IN-DEPTH

Anti-Money Laundering

JAPAN

LEXOLOGY

Anti-Money Laundering

EDITION 1

Contributing Editor

John Binns

BCL Solicitors LLP

In Depth: Anti-Money Laundering provides an insightful overview of anti-money laundering (AML) law and practice in key jurisdictions worldwide. With a focus on recent developments and their practical implications, it analyses key issues including relevant offences, government policy, enforcement trends, international cooperation and much more.

Generated: January 17, 2024

Japan

Daisuke Oda, **Hiroshi Shirane**, **Robyn Nadler** and **Ryosuke Onobori**
Mori Hamada & Matsumoto

Summary

Introduction

Japan has been developing its anti-money laundering (AML) and countering terrorism financing (CFT) framework based on the recommendations of the Financial Action Task Force (FATF), of which it is a member, since 1990.

Currently, the FATF is conducting an enhanced follow-up review for Japan, based on its fourth Mutual Evaluation Report published in August 2021.[2] Japan reports to the FATF on the progress achieved with regard to improvements in the implementation of AML/CFT measures.

Concurrently with the publication of the FATF's fourth Mutual Evaluation Report, the Ministry of Finance (MOF) published its three-year National AML/CFT/CPF Action Plan-[3] to address AML/CFT and proliferation financing. The Plan is currently in its third year, and follow-up is being conducted on the status of the efforts of regulated entities based on the guidelines on AML/CFT countermeasures established by the relevant ministries and agencies. In particular, the Financial Services Agency of Japan (FSA) has required financial institutions to complete the deployment of their governance arrangements for AML/CFT measures in compliance with the guidelines established by the FSA by the end of March 2024.

In addition, in May 2022, the MOF published the 'Strategic Policy towards Promoting AML/CFT/CPF'[4] and announced that it will work on specific measures based on four points: (1) full implementation of risk-based approach; (2) swift responses to new technologies such as cryptoassets; (3) strengthening international cooperation and coordination; and (4) enhancing inter-agency coordination and public–private partnership.

Year in review

i Stablecoin regulations

A regulatory framework for stablecoins came into force on 1 June 2023. The framework was based on discussions at the G20 Finance Ministers and Central Bank Governors' Meeting, among the Financial Stability Board, the FATF and others, on how to deal with global stablecoins, as well as regulatory trends in foreign jurisdictions. Specifically, a licensing and registration system for entities responsible for the issuance and distribution of stablecoins was developed. The framework also imposes new obligations on licensed and registered operators, such as travel rules, in addition to various AML/CFT obligations, including customer management, record-keeping and suspicious transaction reporting.

ii Introduction of travel rules

AML/CFT regulations were amended and became effective on 1 June 2023, to introduce travel rules for cryptoasset exchange service providers, and on 29 December 2022, to increase the statutory criminal penalty for money laundering offences and expand the property that can be confiscated as criminal proceeds. The amendments were based on

the recommendations in the FATF's fourth Mutual Evaluation Report published in August 2021.

iii Enhancement of pre-paid card regulations

The Payment Services Act and AML/CFT regulations were amended to introduce AML/CFT obligations, including customer control, record-keeping and suspicious transaction reporting, on issuers of prepaid cards (e.g., online gift cards) that can record amounts exceeding specific thresholds and that can be electronically transferred. The amendments came into force on 1 June 2023.

Legal framework

Overview of the AML/CFT regime in Japan

Japan's AML/CFT regime is designed to:

1. require certain defined categories of businesses to take AML/CFT measures;
2. punish those who commit money laundering (ML) or terrorist financing (TF);
3. deprive offenders of the proceeds of crime; and
4. prevent terrorist financing.

The regime takes two types of approach, namely for prevention and eradication.

Prevention provisions

The primary AML/CFT legislation obliges financial institutions and designated non-financial businesses and professions (DNFBPs) (such as real estate agents, precious metal dealers and professional experts such as lawyers) to take AML/CFT measures.

Specifically, the Act on Prevention of Transfer of Criminal Proceeds (the AML Act), the main preventive regulation, requires obliged entities to verify their customers at the time of transaction (i.e., conduct know-your-customer (KYC) procedures), prepare and keep records and report suspicious transactions as part of their AML/CFT measures.

In addition, to ensure that these obligations are properly conducted, the competent regulatory authorities of each obliged entity have published AML/CFT guidelines, and financial institutions and DNFBPs are required to establish a governance arrangement for AML/CFT measures in accordance with these guidelines.

Furthermore, the AML Act and the Foreign Exchange and Foreign Trade Act impose obligations on banks and fund transfer service providers to verify the counterparty and purpose of remittances to ensure that their cross-border remittance transactions are not connected to, for example, sanctioned parties designated by UN Security Council (UNSC) resolutions. In addition, 'travel rules' have recently been introduced to impose an obligation on intermediaries dealing with cryptoassets and stablecoins (i.e., virtual asset service providers (VASPs)) to provide information on originators and beneficiaries of transactions

to receiving VASPs when they transfer cryptoassets and stablecoins managed on behalf of their customers.

Eradication provisions

Laws and regulations aimed at eradicating money laundering set out provisions that make money laundering and terrorist financing subject to criminal penalties and deprive offenders of the proceeds of crime.

Specifically, the Organised Crime Punishment Act and the Anti-Drug Special Provisions Law criminalise acts aimed at controlling the business of legal entities through illicit proceeds, or the concealment or receipt of criminal proceeds or drug proceeds, and set out provisions for confiscation, collection and preservation of criminal proceeds.

Associated offences

i Prevention provisions

As mentioned above, financial institutions and DNFBPs must properly fulfil their statutory obligations under the AML Act and the Foreign Exchange and Foreign Trade Act and take necessary measures to address terrorist financing.

In contrast to money laundering, terrorist financing must be prevented regardless of whether the funds have been acquired legitimately or not. For example, financial institutions must refuse to undertake the transfer of funds to sanctioned persons designated by UNSC resolutions, regardless of the source of the funds or the reason for the transfer.

ii Eradication provisions

The legislation regarding the eradication of terrorist financing treats the act of terrorist financing as a criminal offence and requires countermeasures such as freezing the domestic and foreign assets of terrorists. As noted above, unlike money laundering, terrorist financing is subject to punishment and the freezing of assets regardless of whether the funds were acquired legitimately or not.

Specifically, the Law on Punishment of Terrorist Financing punishes the act of providing funds for the implementation of terrorist acts and the provision of funds to a person who intends to provide funds for terrorism.

In addition, with respect to foreign transactions, the Foreign Exchange and Foreign Trade Act imposes measures such as asset freezing by prohibiting the transfer of funds, the depositing or lending of funds, or the trading of securities, with sanctioned parties designated by UNSC resolutions. Furthermore, the International Terrorist Assets Freezing Act implements asset freezes and other measures by prohibiting domestic transactions with these sanctioned persons.

Anti-money laundering regulation

i The AML Act

Overview

The AML Act is the primary regulation for the prevention of money laundering.

The Act imposes obligations on financial institutions and DNFBPs, referred to as 'obliged entities', in relation to the prevention of money laundering. The statutory obligations include: KYC procedures; preparation and storage of records relating to KYC and transactions; suspicious transaction reports to regulatory authorities; and the establishment of a governance arrangement to prevent money laundering. In addition to the above obligations, certain obliged entities are required to comply with confirmation obligations at the time of concluding correspondent agreements and travel rules for foreign remittances and the transfers of cryptoassets and stablecoins.

Obliged entity

Types of obliged entities, which are subject to obligations under the AML Act, are listed in the legislation, and not all business entities are necessarily required to comply with the obligations under the AML Act.

Obliged entities include banks, financial instruments business operators, insurance companies, fund transfer service providers, cryptoasset exchange service providers and other financial institutions, non-financial institutions such as finance lease operators, credit card providers, casino operators, real estate agencies and precious metal dealers, and professional experts such as lawyers, certified public accountants and tax accountants, based on FATF recommendations.[5]

While banks, fund service providers and real estate agencies are licensed by the regulatory authorities and are subject to a licensing system for their business activities, certain obliged entities under the AML Act, such as finance lease operators, are not necessarily subject to a licensing system.

In addition, obligations differ depending on the type of obliged entity. For example, there are cases where banks, fund transfer service providers, and cryptoasset and stablecoin exchange service providers are subject to special obligations that do not apply to other specified obliged entities, such as the travel rules.

Obligation to verify customers and prepare and store records

Obliged entities must carry out KYC procedures, referred to as 'verification at the time of transaction', when conducting specific transactions stipulated in the AML Act.[6]

The AML Act defines the transactions for which KYC procedures are mandatory as 'specified transactions',[7] examples of which are:

1. establishing a business relationship: for example, opening a deposit account, entering into an insurance contract, opening an account for cryptoasset trading and entering into a credit card contract;

2. occasional transactions: cash transfers or the transfer of cryptoassets of more than ¥100,000, currency exchange of more than ¥2 million or the purchase or sale of precious metals, securities or real estate; and
3. transactions suspected of money laundering, terrorist financing or identity theft.

When conducting these transactions with a customer who has previously been verified at the time of transaction, another verification is not, in principle, required if it can be confirmed that the identity of the customer has previously been verified at the time of the transaction.-[8]

The procedure for verifying at the time of transaction is as follows.[9]

Where the customer is a natural person, the following must be verified:

1. name, residence and date of birth by means of identification documents such as an ID card or driver's licence;
2. the purpose of the transaction, as declared by the customer; and
3. occupation, as declared by the customer;

In addition, if the transaction is carried out by an agent, the following matters must be also verified:

1. name, residence and date of birth of the agent by means of identification documents such as an ID card or driving licence; and
2. authority to act on behalf of the principal by, for example, power of attorney.

Where the customer is a legal entity, the following must be verified:

1. name and address of head office by means of a certificate of registered matters or other document;
2. the purpose of the transaction, as declared by the customer;
3. the nature of the customer`s business, as indicated on the certificate of registration, articles of association or other documents;
4. the name, residence and date of birth of the person with effective control of the customer, as declared by the customer;
5. the name, residence and date of birth of the person in charge of the transaction, by means of ID cards, driving licences or other proof documents; and
6. the authority to conduct transactions (e.g., by means of a power of attorney or other evidence such as corporate registration documents indicating that the agent is a representative of the customer).

In the case of non-face-to-face transactions, due to the risk of document forgery or impersonation, it was previously required to take additional steps such as sending a postal letter to the address indicated on the certification documents, which delayed the ability to initiate transactions. To improve this issue, the AML Act was amended in 2018 to introduce

an e-KYC procedure, which allows for the completion of verification process at the time of transaction by checking the customer's appearance and other details online.

The AML Act also requires stricter procedures for certain high-risk transactions than the ordinary verification process.[10] Specifically, when conducting: (1) transactions with customers suspected of impersonating or falsifying information in a previous KYC procedure; (2) certain transactions with customers residing or located in Iran and North Korea; or (3) certain transactions with foreign politically exposed persons, obliged entities must require their customers to submit additional certification documents and, if the transaction involves the transfer of property in excess of ¥2 million, they must also verify the customer's asset and income status. Furthermore, high-risk transactions also require that the person responsible for anti-money laundering measures (MLRO) approves, after careful review, that there is no suspicion of money laundering or terrorist financing.

When verifying at the time of the transaction, obliged entities must immediately prepare records and maintain them for seven years from the date of the termination of the contract in question.[11]

Transaction records obligations and suspicious transaction reporting

The AML Act requires obliged entities to prepare records of transactions with customers and maintain them for seven years from the date of the transaction.[12]

In addition, obliged entities are required to monitor transactions with customers to determine whether property received from customers is suspected of being the proceeds of crime or whether customers are suspected of committing money laundering. If a determination is made that this suspicion exists, obliged entities must promptly notify the regulatory authorities.[13] When obliged entities notify the regulatory authorities of a suspicious transaction, they are prohibited from leaking information relating to the notification to customers or other parties.[14]

Suspicious transaction reports must be filed with the Japan Financial Intelligence Centre (JAFIC) of the National Police Agency, which is the financial intelligence unit in Japan. In practice, obliged entities shall submit suspicious transaction reports to the JAFIC through their regulatory authorities (e.g., the FSA in the case of banks).

Cross-border remittances

When a bank or a fund transfer service provider enters into an agreement with a foreign firm for repeated and continuous fund transfer transactions (correspondent agreement), the bank or the fund transfer service provider is obliged to confirm that the foreign firm has taken measures equivalent to AML/CFT measures required by Japanese domestic regulations and that the regulatory authority in the relevant foreign country appropriately supervises the foreign firm.[15] For this reason, before concluding a correspondent agreement with a foreign firm, banks use questionnaires published by the Wolfsberg Group and other sources to check the foreign firm's governance arrangements for AML/CFT.[16]

In addition, when remitting funds from Japan to a foreign country, the travel rules apply, which require the provision of prescribed information relating to the originator and beneficiary.[17] Whereas previously only the originator's information was required to be

provided, from 1 June 2023 the beneficiary's information must also be provided due to the enforcement of the FATF Recommendation Compliance Act.

Transfer of cryptoassets and electronic payment instruments

The transfer of cryptoassets and electronic payment instruments (stablecoins) also became subject to the obligation to confirm prescribed information concerning a foreign firm at the time of concluding a contract for a transfer with the foreign firm and to comply with the travel rule.[18] In particular, with regard to the travel rules, whereas the banks and fund transfer service providers mentioned under 'Cross-border remittances', above, are subject to the travel rules for cross-border remittances, domestic transfers of cryptoassets and stablecoins are also subject to the travel rules.

With regard to the travel rules, a cryptoasset exchange service provider and an electronic payment instrument exchange service provider (stablecoin intermediary) (collectively, VASPs) are obliged to provide details of both the originator and the beneficiary to a receiving domestic VASP or a receiving VASP located in a jurisdiction designated by the regulatory authorities as a jurisdiction where travel rules have been introduced. They must provide prescribed information relating to the originator and the beneficiary when transferring cryptoassets or stablecoins on behalf of their customers.

In addition, as cryptoassets and stablecoins are expected to be transferred to and from unhosted wallets managed by users themselves, the AML Act imposes an obligation on VASPs that transfer cryptoassets and stablecoins to and from unhosted wallets to make efforts to obtain information about the unhosted wallets concerned.

Governance arrangement obligation

The AML Act requires obliged entities to have in place a governance arrangement to ensure that the obligations detailed above are fulfilled properly. The FSA, which supervises financial institutions, and other regulatory authorities have specified in their guidelines[19] the details of the required governance arrangement for obliged entities, including:

1. ongoing customer management;
2. hiring staff with knowledge of AML/CFT and providing education and training;
3. preparing and reviewing AML/CFT policies and internal rules;
4. the appointment of an MLRO;
5. the preparation and review of a risk assessment report that investigates and analyses the money laundering risks of transactions conducted by the obliged entity itself;
6. the implementation of measures to reduce money laundering and terrorism financing risks based on the content of the risk assessment report; and
7. the implementation of a three lines of defence internal control system.

ii The Foreign Exchange and Foreign Trade Act

The Foreign Exchange and Foreign Trade Act imposes various regulations on foreign exchange, foreign trade and other foreign transactions from the perspective of controlling and coordinating them to the minimum necessary extent, while assuming that they can be conducted freely in principle. As a measure against AML/CFT, transactions with sanctioned persons are prohibited, mainly from the perspective of terrorist financing. When banks, fund transfer service providers, cryptoasset exchange service providers and others deal with, for example, cross-border remittances and cryptoasset transactions, they are obliged to confirm that the transaction requested by the customer is not to transfer funds to or from a sanctioned person.[20]

In its guidelines, the MOF sets out the matters that must be confirmed and the method of confirmation.[21] Specifically, obliged entities are required to confirm the name of the counterparty to the transaction and the purpose of the remittance, and to confirm that the counterparty to the transaction is not a sanctioned party and that there is no suspicion of terrorist financing or proliferation finance.

Anti-money laundering in practice

Overview

Obliged entities are currently preparing their governance arrangements in accordance with the guidelines on AML/CFT measures established by the regulatory authorities. In particular, the FSA has requested that financial institutions complete governance arrangements compliant with the FSA's guidelines by the end of March 2024. The following are some examples of practical measures being taken by financial institutions.

Risk-based approach

When considering AML/CFT measures, obliged entities are required to prepare a risk assessment document, summarising the results of the investigation and analysis of the ML/TF risks of the transactions they conduct. The risk assessment should include a comprehensive identification of the products and services they offer, the type of transactions, the countries and regions in which they operate and the nature of the customer. Measures to reduce ML/TF risks should also be considered, based on the risks identified and assessed.

Updating customer information

Financial institutions are required to maintain up-to-date customer information verified through KYC procedures. In general, deposit agreements require depositors to notify banks of any changes in their previously provided customer information, such as a change of address due to relocation or other reasons. In addition, in recent years banks have been more proactive in confirming with customers whether their information has changed; for example, by sending emails or letters to customers.

In addition, due to the misuse of deposit accounts opened by visitors to Japan, in which the accounts were sold to criminal organisations upon their return to their home countries and used for money laundering, banks now take measures during the KYC procedures, such

as confirming visitors' period of stay in Japan, confirming whether the period of stay has been renewed prior to the expiry of the period, and requesting the closure of the deposit account upon their return from Japan.

Asset freezes

Financial institutions confirm that customers do not fall under the category of 'anti-social forces' such as organised crime groups or persons subject to domestic or international sanctions. In particular, in the case of cross-border remittances, they are also required to confirm that the counterparties of remittance transactions do not fall under the category of sanctioned persons.

Financial institutions with a large number of customers, such as banks, have introduced systems to carry out screening against databases of anti-social forces and sanctioned persons at the time of onboarding and whenever the lists are updated.

In addition, bank accounts used for fraud and other criminal activities can be frozen based on a victim's report or a request from the police.

Transaction monitoring

Financial institutions are required to monitor transactions with customers to ensure that they do not constitute suspicious transactions in terms of ML/TF and to report suspicious transactions to the regulatory authorities. The total number of suspicious transactions reports amounts to approximately 500,000 per year.

Given the huge volume of data relating to instructions for deposits and withdrawals via ATMs or the internet, retail banks typically monitor deposit account transactions using automated systems.

In light of the high cost of implementing a system for each financial institution, the Japanese Bankers Association, an industry association of banks, is working to develop monitoring systems for common use.

Enforcement

Enforcement against obliged entities in Japan is carried out through reporting orders and business improvement orders by regulatory authorities. There are no cases where criminal or financial sanctions have been imposed due to deficiencies in governance arrangements for AML/CFT. In this regard, the FATF's fourth Mutual Evaluation Report also states that Japan should 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 to ensure that sanctions are applied in practice.[22]

Since 2021, the FSA has strengthened inspections focused on AML/CFT measures and off-site monitoring of financial institutions. This is based on the recommendation in the FATF's fourth Mutual Evaluation Report that Japan should require financial supervisors to enhance the supervision on a risk basis, through the development or completion of adequate risk analysis for all supervised financial institutions.[23] As mentioned above, the FSA has requested that financial institutions complete the development of their

governance arrangements in compliance with the guidelines published by the FSA by the end of March 2024. There are currently no published cases of financial institutions having received administrative sanctions such as business improvement orders as a result of these inspections. However, the FSA has indicated that, from April 2024, if they find through inspections that a financial institution has not taken measures to comply with the guidelines and that its AML/CFT arrangements are problematic, the institution may be subject to a business improvement order or other administrative action.

International organisations and agreements

Japan has been a member of the FATF since its establishment in 1990 and it has developed its legal framework for AML/CFT based on FATF recommendations. One of Japan's major banks, MUFG, is also a member of the Wolfsberg Group, which publishes frameworks and guidance for managing financial crime risks, and has contributed to the development of AML/CFT measures in the private sector.

Other laws affecting the response to money laundering

Other laws affecting AML and CFT include the Act on the Protection of Personal Information (APPI) and the Whistleblower Protection Act.

With regard to the handling of personal data, obliged entities (i.e., banks) are, in principle, required under the APPI[24] to obtain a data subject's consent when providing third parties with their personal data. However, they are exempted from this obligation if, for example, the provision of personal data is based on laws and regulations[25] or if it is necessary to protect the life, body or property of an individual where it is difficult to obtain the consent of a data subject.[26]

When obliged entities share customer information including personal data within their group of companies for the purposes of customer management, they need to obtain the customer's prior consent or use available exemptions to comply with the APPI. In relation to suspicious transaction reports, the provision of personal data without the data subject's consent is considered legitimate as it is based on the AML Act.

Under the Whistleblower Protection Act, employees are protected from dismissal or other unfavourable treatment as a result of whistle-blowing about money laundering by their employer.[27]

Outlook and conclusions

Given the increasing strictness and sophistication of AML/CFT measures in accordance with the FATF follow-up process, and the FATF plans to start the fifth round of mutual examinations from 2024, responses to the fifth round of examinations will be carried out in parallel with the follow-up to the fourth round of examinations. As a result, it is assumed that the regulatory authorities will continue to closely supervise obliged entities,

and that obliged entities with inadequate governance arrangements may be subject to administrative penalties.

In addition, the travel rules for cryptoassets and stablecoin transfers have only just come into force, and the practical operational trends will need to be closely monitored.

Endnotes

1 Daisuke Oda is a partner, Hiroshi Shirane is a counsel, Robyn Nadler is a foreign-qualified lawyer and Ryosuke Onobori is a senior associate at Mori Hamada & Matsumoto. ^ Back to section

2 www.fatf-gafi.org/en/publications/Mutualevaluations/Mer-japan-2021.html. ^ Back to section

3 www.mof.go.jp/english/policy/international_policy/amlcftcpf/National_AML_CFT_CPF_Action_Plan_Aug_19_2021.pdf. ^ Back to section

4 www.mof.go.jp/english/policy/international_policy/amlcftcpf/The_Strategic_Policy_towards_Promoting_AMLCFTCPF.pdf. ^ Back to section

5 Act on Prevention of Transfer of Criminal Proceeds (AML Act), Article 2, Paragraph 2. ^ Back to section

6 id., Article 4, Paragraph 1. ^ Back to section

7 Order for Enforcement of the Act on Prevention of Transfer of Criminal Proceeds, Article 7, Paragraph 1. ^ Back to section

8 AML Act, Article 4, Paragraph 3. ^ Back to section

9 id., Article 4, Paragraph 1; Ordinance for Enforcement of the Act on Prevention of Transfer of Criminal Proceeds, Articles 6 to 12. ^ Back to section

10 AML Act, Article 4, Paragraph 2. ^ Back to section

11 id., Article 6. ^ Back to section

12 id., Article 7. ^ Back to section

13 id., Article 8, Paragraph 1. ^ Back to section

14 id., Article 8, Paragraph 3. ^ Back to section

15 id., Article 9. ^ Back to section

16 https://db.wolfsberg-group.org/assets/3964cedf-a462-4e55-a1e7-ca7c70dfa7ec/CBDDQ%20v1.4.pdf. Back to section

17 AML Act, Article 10. Back to section

18 id., Article 10-2 to 10-5. Back to section

19 https://www.fsa.go.jp/common/law/amlcft/211122_en_amlcft_guidelines.pdf. Back to section

20 The Foreign Exchange and Foreign Trade Act, Article 17 to 17-4. Back to section

21 www.mof.go.jp/policy/international_policy/gaitame_kawase/inspection/e_g_zenbun.pdf. Back to section

22 Financial Action Task Force, 'Mutual Evaluation Report (Japan)' (August 2021), p. 137. Back to section

23 id., p. 136. Back to section

24 Act on the Protection of Personal Information, Article 27, Paragraph 1. Back to section

25 id., Article 27, Paragraph 1, Item 1. Back to section

26 id., Article 27, Paragraph 1, Item 2. Back to section

27 Whistleblower Protection Act, Chapter 2. Back to section

MORI HAMADA & MATSUMOTO

Daisuke Oda
Hiroshi Shirane hiroshi.shirane@mhm-global.com
Robyn Nadler robyn.nadler@mhm-global.com
Ryosuke Onobori ryosuke.onobori@mhm-global.com

Mori Hamada & Matsumoto