Results of the 4th round of Mutual Evaluation of Japan

In the 4th round of Mutual Evaluation of Japan, while Japan has been recognized for achieving the AML/CFT/CPF measures based on the various efforts made since the previous evaluation, the overall conclusion was "Enhanced follow-up." The Evaluation Reports says that Japan should mainly address the problem of supervision and inspection of FIs, prevention of misuse of corporations, investigation and prosecution, in order to further improve Japan's countermeasures.

As of the end of March 2022, 19 of the 30 countries and regions that have already been reviewed were designated as "Enhanced follow-up," including the United States and Canada in the G-7. Regular follow-up, which has received a higher rating on AML/CFT/CPF's effectiveness, currently comprises eight countries and regions, including the United Kingdom and Italy among the G-7. At the same time that Mutual Evaluation Report is published, the FATF Member States will begin a follow-up process on Recommendation matters.[54]

[53] Interpretive note to recommendation 19 raises following actions as examples: (1) Limiting business relationships or financial transactions with the identified country or persons in that country; (2) Requiring financial institutions to review and amend, or if necessary terminate, correspondent relationships with financial institutions in the country concerned.

[54] The results of the mutual reviews of Germany and France among the G7 countries have not yet been made public.

Table: Results from FATF Member States that underwent the 4th mutual review

Classification	Country
Regular follow-up (8 countries/regions)	Spain, Italy, Portugal, Israel, UK, Greece, Hong Kong (China), Russia
Enhanced follow-up (19 countries)	Norway, Australia, Belgium, Malaysia, Austria, Canada, Singapore, Switzerland, US, Sweden, Denmark, Ireland, Mexico, Saudi Arabia, China, Finland, South Korea, New Zealand, Japan
ICRG (three countries)	Iceland, Turkey, South Africa

(1) Chapter 5: Preventive Measures (IO. 4)

IO. 4 examines the effectiveness of measures for FIs and DNFBPs based on interviews with FIs and other relevant authorities and materials submitted, and the Key Findings and Recommended Actions were showed as follows:

Key Findings

IO.4 Key Findings	
For financial institutions	
a)	Some FIs have a reasonable understanding of their ML/TF risks, including bigger banks (such as global systemically important banks, which are identified as higher risk institutions) and some MVTS. Other FIs still have a limited understanding of their ML/TF risks. They generally refer to standard categories of risks pointed out by the supervisor, mainly based on the conclusions of the NRA, even if those risks are not relevant to their own business. FIs do not have a deep understanding of the relationship between predicate offences and ML and how the proceeds of crimes enter the banking system, other than via cash transactions.
b)	Where FIs have a limited understanding of ML/TF risks, this has a direct impact on the application of the risk-based approach (RBA). Although some FIs have started conducting their own risk assessment and applying mitigation measures in line with the identified risks, other FIs apply mitigation measures uniformly, and do not go beyond the application of customer's identity verification and confirmation of transactions and STR.
c)	FIs appear to understand TF risk based on proximity to conflict regions, indicating that other types of TF in the financial sector might be neither reported nor investigated. FIs approach transactions with connections to higher risk countries such as Iran and DPRK with extra care.
d)	The adoption of the 2018 JFSA AML/CFT supervisory and enforceable Guidelines was a milestone to help FIs understand and implement their AML/CFT obligations. However, the level of this standard should be increased to ensure effective AML/CFT systems for all FIs, commensurate with their risks.
e)	A relevant part of FIs still do not have a clear and uniform understanding of basic AML/CFT concepts, especially the obligations which have recently been introduced/modified, such as beneficial ownership (BO) identification/verification and the ongoing CDD. Basic transaction monitoring systems are already in place to some extent within some FIs, while transaction screening systems are implemented by most FIs, both with limited effectiveness. FIs have a general awareness of the need to enhance their AML/CFT frameworks and practices to meet the new legislative/regulatory/supervisory obligations. However, deadlines are imposed by the supervisors only to FIs subject to direct supervisory action. Other FIs set up their own deadlines for complying with their AML/CFT obligations which tend to have extended duration. Consequently, there are serious concerns regarding FIs' timely improvement of their customer knowledge and application of adequate AML/CFT mitigation measures.
f)	FIs collect basic customer's information, which limits their knowledge and this information is usually not updated. FIs do not usually perform customer risk rating based on the characteristics of their customers nor make connections between the customer's profile and transactions records. Some FIs recently started conducting full CDD when on-boarding customers. The widespread practice of accounts being sold or stolen is a severe issue FIs face. All these elements raise further concerns on the quality and effectiveness of CDD.
g)	FIs, with few exceptions, do not apply proper EDD measures to higher risk customers, as they usually limit their enhanced measures to the customer's identity verification method and to list screening.
h)	The overall number of STRs filed per year is increasing. Most come from the financial sector, with one third from the bigger banks and refer to basic typologies and indicators, based on the FIU (JAFIC) guidance.
i)	Almost all banks have established AML/CFT internal controls, policies and procedures. Other FIs apply more basic internal controls but most of them have a compliance function that includes AML/CFT measures.
j)	Industry associations, working together with JFSA, play a role in educating FIs on AML/CFT obligations, as well as in communicating supervisory expectations. Despite their efforts, the average level of awareness of AML/CFT measures remains insufficient.

For Virtual Asset Service Providers	
a)	Virtual Currency Exchange Service Providers (VCEPs) have been under an obligation to register and have been appropriately regulated and supervised for AML/CFT purposes since 2017. 19 VCEPs have registered so far.
b)	VCEPs have general knowledge about the crime risks associated with VC activities. Their understanding of TF risks is generally limited.
c)	VCEPs tend to apply basic AML/CFT requirements. Some VCEPs apply enhanced measures to assist them in verifying the customer's identity. In general, they do not have specific policies to tailor mitigation measures to their risks or to apply EDD or specific CDD measures.
d)	VCEPs' STR reporting increased by more than 900% (more than 7 000 reports in 2018) since the obligation was introduced in 2017. This was mainly the result of a series of awareness-raising events and guidance provided jointly by the FIU and JVCEA.

Recommended Actions

IO.4 Recommended Actions	
For financial institutions	
a)	Continue taking appropriate raising-awareness and training initiatives to promote a change in FIs' compliance culture based on ML/TF risks, support a better understanding of ML/TF risks and AML/CFT obligations, with the involvement of supervisory authorities.
b)	Require that all FIs develop adequate risk assessments, tailored to their own business, products, services and customers.
c)	Upgrade the 2018 JFSA AML/CFT Guidelines by integrating the standards set in the Benchmarks for the Three Mega Banks, on a proportionate basis. The need for an appropriate transaction monitoring system should be strengthened and links with an appropriate ongoing CDD clarified.
d)	Define prescriptive and appropriate timetables for all FIs to implement the new legislative / regulatory / supervisory obligations.
e)	Ensure that FIs improve their customers' information verification methods and fully implement ongoing CDD requirements, based on comprehensive and dynamic customers' risk profiles, which take into account transactions records.
f)	Ensure that FIs implement appropriate and comprehensive information systems- taking into account proportionality criteria regarding the complexity of FIs - that integrate CDD data and transaction monitoring, with transaction monitoring parameters attuned to FIs' business, to the identified risks and to customers' behaviour and risk profiles and based on appropriate detection scenarios.
For Virtual Asset Service Providers	
a)	Ensure the timely implementation of the newly adopted AML/CFT requirements to custodial wallet services.
b)	Ensure that VCEPs and custodial wallet service providers are subject to wire transfer obligations once the 'travel rule' solution has been developed.
c)	Continue improving VASPs' understanding of ML/TF risks, and ensure that all new technological developments (such as new business models, proposed VC listings and other innovations associated to VC) are analysed taking into account ML/TF risks.
d)	Continue strengthening the culture of compliance of VASPs through provision of the necessary guidance and support for the understanding and implementation of AML/CFT requirements, with specific emphasis on their own risk assessment and the implementation of the full set of AML/CFT requirements on that basis.
e)	Refine and adjust the guidance provided for reporting suspicious transactions with a view to provide more elaborated scenarios tailored to the specificities of VASPs activities.

Overall Conclusion on IO.4

The conclusion on IO. 4 is as follows; the effectiveness of IO. 4 was rated at the third of the four, "Moderate Level."

Some FIs have a reasonable understanding of their ML/TF risks (including bigger banks and some MVTS), while other obliged entities (FIs, VCEPs and DNFBPs) have a limited understanding of their ML/TF risks. Although FIs have a better awareness of their AML/CFT obligations, the implementation of these obligations is uneven among different FIs. Although some FIs have started conducting their own risk assessment and applying mitigation measures in line with the identified risks, other FIs apply mitigation measures uniformly, and do not go beyond customer's identity verification or the application of basic transaction screening. In addition, FIs generally do not adequately implement the recently introduced or modified obligations, such as ongoing CDD and BO identification/verification, due to limited understanding of these concepts and the lack of deadlines to meet the new obligations. Transaction monitoring systems,

even where already in place, need to be substantially enhanced and integrated with the new CDD tools. The obligations required by the 2018 JFSA AML/CFT enforceable Guidelines also need to be upgraded to ensure effective AML/CFT systems for all FIs, commensurate with their risks.

Other obliged entities –VCEPs and DNFBPs- are at an early stage in compliance with AML/CFT requirements. Suspicious transaction reporting is increasing, especially regarding VCEPs, but involves only basic typologies and indicators. Not all DNFBPs are under reporting obligations.

Considering Japan's role as one of the most important financial hubs in the region, the importance of financial sectors in the Japanese context, and banks being exposed to significant ML/TF risks, as well as the emergence of the VCEP sector with its unique ML/TF risks, major improvements are still needed for IO 4.

Japan is rated as having a moderate level of effectiveness for IO.4.

(2) Chapter 6 : Supervision (IO. 3)

IO. 3 examines the effectiveness of the supervisory authorities for FIs and DNFBPs. The examination of the regulatory and supervisory framework of the authorities was based on the discussions with the relevant authorities and the submitted materials, and the Key Findings and Recommended Actions of the assessment were shown as follows.

Key Findings

IO.3 Key Findings	
For financial institutions	
a)	In general, supervisory authorities conduct standard "fit and proper" reviews for major shareholders and managers of financial institutions (FIs). The checks on beneficial owners (BO) are limited by the challenges linked to the identification of BO (see IO5).
b)	The detection of unregistered/unlicensed FIs is based on information gathered by competent authorities and third parties. Competent authorities force detected unlicensed entities to shut down their business and publicize the measures in case detected entities do not comply, bringing reputational consequences to the managers.
c)	Risk knowledge and understanding differ among the various financial supervisors, but are for the most part adequate. Financial supervisors, in order to identify and understand the ML/TF risks to which FIs are exposed, mainly rely on supervisory information, which provides an appropriate source of information.
d)	The Japanese Financial Services Agency (JFSA) plays a leading role in AML/CFT supervision, given its large supervisory scope. Until 2017, AML/CFT supervision was a component of the prudential supervisory approach conducted by the JFSA and the other supervisory authorities. In 2018, JFSA established a dedicated AML/CFT Policy Office and adopted AML/CFT enforceable Guidelines. These were important steps to upgrade AML/CFT supervision and the implementation of mitigation measures by FIs.
e)	The 2018 JFSA AML/CFT Guidelines help FIs understand their gaps and implement their AML/CFT obligations. Supervisory guidance on how to implement the Guidelines in practice still needs to be developed and clear and prescriptive deadlines need to be imposed to FIs to promptly reach full compliance with the Guidelines. The lack of these deadlines for the whole financial sector weakens the effectiveness of the Guidelines and the gap analysis carried by the FIs. Similar Guidelines are being adopted by other supervisors.
f)	JFSA's AML/CFT supervision on a risk-basis is still at an early stage but is gradually improving. An initial risk classification of FIs is in place, even though at this stage, the RBA is still mostly driven by inherent risks. Weaknesses in AML/CFT safeguards in place are also considered and assessed to target FIs subject to closer monitoring. The other supervisory authorities are at an earlier stage than JFSA in their implementation of a RBA and understanding of risks.
g)	AML/CFT supervisory focus is on bigger banks and VCEPs, which is appropriate from a RBA perspective. The number of AML/CFT targeted on-site inspections of FIs is limited. The supervisory focus on the three mega banks is based on a "through-the-year supervision" that encompasses permanent off-site monitoring and frequent meetings with FIs. For other FIs the supervisory approach is based on periodical submission of information and specific on-site/off-site activities when necessary, which is adequate.
h)	The Ministry of Finance (MOF) concentrates its TFS supervision on FIs that conduct international business, which is appropriate, but inadequately supervises smaller FIs.
i)	The effectiveness of the supervision seems to be mostly limited to the FIs which are subject to direct dialogue with supervisors conducted primarily by the JFSA. Similar efforts should extend to the whole financial sector as the engagement by FIs in fulfilling the new AML/CFT standard is uneven and the effectiveness is questionable. Supervisors can only impose administrative orders for non-compliance and publicize the severe ones (business improvement and business suspension orders), with a dissuasive effect on the system given by the potential reputational damage. While reporting orders are frequently issued to FIs, accompanied by a tight monitoring by the JFSA, public sanctions are rarely imposed, despite the general deterrent effect of improving compliance across the sector. The extended duration for completion of remediation plans weakens their effectiveness.

For Virtual Asset Service Providers	
a)	The JFSA's dedicated team for the supervision of VCEPs has a sophisticated understanding of the risks associated with the VC ecosystem and the range of VC services and products, including ML/TF risks to some extent.
b)	JFSA's periodic collection of information on inherent risks and mitigating controls (see IO 4) is used for JFSA's supervision of the registered providers.
c)	JFSA has conducted inspections on VCEPs in 2018 in response to a major hacking incident. Those inspections revealed weaknesses in internal control/governance systems which in general were not commensurate with the rapid increase of VC transactions (see IO 4).
d)	Given the recent regulation and supervision of VCEPs, there is a substantial body of cases where sanctions have been imposed, including business suspension orders which shows a more forceful approach to the one applied to FIs. However, the main failures involved consumer protection failings (i.e. the safeguard of customers' funds) that justify the severity of the sanctions applied.
e)	Through its dedicated team, JFSA has provided a targeted and timely policy and supervisory response to the VCEP sector.

Recommended actions

IO.3 Recommended Actions	
For financial institutions	
a)	Review the appropriate resources allocation to full time AML/CFT supervision and consider their enhancement to strengthen the supervision To review the assignment of staff specializing in AML/CTF-related supervision and examine the reinforcement of supervision.
b)	Require financial supervisors to enhance the supervision on a risk-basis, through the development/completion of adequate risk analysis for all supervised FIs.
c)	Conduct risk-based, TF-prevention outreach among FIs, modelled after that of PF TFS and drawing on the expertise of counterterrorism experts in NPA Security Bureau and JAFIC and require more joint supervisory inspections between JFSA and the MOF.
d)	Strengthen and expand AML/CFT dedicated supervisory activities, following a RBA, based on a combination of off-site reviews and onsite inspections, and extend and deepen the scope of assessment.
e)	Encourage better coordination between the JFSA and other financial supervisors, especially for the supervision of TFS which is the MOF's responsibility. Promote FIs' understanding of AML/CFT obligations and ML/TF risks by publishing supervisory guidance and good practices for the implementation of the JFSA Guidelines, with clear supervisory expectations on the preventive measures to be put in place by any FIs.
f)	Require clear and prescriptive deadlines for the whole financial sector to comply with the applicable AML/CFT framework and address the identified gaps, ensuring that higher risk FIs accelerate their compliance process.
g)	Review the appropriateness of the range of available sanctions, to ensure that the non-compliance with AML/CFT requirements is effectively and proportionately sanctioned and assure that sanctions are applied in practice.
h)	Enhance trainings on AML/CFT and associated ML/TF risks for all supervisors.
i)	Reinforce the coordination between national and local supervision, namely Local Finance Bureaus (LFBs).
For Virtual Asset Service Providers	
a)	Require the enhancement of existing ML/TF risk mapping tools of all registered VASPs leading to the risk classification of VASPs. This could include the types of virtual assets offered, the extent to which customers' virtual assets are held in hot wallets (online) as opposed to cold storage (offline) and whether the VASPs use analytical tools to track the flow of virtual assets.
b)	Design an AML/CFT supervisory program me on the basis of the VASPs' risk classification that involves proactive onsite inspections on a regular basis, the identification of the controls most exposed to risks and their regular review.
c)	Provide comprehensive, practical guidance for VASPs on ML/TF risks, the risk assessment process, AML/CFT requirements and supervisory expectations regarding their implementation.
d)	Ensure that resources allocated to VASP supervision remains adequate, in terms of number and expertise, and is strengthened in line with the growth of the market and the registration of new entities.

Overall Conclusion on IO.3

Overall conclusion on IO. 3 was assessed as Moderate Level as follows:

Financial supervisors have taken positive steps to conduct AML/CFT supervision on a risk-basis; the process is at an early stage, it is ongoing and is gradually improving. The JFSA has developed relevant tools, has sufficient risk knowledge and understanding, and demonstrated a proactive approach to supervision. Nevertheless there is large room for enhancement, while the effectiveness of supervisory actions on FIs compliance is affected by the slow approach to change shown by FIs in Japan. Supervisory authorities, to take actions in order to promote FIs' compliance, should reconsider the use, effectiveness and dissuasiveness of the range of sanctions.

The JFSA has taken prompt and adequate actions to address VC exchange service providers' AML/CFT issues, including imposing dissuasive sanctions, and

the JFSA is on the path to expand these efforts to other FIs on a risk-basis.

The major gaps in AML/CFT supervision of DNFBP sectors are an important area of concern but the weight of these weaknesses is more limited in the Japanese context given the less significant weight of these sectors.

Given the most significant weight and materiality of the Japanese banking sector and also the significant weight of the VC exchange service sector and the major supervisory role of the JFSA, the effectiveness of supervision in Japan still requires major improvements.

Japan is rated as having a moderate level of effectiveness for IO.3.

Chapter 4. FSA's Initiatives on AML/CFT/CPF

1. Establishment and revision of Guidelines

Since the publication of the Guidelines in February 2018, the FSA has monitored FIs based on the Guidelines in order to promote AML/CFT/CPF measures.

Taking into account the facts identified from the monitoring, the FSA revised the Guidelines for the first time in April 2019 and for the second time in February 2021 in order to clarify the intent of the Guidelines and to promote the effective development of FIs' control frameworks by providing new points to be considered.

The main changes are as follows:

(1) Involvement and understanding of management

The ML/TF risk management framework needs to be developed in a comprehensive manner by allocating various resources, and the management is responsible for this. However, some FIs are thought to be unable to promote AML/CFT/CPF measures due to inadequate involvement of management. Therefore, the involvement of the board was clarified by introducing the new expression "It is essential for the Board to take the initiative" and calling for appropriate support and guidance for the relevant divisions.

(2) Risk Identification and Assessment

(a) Risk identification and assessment process

As some FIs failed to comprehensively and specifically evaluate risks because of not covering all products and services they handle in risk assessment, or because of confusing risk identification with assessment. Therefore, the distinction between risk identification and risk assessment was clarified by showing that both processes are linked.

(b) Evaluate the risk control framework of alliance/business partner, etc. prior to offering new products and services

FIs are obliged to develop a risk control framework to ensure that their businesses and services are not abused in ML/TF. When providing new products and services through business alliances, it is necessary to evaluate ML/TF risks,

including the effectiveness of the risk control framework taken by the business partners, as part of their own risk management, before providing such products and services.

(c) Analysis of Suspicious Transaction Reports, etc.

The results of analyzing suspicious transaction reports in a risk assessment were clarified as "required actions," thereby requiring FIs to more specifically assess the risks they face.

(3) CDD

(a) Customer risk assessment

In order to reduce ML/TF risks, it has been emphasized by the FSA that it is essential for FIs to have a process for assessing the risks of all customers and to take risk mitigation measures in accordance with those assessed risks. On the other hand, some FIs conducted customer risk assessments that are inconsistent with enterprise-wide risk assessments by formally applying scoring and ratings based on customer attributes and transaction details, etc., thus the FSA demonstrated in revised guidelines once again that it is important for FIs to conduct customer risk assessments for all customers based on enterprise-wide risk assessments.

(b) Additional Measures for High-Risk Transactions, etc.

There were cases where unnatural cross-border remittances were executed, which were caused by a lack of confirmation in terms of consistency between customer's business and its transactions. To identify and stop such high-risk transactions, it was clarified that additional measures, such as identifying the actual business conditions and locations, are required prior to the commencement of transactions or when a large amount of transactions are conducted.

(c) Simplified risk-based customer due diligence (SDD)

In order to avoid confusion with "transactions for which simplified due diligence is acceptable" prescribed in the APTCP framework and to clarify the

content of SDD, the wording used in the Guidelines was revised to "simplified risk-based customer due diligence (SDD)" and the following example was added: "Taking into account the nature of the risk, such as varying the scope, methods, and frequency of investigation and updating of customer information, raising the threshold for monitoring transactions conducted by customers may also be considered." Approaches and examples of SDD are described in the FAQ, and reasonable consideration is encouraged for each FI. For example, with regard to accounts that meet certain criteria, the FAQ shows that it is possible to defer the periodic assessment at a risk-based frequency subject to an appropriately established transaction monitoring system, since the accounts can be deemed unlikely to be traded for ML purposes.

It is necessary for each FI to make reasonable judgments on SDD approaches while referring to the FAQ. However, the FSA has clarified the points to be kept in mind again in the revised FAQ published in March 2022, and it will present its view on rational ways of utilizing SDD and ways of managing customers subject to SDD through introductions to good practices.[55,56]

(d) Linking customer risk assessment and transaction monitoring

From the perspective of a risk-based approach, the content of risk mitigation measures needs to be linked with customer risk assessments revised based on Ongoing Customer Due Diligence. Therefore, a statement was added to the revised guidelines to the effect that that customer risk assessments revised based on Ongoing Customer Due Diligence should be appropriately reflected in transaction monitoring.

(4) Transaction monitoring and filtering

With respect to transaction monitoring and filtering, since each required action for FIs is different, these two items should be separately addressed. With respect to screening (transaction filtering), the FSA has decided to require FIs to take actions such as incorporating newly designated persons subject to economic

[55] It is necessary to conduct constant monitoring using a transaction monitoring system with appropriately set thresholds, and when it is detected that funds have started to move, it is necessary to immediately contact the customer to understand the actual state of account use and investigate it as necessary.

[56] Frequently asked questions (FAQs) are described in Chapter 4, "2. Frequently Asked Questions (FAQs) on the Guidelines".

sanctions into their own sanctions list without delay and checking all existing customers and their beneficial owners.[57]

(5) Cross-border remittances

With regard to cross-border remittances, it was added to the revised guidelines that confirming the control framework and reviewing the risk assessment of correspondent FIs and outsourcer FIs entrusting other FIs with cross-border operations are required because correspondent contracts with foreign FIs are a prerequisite for cross-border remittances and there are many outsourcing cases where other FIs are entrusted with remittance.

(6) Financing and extending credit involving trade based finance

Compared to domestic transactions, it is easy to abuse trade finance for illicit purposes due to the fact that it is more difficult to verify the actual condition of import/export transactions, and it is easy to transfer the proceeds of crime by disguising import/export transactions or manipulating the price on an invoice.

When FIs provide guarantees in the event of default, performance guarantees, or financing based on import/export transactions, it is necessary for them to be aware of the ML/TF risks attached to trade activities and that such actions may be misused for ML/TF through the above-mentioned method. Therefore, in addition to the "Cross-border wire transfers and similar transactions" section above, a new section titled "Financing and extending credit involving trade-based finance" has been added.

2. Frequently Asked Questions (FAQs) about the Guidelines

Following the revision of the Guidelines mentioned in section 1 above, the FSA formulated and published "Answers to Frequently Asked Questions Regarding "Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism"(FAQ)" in March 2021 in order to clarify "required actions" of the Guidelines and to accelerate the effective development of a control framework for FIs. In addition, the FAQ was revised in March 2022 in order to further clarify the

[57] If sanctions are designated by the UNSC Resolution, verification of the list is required within 24 hours of designation, and if sanctions are designated by the laws and regulations of each country, including Japan, verification of the list is required immediately.

points to be noted in SDD.

The FAQ provides details, concepts, and specific examples of how to respond to all "required actions" in the Guidelines.

FIs are required to reconfirm whether they have properly developed a control framework in accordance with the FAQ that clarifies the Guidelines and with the concept of the Guidelines, including the revised points of the Guidelines. If a gap with the current situation is recognized, they are required to appropriately formulate and implement a specific plan to address the gap identified.

3. Requests for reporting of quantitative and qualitative information on the status of AML/CFT/CPF execution by FIs

The FSA published the Guidelines in February 2018 and, requested each regulated entity to report quantitative and qualitative information on their transactions and current status of control-framework development from March 2018 in order for the FSA to regularly identify their transactions, their status of control framework, and the effectiveness of their AML/CFT/CPF practices.

Furthermore, from May to June 2018, the FSA requested them to analyze the gaps between the "required actions" of the Guidelines and their status of AML/CFT/CPF practices, and to prepare and implement a remedial action plan to address the gaps identified.[58]

Since then, the FSA has required regulated entities to annually report on their transactions and analyses on the gaps mentioned above every March. In September 2021, the FSA conducted a questionnaire survey on them in order to confirm the progress of the enhancement of the control framework as of September 2021 in more detail.

Based on quantitative and qualitative information collected from FIs, etc., the FSA has identified and assessed the risks of each sector and FIs (Corporate Risk Rating ("CRR")), and monitors the progress of individual FIs' development of ML/TF risk control.

In March 2021, the items required to be reported by FIs, etc. and the risk

[58] For the three mega banks, FSA issued "AML/CFT benchmarks for three mega banks" requiring the mega banks to develop the control framework which is applied group-widely and globally in addition to the Guidelines and to analyze the gaps between the actions required by the benchmarks and their current AML/CFT practices and to prepare a remedial action plan to address the gaps identified.

assessment method were changed in order to upgrade CRR, partly because the level of "required actions" was raised by the revision of the Guidelines.

4. Clear indication of the deadline for the development of a control environment for AML/CFT/CPF measures

In April 2021, in light of the fact that three years had passed since the Guidelines were formulated and published, and that awareness of control-framework development had permeated FIs, the FSA notified FIs of the completion deadline for all items in "required actions" of the Guidelines (March 2024) through various industry associations and posted a request to FIs to develop a more effective control framework on the FSA's website.

In the Guidelines, "development of a control framework" required here means that all "required actions" have been completed, including the creation of organizations, policies and procedures. In the FSA, measures are being taken to ensure that the development of a control framework is completed at an early stage. Measures include monitoring, inspections, and reporting of FIs to monitor the progress of control-framework development at FIs on a daily basis. At the same time, efforts are being made to clarify the matters that FIs should address through outreach activities, such as study sessions.

However, it has been pointed out that some items in the guidelines are difficult to fully address only by the efforts of FIs. For example, in Ongoing Customer Due Diligence, FIs are required to review their customer risk assessments based on the information obtained by sending questionnaires to customers to confirm their transaction information. However, there are some cases where FIs have difficulties in updating customer's information as they do not receive any replies from customers even after mailing them. In Ongoing Customer Due Diligence, FIs utilize various channels to promote Ongoing Customer Due Diligence, such as contacting customers at branches, updating information on internet sites and applications, and printing a message asking for information updates on a bill after using ATMs, in addition to mailing. Although the optimal channel and means of contacting customers vary among banks, it is important for FIs to utilize their available resources to try to grasp the actual situation of more customers by the deadline to complete the response (March 2024).

5. Implementation of inspections focusing on AML/CFT/CPF measures

Since FY 2021, as part of strengthening risk-based inspection and supervision, the FSA has intensively conducted inspections that focus on the ML/TF risk control framework, giving priority to businesses in FIs where ML/TF risks are considered high.

The FSA cooperates with relevant Ministries and Agencies, including Local Finance Bureaus[59], to conduct inspections. As necessary, in order to avoid placing an excessive burden on FIs, the FSA avoids duplication with inspections and on-site examinations by other authorities and promotes the use of a video conference system that takes into account the COVID-19 situation. The FSA will flexibly conduct inspections while taking into account the impact of COVID-19 from now on.

6. Sharing of systems related to AML/CFT/CPF measures

The Future Investment Council in October 2019 requested that future regulatory approaches be considered in the three fields of mobility, finance, and architecture, given that AI-based big data analytics give rise to the significant possibility of establishing regulatory systems that do not rely on existing uniform methods. The New Energy and Industrial Technology Development Organization (NEDO) invited public offerings for research projects, and the Japanese Bankers Association (JBA) and KPMG SA (KPMG) were responsible for the research field and NEC Corporation (NEC) for the R & D field in the area of finance. Since April 2020, the three companies started the research projects of AI-driven sharing AML/CFT/CPF systems.[60]

The background to this project is banks' huge costs for introducing and managing AML/CFT/CPF systems for transaction monitoring sanction screening (transaction filtering). At present, each financial institution individually installs and implements its own AML/CFT/CPF systems. These AML/CFT/CPF systems adopted by most FIs are very simple and need labor-intensive work to ensure efficiency and accuracy, such as checking for false positives. Also, the progress of IT technologies and the globalization of the economy require financial industries to comply with a higher level of international AML/CFT/CPF standards. The aim of this project is to verify the possibility of establishing an efficient, effective AML/CFT/CPF framework by

[59] Local Finance Bureaus, Fukuoka Local Finance Branch Bureau, and Okinawa General Bureau

[60] NEDO Implementation Framework for Developing Digital Technology for the Elaboration of Regulations
https://www.nedo.go.jp/koubo/CD3_100203.html
https://www.nedo.go.jp/koubo/CD3_100202.html

sharing AI-driven AML/CFT/CPF systems and find what regulatory improvements are required to share AML/CFT/CPF systems.

In this project, an AI-driven mini system was developed for (1) screening (transaction filtering) systems and (2) transaction monitoring systems and with the cooperation of FIs, the project team evaluated the accuracy of detection and judgment of an AI-based AML/CFT/CPF system using actual transaction data. The report was prepared in March 2021 (published by NEDO in July 2021).

The main results of the project are as follows:

- An AI model generated from real transaction data from several FIs filtered and monitored other FIs' transaction data. As a result, the accuracy of discrimination was high and its effectiveness was confirmed.
- It was confirmed that the AI model could improve operational efficiency, for example, by using the AI for primary judgment of transaction monitoring and transaction filtering, and reducing the work of the confirmation in secondary judgment by humans according to the AI-output scores.

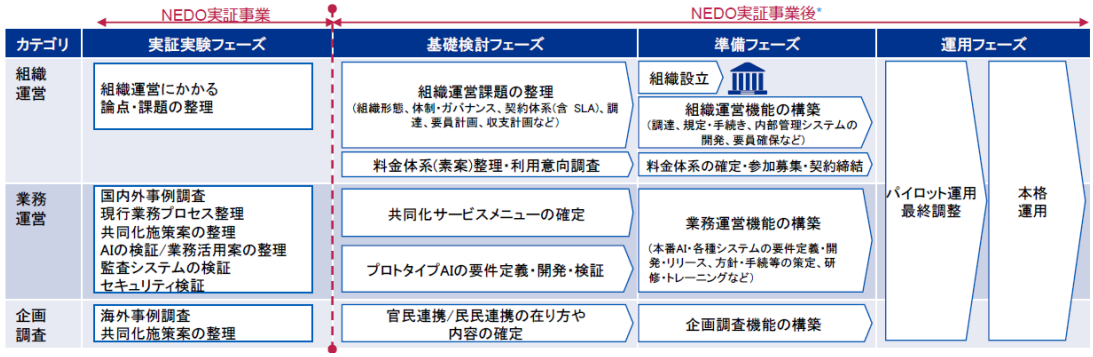
A report published by the FATF in July 2021 titled "STOCKTAKE ON DATA POOLING, Collaborative Analytics and Data Protection," introduces the NEDO's project of sharing AML/CFT/CPF systems in Japan as an advanced initiative aimed at enhancing screening (transaction filtering) and monitoring with AI models generated from transaction data.

Following this result of the project, the JBA established the Task Force on Sharing of AML/CFT/CPF Services in 2021 in order to discuss the expected services and management structure of shared AML/CFT/CPF systems. The Task Force is studying issues based on the roadmap for the practical application of the shared system shown in the NEDO report. In order to clarify the beneficiaries and the menu of services, the Task Force conducted a survey on member banks of the Regional Banks Association of Japan and the Second Association of Regional Banks in order to understand the situation and needs for AML/CFT/CPF systems. The Task force is considering clarifying common issues and discussing the scope of the shared systems based on this survey.[61]

[61] Press Conference by the Chairman of the JBA (July 15, 2021)
https://www.zenginkyo.or.jp/news/conference/2021/210715/

JBA's Roadmap for shared systems

	基礎検討フェーズ	準備フェーズ	運用フェーズ
組織運営	◘ 組織運営にかかる課題(組織形態、体制・ガバナンス、契約体系(含 サービスレベルアグリーメント)、調達、要員計画、収支計画など)を整理。	◘ 申請・届出などを行い、組織を設立。また、基盤の調達や内部管理機能など組織運営にかかる機能を構築し、運用開始の準備を完了。	◘ 一部参加機関に限定し、パイロット運用を実施。 ◘ 当該運用の結果を踏まえ最終調整を実施し、本格運用を開始、参加機関を徐々に拡大。
	◘ 料金体系(素案)を整理し、利用意向調査を実施。	◘ 料金体系を確定し、参加機関の募集や契約締結を開始。	
業務運営 企画調査	◘ 共同化のサービスメニュー等を確定する。 ◘ 実務に即した本番AIの開発に向け課題を整理するため、プロトタイプAIを開発。	◘ サービス提供等にかかる準備を完了。具体的には手続レベルの業務フローの整理や本番AI・システムのリリース、方針・手続の策定、トレーニングなど。	



Source: Excerpt from JBA Briefing Paper, Financial System Council, "PSA Working Group" (1st meeting), October 13, 2021 (Wednesday)

In light of this situation, the FSA established the Working Group on Payment Services" (provisional English title) of the Financial System Council in October 2021 to discuss measures for institutions that provide services for sharing AML/CFT/CPF systems. The Working Group discussed measures to ensure the quality of business operations of entities entrusted by banks, etc. (deposit-taking FIs and funds transfer service providers) that analyze whether customers are subject to sanctions in relation to exchange transactions and whether each transaction has suspicious points, and to notify banks, etc. of the results of such analysis. The Working Group published a report summarizing the results of its discussions on January 11, 2022.[62]

Based on the contents of this report, the FSA submitted to the Diet on March 4, 2022, a bill to amend the PSA for the Establishment of a Stable and Efficient Payment Services System, which will allow the authorities to conduct inspection and supervision in order to ensure the quality of business operations of firms that are entrusted by banks, etc. and provide screening (transaction filtering) services and other operations on banks' money transfer transactions in order to ensure the quality of business operations.

The FSA will continue to work with the financial industry to support its development of such sharing of AML/CFT systems and services.

---

62 Publication of the Report of the Working Group on Payment Services Working Group of the Financial System Council
https://www.fsa.go.jp/singi/singi_kinyu/tosin/20220111.html

7. Request for courteous customer service (including service for foreign nationals)

With regard to CDD, a core element of risk mitigation measures, ongoing CDD is one of the most important elements, and FIs/CESPs are making progress to complete it. However, there have been some cases in which customers have complained about updates of customer information to banks. In October 2020, the FSA, through industry associations, requested FIs/CESPs to provide more courteous explanations to customers.

Furthermore, risk-based CDD on foreign residents in Japan is required in accordance with the APTCP and other related laws and regulations as well as the Guidelines. In particular, in cases where an account of a foreign resident in Japan is expected to be closed in the near future, the FSA requires FIs/CESPs to identify and assess the risk of the account being sold or abused for financial crime and to take appropriate risk mitigation measures.

Given that the number of foreign nationals residing in Japan is expected to increase, in June 2019, the FSA, through industry associations, requested FIs/CESPs to take risk-based AML/CFT/CPF measures based on good communication with foreign nationals. In addition, the Ministerial Conference on the Acceptance and Coexistence of Foreign Human Resources decided "Comprehensive Measures for the Acceptance and Coexistence of Foreign Human Resources" in 2018. In order to further support foreign nationals, the FSA published "Points to Consider When Dealing with Foreign Customers," along with good practices by FIs as the "Examples of Dealing with Foreign Customers."

Following the FSA's actions above, while some FIs/CESPs are lagging behind in their efforts to deal with foreign residents as described below, others are advancing their efforts. Also, some FIs take into account cases where foreign residents are changing or extending their status of residence due to the recent spread of COVID-19.

It is not intended, in any case, to cause a situation in which a foreign national is unable to open a bank account just because of his/her nationality. FIs should also take actions to align with the COVID-19 measures for extension of the status of foreign residence, which was granted by law. The FSA will continue to require FIs/CESPs to take appropriate measures for dealing with customers, including foreign residents, related to AML/CFT/CPF measures.[63]

[63] Under the provisions of Article 20, Paragraph 6, and Article 21, Paragraph 4 of the

[Cases where delays in efforts were recognized]

- An FI has not been able to confirm the period of stay of existing foreign customers, or has not considered specific measures to ascertain the period of stay.
- An FI did not ascertain the exact number of foreign residents' accounts, and based on its self-assumption that such accounts were not large in number, it did not consider management methods, including the way to grasp information on existing foreign residents' accounts.

There were inappropriate cases in which: an FI inquired about periods of stay of permanent residents, including special permanent residents; and an FI set criteria for names that appear to be foreign nationals and asked customers with Japanese nationality about their period of stay. In both cases, the FSA asked both of the FIs to improve their measures.

[Examples of progress in initiatives]

- An FI, in cooperation with companies where foreign residents work, checked the expected period of stay of these foreign nationals, and the FI contacted each customer to check evidence, such as residence certificates, and reviewed their ratings.
- In order to prevent the sale accounts of foreign residents who already left Japan, an FI distributed leaflets in multiple languages.
- An FI took measures following the special regulations of Article 20, Paragraph 6 (change of status of residence) and Article 21, Paragraph 4 (renewal of status of residence) of the Immigration Control and Refugee Recognition Act.

8. Strengthening inter-agency cooperation

With regard to AML/CFT/CPF measures, not only FIs supervised by the FSA, but also other institutions under the APTCP, including other FIs and DNFBPs, are widely

Immigration Control and Refugee Recognition Act, if a disposition on an application filed before the expiration date of the period of stay is not made by the expiration date of the period of stay, the applicant may continue to reside in Japan with such status of residence even after the expiration date of the period of stay, either until the disposition is made or until two months pass from the expiration date of the previous period of stay, whichever comes first.

required to take risk-based measures. It is therefore important to ensure that no business becomes a loophole. The FSA cooperates closely and exchanges information with other authorities. Also, the FSA works with relevant ministries and agencies to follow-up on the FATF 4th Mutual Assessment of Japan, update the NRA, and implement joint financial inspection with foreign exchange inspections.

(1) Establishment of AML/CFT/CPF Policy Board

At the timing of the publication of the FATF 4th Mutual Evaluation Report of Japan, the AML/CFT/CPF Policy Council (hereinafter referred to as the "Policy Council"),[64] co-chaired by the National Police Agency and the Ministry of Finance, was established to work on the governmental AML/CFT/CPF policies. The "Government Action Plan" was published on August 30, 2021.

The purpose of the Policy Council is to plan and promote AML/CFT/CPF national policies and concrete actions based on them, and ensure close cooperation among the relevant authorities. The National Police Agency and the Ministry of Finance chairs the council. The FSA, the Ministry of Justice and the Ministry of Foreign Affairs serve as its secretary, and 17 Ministries and Agencies join the Policy Council.

At the first meeting on 19 August 2021, the Council approved the Government Action Plan, which sets out AML/CFT/CPFCFT policies and deadlines for the next three years. In the Action Plan, AML/CFT/CPF measures and supervision of FIs are required as follows:

[64] Ministry of Finance "Inter-Ministerial Council for Anti-Money Laundering (AML), Countering the Financing of Terrorism (CFT), and Countering Proliferation Financing (CPF) Policy"
https://www.mof.go.jp/policy/international_policy/councils/aml_cft_policy/index.html

Table: The Government Action Plan (excerpt)

2. Preventive measures by Financial Institutions (FIs) and Virtual Currency Exchange Providers (VCEPs) and Supervision				
	Outcome	Actions	Time frame	Authorities in Charge
(1)	Strengthening supervision of AML/CFT/CPF measures taken by FIs and VCEPs	Enhance coordination among financial supervisors for FIs' and VCEPs' implementation of AML/CFT/CPF measures, develop an appropriate supervisory regime, and strengthen risk-based supervision and inspection.	By autumn 2022	FSA, other financial supervisory authorities
(2)	Enhancing FIs' and VCEPs' understanding of risks and ensuring their appropriate risk assessments	Enhance FIs' and VCEPs' risk understanding and ensure that they conduct their own risk assessment by updating/developing supervisory guidelines and raising their awareness on AML/CFT/CPF obligations.	By autumn 2022	FSA, other financial supervisory authorities
(3)	Fully implementing ongoing customer due diligence by FIs and VCEPs	Enhance risk-based AML/CFT/CPF preventive measures taken by FIs and VCEPs, including ongoing customer due diligence, by settling a clear and prescriptive deadline for its implementation and by strengthening transaction monitoring.	By spring 2024	FSA, other financial supervisory authorities
(4)	Operationalizing a new shared information system for transaction screening and monitoring	Operationalize a new shared information system for transaction screening and monitoring to strengthen and further enhance the quality of verification at the time of transactions and customer due diligence measures, and also promote public understanding by utilizing the Government's public relations platforms.	By spring 2024	FSA

As mentioned above, the FSA has made efforts to strengthen AML/CFT/CPF supervision, including revising the Guidelines, publishing FAQs, and setting clear deadlines for all FIs to complete their AML/CFT/CPF measures. In addition, as stated in the "Basic Policies for Economic and Fiscal Management and Reform 2021," the FSA declares that the FSA strengthens the financial inspection and supervision with the Local Finance Bureaus. Based on the "Government Action Plan," the FSA will continue to cooperate with relevant authorities to promptly follow-up the recommendations by the FATF.

(2) Cooperation with other supervisory authorities of FIs

In order to effectively and efficiently ensure FIs' compliance with relevant laws and regulations, the FSA conducts joint financial inspections with foreign exchange inspections conducted by the Ministry of Finance utilizing the knowledge of the staff of both entities and reducing the burden on FIs. Both authorities adjust inspection targets for FIs, schedules, and checkpoints to be examined. The joint inspection framework is reviewed and revised as necessary to ensure efficient inspections and consider FIs' burden.

The FSA also supports AML/CFT/CPF inspection conducted by the Ministry of Health, Labour and Welfare, which supervises labour banks (Rokin Banks), by sharing viewpoints and offering training for inspectors.

(3) Establishment of Benefit Owner List System by Ministry of Justice

The APTCP requires specified business operators to confirm information on beneficial owners (BOs) in order to prevent abuse of corporation vehicles.

To ensure greater transparency about the ultimate ownership and control of legal persons, the FATF and other countries are reviewing standards and regulations. In Japan, the Ministry of Justice established a study group in April 2022 to utilize information on the beneficial owners of legal entities at the Commercial Registries and the FSA participated.[65]

With the conclusion of the study group, the beneficial owners List System[66] was started on January 31, 2022. The Commercial Registry Offices check documents of beneficial owners submitted by companies, etc. (users) and issues copies of a list of the beneficial owners of the companies. The copies of the beneficial owners list is expected to facilitate the confirmation of information on BOs. The FSA cooperates with the Ministry of Justice and encourages use of this system by the financial industry.

(4) Other activities with relevant authorities

- In order to improve supervisory activities in other financial sectors, the FSA cooperates in financial inspections and monitoring with the Ministry of Finance, Ministry of Economy, Trade and Industry, Ministry of Health, Labour and Welfare, Ministry of Agriculture, Forestry and Fisheries, and Ministry of Land, Infrastructure, Transport and Tourism. The FSA exchanges views and holds seminars as necessary with other relevant ministries and agencies, including the Cabinet Secretariat, Consumer Affairs Agency, Ministry of Justice, and Public Security Intelligence Agency.
- The FSA shared its risk-based supervisory activities with the authorities supervising DNFBPs (January and April 2021).
- The FSA has close cooperation with the Ministry of Finance, the National Police Agency, Ministry of Foreign Affairs, and Ministry of Justice, which are other leading agencies, and the main authorities of the FATF 4th Mutual Evaluation have meetings throughout the year.

---

[65] MOJ "Study Group on Promotion of Understanding of Information on Beneficial Owners of Corporations at Commercial Registry Offices" https://www.moj.go.jp/MINJI/minji06_00044.html
[66] MOJ "Establishment of the Beneficial Owners List System" https://www.moj.go.jp/MINJI/minji06_00116.html

- The FSA shares information of the financial sectors with the National Police Agency to prepare the annual NRA.
- The FSA, in collaboration with the Cabinet Secretariat (secretariat of the Growth Strategy Council), the Ministry of Economy, Trade and Industry, and the New Energy and Industrial Technology Development Organization (NEDO), promotes the project of the AML/CFT/CPF sharing system (October 2019 - March 2021).
- Based on the request by the National Tax Agency, the FSA added an explanation to the FAQ that "the Organized Crime Punishment Act was revised in June 2017 and the scope of predicate crimes was expanded to violations of various tax laws." Also, the FSA requested financial industry associations to widely encourage members to pay special attention to transactions that are suspected to be for the purpose of tax evasion (June 2021).
- The FSA conducts training for private business operators to promote understanding of ML/TF risks in cooperation with the National Police Agency (as appropriate). The National Police Agency and the FSA conduct outreach to Local Finance Bureaus in November (due to COVID-19, they have only distributed materials since 2020).

(5) Cooperation with Bank of Japan

Today, the environment of the financial system has become increasingly complex, and the risks that supervisors have to monitor have expanded, including climate change risk, cybersecurity, and ML/TF. In March 2021, the Bank of Japan and the FSA published "Initiatives for Further Strengthening Cooperation between the FSA and the Bank of Japan" to strengthen cooperation for higher-quality monitoring and reducing the burden on FIs. The Bank of Japan and the FSA work together in AML/CFT/CPF monitoring and inspection, which is important for maintaining the credibility of FIs in Japan.

9. Strengthening partnerships with private sector entities

It is important that management and all three defense lines have a broad understanding of the FSA's Guidelines to effectively promote AML/CFT/CPF measures. The government promotes public-private partnerships to enhance AML/CFT/CPF measures. The FSA cooperates with industry associations and Local Finance Bureaus and continuously conducts outreach activities, including

AML/CFT/CPF seminars for management.

(1) AML/CFT/CPF Public-Private Partnership Meeting

The AML/CFT/CPF Public-Private Partnership Meeting, which was established in April 2018, is composed of the FSA, the Ministry of Finance, the National Police Agency, the Ministry of Justice, the Bank of Japan, and industry associations supervised by the FS. The members share information and discuss issues to enhance AML/CFT/CPF measures.

Information shared by authority members concerns, for example, progress of the government's AML/CFT/CPF policies, results of AML/CFT/CPF inspection and monitoring, the latest national AML/CFT/CPF risk assessment results, and international discussions and issues at the FATF. Industry associations explain the progress of measures in each industry and the issues they face.

This meeting plays a central role in promoting public-private partnership across relevant authorities and financial sectors that provide support to enhance the AML/CFT/CPF measures of FIs.

(2) AML/CFT/CPF Study Group of the JBA

The JBA established the AML/CFT Study Group in June 2018 to study international practices and consider other AML/CFT/CPF issues, such as sharing AML/CFT/CPF operations among banks to enhance their AML/CFT/CPF measures. The FSA has joined the group as an observer. From April 2020 to March 2021, the group managed the sharing of the AML/CFT/CPF project, and it discussed problems facing the current AML/CFT/CPF operational flow and possible solutions through future sharing systems. The final report on the sharing system project reflected the group's discussions.

In January 2022, the group published the "Report on the Overseas Situation of Continuous Customer Due Diligence" about efficient methods for acquiring and updating customer attribute data at overseas mass retail FIs. This report is based on the results of the survey on efficient methods for performing continuous customer management in the United States, the United Kingdom, Germany, Sweden, Australia, Hong Kong, Singapore, and India. It summarized the situation of continuous customer due diligence in foreign countries, differences between the countries and reasons for them from Japanese banks, and the suggestions for Japanese banks.

(3) Conducting outreach and training for industry associations

The FSA has cooperated with the financial industry associations to further enhance AML/CFT/CPF measures. Taking into account the characteristics of each business sector, the FSA conducts various outreach activities for FIs, including regular meetings between associations and the FSA's executives. The FSA will continue to keep a close relationship with the associations and encourage discussions and improvements on their AML/CFT/CPF measures.

- In July 2019, the FSA announced that asset management companies, which generally outsource the sale of investment trusts and other investment products to other FIs, should identify and assess AML/CFT/CPF risks on their business, including the identification of the beneficial owners of the sales companies and monitoring of these company's AML/CFT/CPF management frameworks. They should also implement ongoing risk control on a risk basis.
- In June 2020, as financial crimes related to the COVID-19 pandemic and non-face-to-face transactions increased, the AML/CFT/CPF risks are estimated to increase, and it is necessary for FIs to take actions against these risks. The FSA informed the financial industries that risk-based flexible responses are expected to support customers' needs for funds due to COVID-19, which is an important social role for FIs.
- In June 2019, the FSA requested to implement the asset freeze without delay following the UNSCRs. In September and October 2020, it repeated the request to financial industries.
- In October 2020, the FSA requested courteous customer services of financial industries because there were many complaints about the CDD investigations by FIs that tried to update customer information as ongoing CDD. The FSA also organized simplified CDD approaches for low-risk customers and held seminars 40 times to explain simplified CDD.
- The FSA had seminars 24 times for financial industries to explain the contents and concepts of the Guidelines when revising the Guidelines and publishing the FAQ, and briefings seven times when requiring FIs to complete the Guidelines by March 2024.
- In June 2021, the National Police Agency and the FSA distributed training materials to FIs in order to deepen their understanding of the STR framework in Japan while taking into account the status of the COVID-19

pandemic.

- Based on the FATF 4th Mutual Evaluation Report for Japan and the Government Action Plan released on August 30, 2021, the FSA held briefing seminars on the summary of the FATF Mutual Evaluation Report and the Action Plan.
- The FSA participated in seminars and lectures hosted by domestic and overseas organizations and universities 27 times in total (in fiscal 2020).
- When the Panel of Experts of the UNSC Sanctions Committee on North Korea regularly publishes reports on sanction measures against North Korea, the FSA asked financial industry associations to take appropriate measures based on the reports. The FSA also provided FIs and related associations with lists of the vessels which may be involved in activities in violation of UN sanctions described in the reports, and exchanged views with experts of the UNSC Sanctions Panel on North Korea.
- The FSA, in cooperation with financial industry associations, holds study seminars that help the participants from member FIs to understand the "required actions" in the Guidelines and enhance the level of AML/CFT/CPF measures in the industry.

10. Public relations activities to increase general users' understanding

Users' understanding and cooperation is the key for FIs to smoothly implement AML/CFT/CPF measures. The FSA and financial industry associations continue public relations on the necessity of AML/CFT/CPF measures as follows.

The public relations by the JBA aimed to raise awareness of the need of ongoing CDD. The mediums included newspaper advertisements, TV commercial videos, and online advertisements that emphasize the importance of customer identification and the necessity of ongoing CDD.[67]

The National Association of Shinkin Banks prepared a leaflet jointly with the FSA explaining the purpose of updating customer information on ongoing CDD (available in 15 languages in addition to Japanese) and provided it to each Shinkin Bank to be displayed and distributed to users. It also produced a video on requests for

[67] It was published in the morning edition of the Yomiuri Shimbun on March 23, 2021, and carried out on November 25, 2019.

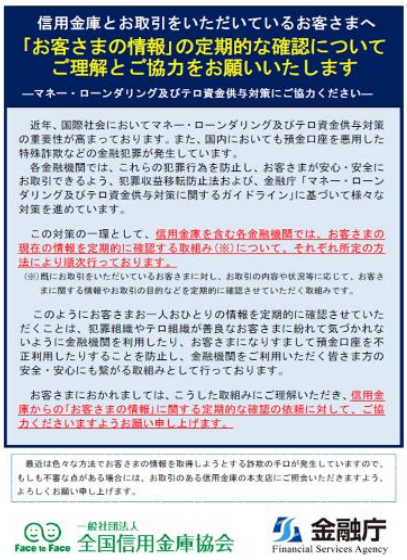
cooperation with their AML/CFT/CPF measures, uploaded it on the Association's website, and delivered it through YouTube. The National Central Association of Credit Cooperatives prepared a leaflet as well in the joint name of the FSA and provided it to Credit Cooperatives so that it could be presented to their customers.

Newspaper Advertisement (JBA)

Internet Advertisement (JBA)

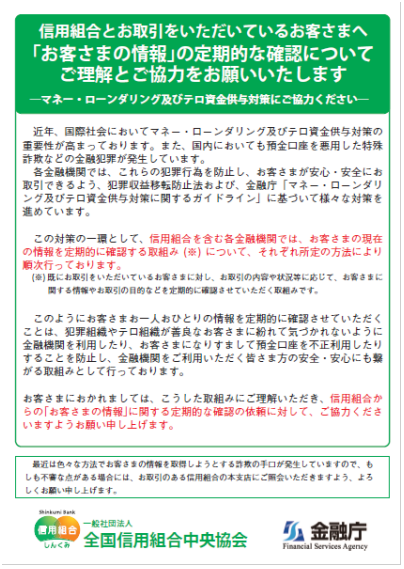
Flyer

(The National Association of Shinkin Banks)



Flyer

(Central Association of National Credit Associations)



The FSA updated its website related to Ongoing Customer Due Diligence in order to ask for the understanding and cooperation of the people of the FSA with AML/CFT. As part of promoting public relations with the JBA, Financial Services Agency posted a video commercial made by the JBA in the previous year.

AML/CFT/CPF website page (FSA)

【参考リンク】（全国銀行協会）
TVCM・店頭動画

テレビCM用映像（30秒）

店頭用映像（2分）

Since 2022, the FSA started delivering internet advertisements to further promote understanding of ongoing CDD. In the past, FSA has used the government PR media to promote understanding of ongoing CDD. In March 2022, the FSA also posted a special article on the Government Public Relation Online website and broadcasted FM radio commercials that feature AML/CFT/CPF measures and ongoing CDD.

The FSA will continue public relations to promote the understanding and cooperation of users on AML/CFT/CPF measures with relevant government ministries and financial sectors.

Internet advertising (FSA)

(Left : Image of search engine advertisement; Right : Internet display advertisement (2 types). These link to the FSA's AML/CFT/CPF website when clicked.)

Special Online Feature Page for Government Information

(Left: Image from the government's public relations online website; Right : Excerpt from the special feature article page on ongoing CDD)

11. Contributions to the FATF (other than Mutual Evaluation)

The FSA actively contributes to policy-making discussions at the FATF, in cooperation with the relevant ministries and agencies. The following is a summary of recent discussions at the FATF that are primarily relevant to the FSA.

(1) Contribution to the FATF Discussion on Crypto-Assets

Since finalizing the FATF Standards on virtual assets and virtual asset service providers in June 2019, the FATF has established VACG[68] in the FATF, co-chaired by the FSA, and has engaged in dialogue with the industry and monitored the industry's efforts to comply with the standards.

Based on the results of the VACG activities, in July 2020, the FATF published its first 12-month Review Report on the revised FATF Standards for Virtual Assets and Virtual Asset Service Providers,[69] which summarizes the current status of and challenges to the implementation of the FATF Standards by the public and private sectors. In addition, with regard to stablecoins, the FATF published the FATF Statement[70] in October 2019 and the FATF Report to the G20 Minister of Finance

[68] See Chapter 2 (2) C. "Notification of information on the originator and beneficiary at the time of transfer of crypto-assets"
[69] For more information about this report, see: https://www.fsa.go.jp/inter/etc/20200701_2.html.
[70] For this statement, see: https://www.fsa.go.jp/inter/etc/20191021-3.html.

and Central Bank Governor on stablecoins in July 2020.[71]

In line with the findings of these reports, the FATF Second 12-Month Review Report on the FATF Standards for Virtual Assets and Virtual Asset Service Providers[72] was adopted in June 2021. This report requests national authorities to implement the FATF Standards and travel rules by both the public and private sectors, as soon as possible in order to prevent regulatory arbitrage. The Report also introduces risks associated with the nature of crypto-assets, as well as risks associated with P2P transactions.[73] It summarizes that the FATF will continue monitoring and dialogue with the industry, and will work to promote global implementation of the FATF Standards as a whole and travel rules, and address ransomware-related issues.

Furthermore, in October 2021, the FATF revised and published the Guidance on Risk-Based Approaches to Virtual Assets and Virtual Asset Service Providers, which was originally adopted with the finalization of the FATF Standards in June 2019, to provide further guidance to countries and relevant industries on the implementation of the FATF Standards.[74]

The six main areas, regarding which previous reports mentioned that further clarification would be required, are: (1) the scope of application of the FATF Standards to Virtual Assets and Virtual Asset Service Providers (clarifying definition of these); (2) the application of the FATF Standards to so-called stablecoins; (3) risks and risk mitigation measures for transactions without being involved in any obliged entities (P2P transactions); (4) registration and licensing of Virtual Asset Service Providers; (5) implementation of obligations related to wire transfer in the area of Virtual Assets (so-called travel rules); and (6) principles for information sharing and international cooperation in supervision.

FSA contributed to the work on the revision of the Guidance as a VACG Co-Chair, Co-lead of the Guidance Update Project Team, and Topic Leads.[75] The FATF will continue to monitor crypto-assets, including stablecoins, P2P transactions, non-

---

[71] For more information about this report, see: https://www.fsa.go.jp/inter/etc/20200701.html.
[72] For more information about this report, see: https://www.fsa.go.jp/inter/etc/20210706/20210706.html.
[73] For more information, see the column: "ML/TF Risk Trends in Crypto-Assets" (page 7).
[74] For this guidance, see: https://www.fsa.go.jp/inter/etc/20211101/20211101.html.
[75] The second 12-month review report is highly expected by the international community. For example, the Communique of the G20 Minister of Finance and Central Bank Governors Meeting in October 2021 explicitly welcomed the revised guidance in both that communique and the Communique of the G20 Meeting in February 2022.

fungible tokens (NFTs), and decentralized finance (DeFi).

FSA will continue to lead international discussions by making the best use of Japan's regulatory and supervisory experience and knowledge, and at the same time it will utilize the knowledge gained from such international discussions in Japan's regulation and supervision as well.

Column [Revised "FATF Guidance on Risk-Based Approaches to Virtual Assets and Virtual Asset Service Providers"]

In June 2019, in line with the revision of the FATF Standards for crypto-assets, the FATF published guidance outlining its approach to those standards. In October 2021, the FATF revised and published this document to provide further guidance to countries and relevant industries on the issues identified in the "12-MONTH REVIEW OF THE REVISED FATF STANDARDS ON VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS" published in July 2020.

The key points of the revisions are as follows :

① Scope of application of FATF Standards

The definition of Virtual Asset Service Providers, hereinafter referred to as "VASP" needs to be broadly interpreted on a functional basis, and the applicability about whether an entity is undertaking the VASP's function should be determined not by the nomenclature or terminology that the entity adopt, nor technology employed by the entity but by the activities and functions of the entity (e.g., DeFi, etc.).

② Reducing risks in P2P transactions

Examples of risk mitigation measures that can be taken in a country and/or VASPs.

③ Stablecoins

As virtual assets or other emerging assets, they are subject to the FATF Standards. In addition, it is necessary to conduct forward-looking and ongoing risk analysis and address risks before the launch (launch is not allowed if risks are insufficiently addressed).

④ Travel Rules

The description has been enriched from the viewpoint of clarifying how this rule, which has been applied to financial institutions, is applied to virtual assets (e.g., information to be provided by the originator VASP to the beneficiary VASP, the timing and method of identifying the counterparty VASPs, and measures to for sunrise issues*).

⑤ Licensing and registration examination

Describe how to identify VASP that requires registration and a license in each country, and points to note in registration and license examination.

⑥ Principles for Information Sharing and International Cooperation in Supervision

Present general principles from the perspective of promoting supervisory cooperation.

* Sunrise Issues
As the timing of the introduction of travel rules in each country is not always the same, there is a mixture stage of countries having implemented travel rules and those that have not. As the number of countries that have implemented travel rules increases in the phased manner, there is a burden for VASPs to individually address the introduction of new regulations in each country each time.

(2) Guidance on supervision with a risk-based approach

In March 2021, the FATF published its Guidance for a Risk-Based Approach to Supervision.[76]

This Guidance is showing global awareness of the significance of a risk-based approach to supervision, and the publication of this Guidance indicates that the FATF recognizes that strengthening AML/CFT/CPF supervision is an important task.

FSA, which has been conducting on-site and off-site monitoring continuously through fact-finding and dialogue, and taking supervisory measures as necessary, will continue to deepen AML/CFT/CPF supervision based on the risk-based approach in light of this Guidance.

Column [Guidance on Supervision under the FATF Risk-based Approach]

The FATF requires AML/CFT supervision to be conducted through a risk-based approach, which identifies and assesses risks and takes actions according to the assessed risks. This Guidance, published in March 2021, provides high-level guidance on risk-based approach supervision and provides examples of how common challenges can be addressed and country examples. The main components of the Guidance are as follows :

1. High-level Guidance on Risk-based Supervision
   (1) Supervisors' risk understanding
   (2) Risk-based approach to supervision
   (3) Cross-cutting issues
2. Strategies to address common challenges in risk-based supervision and jurisdictional examples
   (1) Strategies to address challenges in assessing ML/TF risks
   (2) Challenges and solutions in applying risk-based supervision
3. Country examples

[76] For this guidance, see: https://www.fsa.go.jp/inter/etc/20210305.html.

(1) Supervision of financial institutions

(2) Supervision of DNFBPs

(3) Supervision of VASPs

(4) Supervision in the COVID-19 context

(3) Other discussions at the FATF

The FATF is working on projects to explore the AML/CFT/CPF benefits, efficiencies, cost reductions, and challenges that digital transformation could bring to the AML/CFT/CPF measures. In July 2021, the FATF published two reports titled "Opportunities and Challenges of New Technologies for AML/CFT" and "Stocktaking on Data Pooling, Collaborative Analytics, and Data Protection."[77]

In addition, with the aim of improving cross-border payments, the FATF published the findings in a report titled "Cross-border payments Survey Results on Implementation of the FATF Standards"[78] in October 2021.

Column [Digital transformation in AML/CFT area]

The FATF published two reports on digital transformation in July 2021.

① Opportunities and Challenges of New Technologies for AML/CFT

Based on the recognition that the use of new technologies can contribute to improving the effectiveness and efficiency of AML/CFT measures, this report introduces examples of new technologies, their expected effects, and challenges, with examples from both the public and private sectors in each country. It also includes an initiative to support the use of new technologies, namely "Blockchain Governance Initiative Network (BGIN)," which is developing blockchain technology in line with the multi-stakeholder approach mentioned by the FSA as the 2019 G20 Chair.

✓ Examples of new technologies :

AI (machine learning), natural language processing, distributed ledger technology, etc.

✓ Expected benefits :

Improving risk assessment and management, speeding up and improving the accuracy of large-scale data analysis, efficient identification (KYC), reducing costs and limiting the number of manual tasks, and improving the quality of suspicious transaction reporting (STR).

✓ Challenges in utilizing new technologies:

[77] For these reports, see: https://www.fsa.go.jp/inter/etc/20210702.html.
[78] For more information about this report, see: https://www.fsa.go.jp/inter/etc/20211025/20211025.html.

Regulatory and operational challenges, avoiding unintended consequences (e.g., privacy breaches), assessing the effectiveness of solutions and addressing residual risks.

② Stocktake on Data Pooling, Collaborative Analytics and Data Protection

This Report is based on the recognition that the sharing of ML/TF information among financial institutions can contribute to improving the effectiveness and efficiency of AML/CFT, whereas, at the same time, it is also necessary to ensure consistency with data protection and privacy regulations. From this context, the objectives of data sharing, data subject to sharing, emerging technologies, and challenges are introduced with examples from various countries, including Japan's "proof of concept" project conducted by New Energy and Industrial Technology Development Organization (NEDO), aiming for use of AI-featured AML/CFT systems by financial institutions supported by the FSA.

✓ Purpose of data sharing :

Transaction monitoring, risk management (including ongoing customer due diligence), identify typologies, onboarding customers (KYC), identification of beneficial owners, etc.

✓ Targeted Data (including under consideration) :

Customer information (including beneficial owners information), red flags (red flag indicators for suspicious transactions used by FIs), transaction history, account information, risk indicators (including STR information), etc.

✓ Promising new technologies for data sharing and analysis :

Encryption technology, machine learning, etc.

✓ Challenge :

Ensuring consistency with regulations on the protection of data and privacy, explainability and interpretability of new technologies, data quality and standardization, clarification of regulatory requirements for the use of new technologies, costs, confidentiality of STR, market structure and competitive issues, de-risking, security, AI bias, human rights protection, etc.

Column [FATF Report "Cross-border payments- Survey Results on implementation of the FATF Standards"]

Given the growing awareness of the high cost, lack of speed, and lack of transparency of conventional cross-border transactions behind the emergence of the global stablecoin concept, the G20 Minister of Finance and Central Bank Governors Meeting in February 2020 decided to address the improvement of cross-border transactions as a priority. The Financial Stability Board (FSB) and other international organizations are currently working in coordination on 19 Building Blocks (BBs) for improving the issues, and the FATF has published this report on BB5: "Applying AML/CFT

rules consistently and comprehensively," in which the FATF played a leading role.

In this Report, based on survey results from cross-border payments providers and an exchange of views with the private sector, the Report has identified (in order of most frequently pointed out) : (1) identification and verification of customer and beneficial owners, (2) sanction screening, (3) sharing of customer and transaction information, (4) correspondent banking relationships, etc. as topics where regulatory requirements that vary from country to country give rise to issues such as high costs in cross-border payments. The Report has also identified the existence of country-specific AML/CFT regulations that are outside the FATF standards, as well as information-sharing issues (data protection / privacy legislation, data standardization).

In addition, the FATF has revised its Standards [79] and Guidance [80] on risk assessment and mitigation in PF. The FATF has also added examples of environmental crimes as a non-exhaustive list to the Glossary of the FATF Standards following the publication of its reports[81] on illegal wildlife trade and environmental crime. In order to improve the transparency of the "beneficial owners" of legal entities, the FATF Standards (Recommendation 24) have been adopted and published[82] in March 2022, and guidance is currently being prepared on this matter. In addition, another work is underway regarding the revision of Recommendation 25 (Beneficial owners of legal arrangements) in light of the revision of R24.

(4) International cooperation

The significance of international cooperation between AML/CFT/CPF supervisory authorities has been recognized as important by the FATF in recent years, and the FSA has been exchanging information with foreign authorities on a bilateral and multilateral basis as necessary.

In recent years, at the supervisory colleges[83] of internationally active FIs, the FSA has also shared Japan's supervision examples and experience through discussions, setting conduct risk, including ML/TF risks in the agenda. In

[79] For these revised standards, see:http://www.fatf-gafi.org/publications/financingofproliferation/documents/statement-proliferation-financing-2020.html

[80] For this guidance, see: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/proliferation-financing-risk-assessment-mitigation.html

[81] For these reports, see: http://www.fatf-gafi.org/publications/environmentalcrime/environmental-crime.html?hf=10&b=0&s=desc(fatf_releasedate)

[82] For these revised standards, see:https://www.fatf-gafi.org/publications/fatfrecommendations/documents/r24-statement-march-2022.html

[83] A platform for globally ensuring effectiveness of supervisory activities by information exchange and recognition sharing between "home" and "host" supervisors.

particular, exchanges of views on AML/CFT/CPF frameworks with the supervisors where FIs in Japan have established their overseas offices contribute to the enhancement of their overseas risk control framework at the group and global levels. Since 2018, the FSA has held regular or ad-hoc meetings with the relevant authorities of the U.S., U.K., Netherlands, China, Singapore, Hong Kong, Indonesia, Thailand, and other jurisdictions.

End