PUBLIC CONSULTATION ON A PROPOSAL FOR INFORMATION SHARING AMONG AUTHORIZED INSTITUTIONS TO AID IN PREVENTION OR DETECTION OF CRIME

Hong Kong Monetary Authority

23 January 2024

Contents

1. **Foreword** 1
2. **Personal Information Collection Statement** 3
3. **Executive summary** 5
4. **Background** 8
5. **Why do AIs need to share information?** 10
6. **What information would be shared and how?** 15
7. **How will this affect the existing STR regime?** 16
8. **Safeguards** 17
9. **Implementation and timing** 20

Annex 21

1. Foreword

1.1 The Hong Kong Monetary Authority (HKMA) issues this consultation paper to seek views on proposals to facilitate sharing among Authorized Institutions (AIs)[1] of information on customer accounts for the purpose of preventing or detecting crime. The proposal aims to help protect bank customers from losses and the banking system against abuse for fraud, money laundering and terrorist financing (ML/TF).

1.2 Members of the public are invited to submit written comments on or before 29 March 2024 through the following channels:

By email to (recommended means): ai-to-ai-information-sharing@hkma.gov.hk

(Subject: Public Consultation on Information Sharing among Authorized Institutions)

By mail to: -

Hong Kong Monetary Authority
55/F, Two International Finance Centre
8 Finance Street
Central, Hong Kong
(Subject: Public Consultation on Information Sharing among Authorized Institutions)

1.3 Persons submitting comments on behalf of an organisation should provide details of the organisation whose views they represent.

1.4 Please note that the names of commentators and the contents of their submissions may be published on the HKMA website and/or in other

[1] Institutions authorized in Hong Kong under the Banking Ordinance.

documents to be published by the HKMA. Please read the Personal Information Collection Statement in the following section for details.

1.5 If you do not wish your name or submission to be published by the HKMA, please indicate this when you make your submission.

2. Personal Information Collection Statement

2.1 This Personal Information Collection Statement (PICS) is made in accordance with the guidelines issued by the Privacy Commissioner for Personal Data. The PICS sets out the purposes for which your Personal data[2] will be used following collection, what you are agreeing to with respect to the HKMA's use of your Personal Data, and your rights under the Personal Data (Privacy) Ordinance (Cap. 486) (PDPO).

Purpose of collection

2.2 The personal data provided in your submission in response to this consultation paper may be used by the HKMA for one or more of the following purposes –

- to perform statutory functions under the provisions of the Banking Ordinance (Cap. 155);
- to administer the provisions of the Banking Ordinance (Cap. 155) and guidelines published pursuant to the powers vested in the HKMA;
- for research and statistical purposes; or
- for other purposes permitted by law.

Transfer of personal data

2.3 Personal data may be disclosed by the HKMA to members of the public in Hong Kong and elsewhere as part of this consultation. The names of persons who submitted comments on this consultation paper, together with the whole or any part of their submissions, may be disclosed to members of the public. This will be done by publishing this information on the HKMA website and/or in documents to be published by the HKMA during the consultation period or at its conclusion.

[2] Personal data means personal information as defined in the Personal Data (Privacy) Ordinance (Cap. 486).

Access to data

2.4 You have the right to request access to and correction of your personal data in accordance with the provisions of the PDPO. Your right of access includes the right to obtain a copy of your personal data provided in your submission on this consultation paper. The HKMA has the right to charge a reasonable fee for processing any data access request.

Retention

2.5 Personal data provided to the HKMA in response to this consultation paper will be retained for such period as may be necessary for the proper discharge of its functions.

Enquiries

2.6 Any enquiries regarding the personal data provided in your submission on this consultation paper, requests for access to personal data or correction of personal data should be addressed in writing to –

Personal Data Privacy Officer
Hong Kong Monetary Authority
55/F, Two International Finance Centre
8 Finance Street
Central, Hong Kong

3. Executive summary

3.1 This consultation seeks views and suggestions on the need to facilitate AI-to-AI sharing of information on customers, accounts and transactions for the purpose of preventing or detecting financial crime by allowing AIs to alert each other to potential fraud and ML/TF concerns, thus helping to protect bank customers from losses and the banking system from being abused for fraud, money laundering and terrorist financing.

3.2 Recent years have seen a sharp global increase in financial crime, especially digital fraud, including in Hong Kong. This has led to increasing concern about harm to victims, damage to consumer confidence in the use of new digital financial services and possible wider impacts on the stability and integrity of the banking system.

3.3 Experience shows that information sharing among banks and law enforcement agencies (LEAs) is key to combatting financial crime by targeting related money laundering. The HKMA, the banking sector and the Hong Kong Police Force (HKPF) have responded with a number of public-private partnerships including the Fraud and Money Laundering Intelligence Taskforce (FMLIT)[3] and Anti-Deception Coordination Centre (ADCC)[4].

3.4 While these public-private initiatives have achieved considerable success, they are not, by themselves, sufficient to fully address the issue of money laundering via networks of accounts maintained or controlled by criminals (referred to as "mule account networks") because such arrangements generally only operate in cases where

[3] The FMLIT was established in May 2017 by the HKPF, supported by the HKMA. Ten retail banks participated initially, which had increased to 28 by the end of June 2023.

[4] The ADCC was established in July 2017 by the HKPF to combat deception and enhance public awareness of scams. Twenty-eight major retail banks have joined the "24/7 Stop Payment Mechanism", established by the ADCC to assist the HKPF in intercepting fraudulent funds promptly.

LEA investigations are already active, and may not support the sharing of information quickly enough for illicit funds to be intercepted. Criminals seeking to use the banking system to rapidly move and conceal illicit funds are able to exploit information gaps between AIs. For example, by the time one AI has taken action against illicit activity, those responsible have often been able to move their activities to mule accounts in other AIs, whom the first AI is unable to alert.

3.5 There is therefore a need for additional ways to combat illicit activity, which is reflected in a growing trend internationally towards cooperation between private-sector financial institutions (FIs), which share information to combat crime and related money laundering. In Hong Kong, the Financial Intelligence Evaluation Sharing Tool (FINEST) [5] was introduced in June 2023, with support from the HKMA and the HKPF, to facilitate a measure of information sharing among AIs. Currently, FINEST only covers information on corporate accounts because of concerns over data privacy if sharing is extended to personal accounts. The ability of FINEST to prevent and detect crime will be greatly enhanced with the inclusion of personal account information, since the majority of accounts used in money laundering related to fraud are held by individuals.

3.6 Safeguarding data privacy and customer confidentiality is crucial to the banking sector, while there is also an increasing view that such considerations should be balanced against the need for some degree of information sharing to help prevent or detect illicit activity. Several overseas jurisdictions have introduced legal protection for information sharing among FIs in cases where fraud or ML/TF are suspected, subject to appropriate safeguards.

[5] FINEST is a platform for sharing information on bank accounts, where crime is suspected. The pilot phase was launched on 20 June 2023.

3.7 Depending on the outcome of this consultation, the HKMA may propose legislative amendments to provide "safe harbour" protection to AIs sharing information solely for the purposes of preventing or detecting fraud or ML/TF, subject to safeguards to ensure appropriate handling of shared information.

4. Background

4.1 The Hong Kong Money Laundering and Terrorist Financing Risk Assessment Report[6] published by the Government in July 2022 identifies the banking sector as being at high risk of exploitation for money laundering, which is similar to the position in other international financial centres. The Report notes that 72.6% of money laundering investigations between 2016 and 2020 were fraud related.

4.2 Recent years have seen a sharp global increase in financial crime, especially digital fraud, and related money laundering. In Hong Kong, 27,923 deception cases were reported to the HKPF in 2022 (45% more than in 2021 and more than three times the number in 2018), involving estimated losses to victims of about HK$4.8 billion. Cases surged further in the first ten months of 2023 by 52.1% year-on-year to 33,923 cases, with estimated losses of about HK$7.2 billion. The HKMA continues to receive increasing numbers of fraud-related banking complaints. In 2023, we received over 1,200 cases, more than double the total of 555 cases for the whole of 2022. Similar increases in fraud cases overseas also affect Hong Kong which, as an international financial centre, is often abused as a destination or conduit for the proceeds of crimes committed elsewhere. The stolen funds are typically laundered via networks of accounts established or controlled by "money mules", persons who transfer money that has been acquired illegally such as by theft or fraud. The majority of such accounts are held with banks.

4.3 While these financial crimes and related money laundering have not so far significantly threatened the stability of the financial system, there is increasing concern globally about the rising trend of financial crime, especially digital fraud. In addition to the harm caused to victims, large-scale digital fraud could undermine public confidence in the use of new digital financial services, which in turn

[6] https://www.fstb.gov.hk/fsb/aml/en/doc/Money%20Laudering%20Report_2022_EN.pdf

could undermine the stability and integrity of the financial system. There is therefore a need to step up efforts to detect and prevent illicit activity and, where fraud does occur, trace and confiscate funds for return to victims where possible.

5. Why do AIs need to share information?

5.1 The Financial Action Task Force (FATF), the international anti-money laundering and counter-financing of terrorism (AML/CFT) standard setting body[7], advocates effective information sharing as one of the cornerstones of a well-functioning AML/CFT framework[8] and timely exchange of information is a key element of the FATF standards. A 2021 FATF publication[9] notes that "In order to better prevent and detect the abuse of the international financial system for ML/TF purposes, FIs could consider collaborating …… within a financial group, and between FIs that are not part of the same financial group" provided that data protection requirements are met. A 2022 report[10] "Partnering in the Fight Against Financial Crime" presents case studies of information-sharing initiatives in several jurisdictions and notes that "the public sector should consider taking an active facilitation role in private sector information sharing initiatives", including by updating laws or supervisory arrangements.

5.2 Experience in Hong Kong and overseas demonstrates that information sharing among LEAs and banks is a crucial element in preventing, detecting and disrupting the mule account networks through which criminals seek to move and conceal illicit funds. Information sharing is also crucial to intercepting and freezing funds by LEAs with a view to eventual confiscation and, where possible, return to victims.

5.3 AIs are under a legal obligation to report suspicion regarding funds representing the proceeds of, or otherwise connected to, criminal activity[11] by filing suspicious transaction reports (STR) to the Joint Financial Intelligence Unit (JFIU). For this purpose, AIs seek to

---

[7] Hong Kong has been a FATF member since 1991.

[8] FATF Guidance "Private Sector Information Sharing" published in November 2017. https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Private-Sector-Information-Sharing.pdf.coredownload.pdf

[9] https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Stocktake-Datapooling-Collaborative-Analytics.pdf.coredownload.pdf

[10] https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-int-the-fight-against-financial-crime.pdf

[11] Under section 25A of the Organized and Serious Crimes Ordinance (Cap. 455), section 25A of the Drug Trafficking (Recovery of Proceeds) Ordinance (Cap. 405) and section 12 of the United Nations (Anti-Terrorism Measures) Ordinance (UNATMO) (Cap. 575) in relation to terrorist financing.

identify unusual or suspicious activity, such as transactions that are inconsistent with AIs' knowledge or information about the customer. This requirement is in line with the international FATF standards and, as in other financial centres, the Hong Kong banking sector contributes the great majority of STRs[12] providing useful information for follow-up and investigation by LEAs.

5.4 Stronger cooperation and coordination through public-private partnerships, including the FMLIT and the ADCC, have achieved positive results[13]. However, these public-private partnerships are not, by themselves, sufficient to fully address the issue of mule account networks because such arrangements generally only operate in cases where law enforcement investigations are already active, and may not support sharing of information quickly enough to allow illicit funds to be intercepted. Given the fast-changing global threat landscape in fraud and related mule account networks, there is an increasing need for innovative and speedy ways to promote collaborative efforts in combating these financial crimes. We believe that closing the information gaps among AIs by allowing them to share information has the potential to greatly assist AIs and LEAs in combating financial crime, especially digital fraud, and related money laundering.

5.5 Recent developments in the speed with which funds can be moved have highlighted three areas with potential to enhance the detection, prevention and disruption of money laundering: improving the quality of STRs, speeding up the interception of illicit funds and preventing mule account networks that are disrupted at one bank moving to another. These objectives would be best served by private-to-private sharing of information by AIs, which would complement, but not replace, the existing public-private channels.

[12] Around 81% in 2022.

[13] Since inception in 2017 until October 2023, identification of accounts in FMLIT cases has led to HK$1.09 billion being restrained or confiscated. Some HK$12 billion in suspected crime proceeds have been intercepted under the 24/7 stop payment mechanism since its establishment in 2017.

Improving STR quality

5.6 When deciding whether to file an STR, an AI must assess whether the observed activity meets the legal threshold of knowledge or suspicion[14] based on the information it holds about the customer, account(s) and relevant transactions. In many cases, the AI is aware of transfers to or from other AIs. Currently, legal and contractual confidentiality requirements limit AIs' ability to share customer information with other AIs directly. Enabling AIs to share information where they observe activity that may indicate that a person, account or transaction is involved in fraud or ML/TF would help to facilitate timely decisions on whether to file STRs and reduce "false positives" in cases where information provided by another AI explains activity that appeared potentially suspicious at first sight.

5.7 Sharing information would also improve the quality of STRs by including information from more than one AI. Individual AIs only see activity through their own accounts and combining information from two or more AIs may provide more actionable intelligence for LEAs to investigate.

Interception of illicit funds

5.8 Criminals seeking to move and hide illicit funds will typically try to move them multiple times using accounts at multiple institutions and as quickly as possible. By the time AIs suspect that funds passing through their accounts are linked to illicit activity, the funds have often already been transferred to other, often multiple, AIs and may then be transferred further, sometimes overseas, making them difficult or impossible to trace and intercept. While AIs will file STRs, it takes time for LEAs to investigate and alert AIs further down the chain. Allowing AIs to share information directly should increase the speed of detection and the ability to "follow the money", which may in turn prove crucial in helping LEAs to intercept illicit funds.

[14] "Where a person knows or suspects that any property" represents proceeds of crime or was used, or is intended to be used, in connection with a serious criminal offence. A similar threshold applies for terrorist property under UNATMO.

Avoiding risk displacement

5.9 Direct sharing of information among AIs will also help to address the issue of "risk displacement". This refers to situations where an AI identifies mule account networks within its own customer base, files an STR and takes action to prevent further illegal activity but is currently unable to alert other AIs even if it is aware of transfers to or from other institutions. Criminals controlling the mule accounts can often exploit the resulting information gap and simply continue their activities at other AIs.

5.10 While there are ways to permit sharing of customer information where illicit activity is suspected, for example by seeking customer consent in terms and conditions, it is difficult for AIs to obtain explicit consent from existing customers, who may decline (or simply not respond to) such requests. Also, anyone engaged in financial crime would obviously refuse to give consent. The FINEST initiative is currently limited to corporate accounts because of concerns over personal data privacy if sharing is extended to personal accounts in the absence of a "safe harbour" provision. However, the great majority of mule accounts used for money laundering linked to fraud have been individual accounts.

5.11 Safeguarding data privacy and customer confidentiality is crucial for customers and the banking sector. However, there is also an increasing view that such considerations should not impede information sharing that will help AIs to file STRs containing relevant information to support LEAs' investigations, help detect or prevent crime and facilitate the interception of illicit funds. The US, the UK and Singapore have introduced provisions allowing FIs to share information in cases where financial crime is suspected. While these overseas arrangements, which are briefly summarised at the Annex, differ in various aspects, they all provide legal protection or a "safe harbour" for institutions disclosing information, subject to certain safeguards.

5.12 The HKMA believes that allowing AIs to share information, subject to appropriate safeguards, would support the purposes of preventing and detecting criminal activity. AIs which observe activity that may indicate that persons, accounts or transactions may be involved in fraud or ML/TF would be allowed to request information from other AIs which they reasonably believe may be able to provide information that will shed light on potential fraud or ML/TF risks, or to alert other AIs that may be at risk of being targeted by criminals. Such sharing would be voluntary as we believe that this is appropriate between private sector institutions, in contrast to the legal requirement to report suspicious transactions to LEAs. Similar arrangements in other jurisdictions are generally voluntary in nature.

5.13 We would also propose that AIs should be given legal protection or "safe harbour". This would mean that, provided AIs comply with all applicable requirements, disclosure of information under the proposed mechanism would not be treated as a breach of legal, contractual or other restrictions on disclosure of information. AIs disclosing information would also not be liable for any claimed loss arising out of such disclosure.

Consultation Questions:

Q1 Do you agree that AI-to-AI information sharing as described in this consultation paper, could help facilitate the swift identification and tracing of illicit funds and so should be established in Hong Kong to support efforts to detect or prevent crime?

Q2 Do you agree that AIs disclosing information under such an arrangement should be given legal protection, provided they share information solely for the purpose of preventing or detecting financial crime?

Q3 Do you agree that AIs should be able to participate in such information sharing on a voluntary basis?

6. What information would be shared and how?

6.1 The information to be shared would depend on the circumstances of individual cases and could generally include:

(a) bank account number(s);
(b) personal data[15] of a customer or counterparty who is a natural person;
(c) personal data of any beneficial owner(s) or connected party[16] of a customer who is a legal person, a trust, or a legal arrangement similar to a trust;
(d) personal data of any person purporting to act on behalf of a customer (e.g. acting under power of attorney, or an account signatory);
(e) details of relevant transaction(s) including counterparties; and
(f) reasons why the transaction(s) or activity may be involved in fraud or ML/TF.

Consultation Questions: Q4 Do you have any comments on the scope of information to be shared for the purposes of preventing or detecting financial crime?

6.2 Sharing will be via secure channels including dedicated electronic platforms such as FINEST. There will be appropriate measures to ensure that these channels are subject to strict cyber security and other relevant requirements, including restricting access to dedicated staff at AIs.

[15] E.g. name, date of birth, ID number.
[16] Connected party: (a) in relation to a corporation, means a director, (b) in relation to a partnership, means a partner, (c) in relation to a trust or similar legal arrangements means a trustee (or equivalent).

7. How will this affect the existing STR regime?

7.1 Sharing of information among AIs is proposed to be volunatary and separate from the obligation to file STRs to the JFIU. However, because AIs sharing information under the proposed arrangements are likely to file STRs in most cases, we propose to include a provision that such sharing will not constitute "tipping off" under the relevant legislation[17]. While information sharing via secure channels should not interfere with investigations resulting from STRs, we propose to put the "tipping off" point beyond doubt.

Consultation Questions:

Q5 Do you agree that information sharing among AIs as described in this paper should not constitute "tipping off" under the relevant legislation?

Q6 Do you have any other views on how the proposed information sharing arrangement should interface with the STR regime?

[17] Under section 25A(5) of OSCO and DTROP a person commits an offence if, knowing or suspecting that a disclosure has been made under subsection (1) or (4), he discloses to another person any matter which is likely to prejudice any investigation which might be conducted following that first-mentioned disclosure.

8. Safeguards

8.1 The importance of personal data privacy and customer confidentiality in banking and other financial services is well recognised, as is the need for an appropriate balance to protect the public against criminal activity, especially fraud, and safeguard the financial system against exploitation for ML/TF.

8.2 To provide appropriate safeguards to protect the interests of legitimate customers, we propose that the "safe harbour" should only apply where information is shared among AIs for the purpose of detecting or preventing financial crime. Information sharing would only be permitted among AIs, i.e. banking institutions authorized and regulated in Hong Kong under the Banking Ordinance. If an AI shares information for any other purpose, or with a non-AI, the "safe harbour" would not apply and the AI would remain subject to existing legal and contractual obligations. We would propose that AIs receiving information via the sharing mechanism should be subject to specific requirements to treat it in the same way, and to the same standards of confidentiality, as other confidential information.

8.3 We propose to impose a specific requirement to this effect in the legislative amendments and the HKMA will also issue statutory guidance setting out its expectations on how relevant requirements should be met and the circumstances in which information may be shared. Onward sharing of information received under the proposed arrangements to another AI, which is often necessary when funds are found to have been transferred after the AI has been alerted about a suspected illicit origin, would also be restricted to the same purpose of detecting or preventing financial crime and subject to the same requirements regarding confidentiality.

8.4 As noted above, information sharing will only be permitted via secure channels including dedicated electronic platforms such as FINEST. Only AIs that are technically and operationally ready and

can demonstrate that they have implemented appropriate systems and controls will be permitted to access such platforms[18].

8.5 Sharing will also only be permitted among AIs that are in a position to provide or use information for the purpose of preventing or detecting financial crime. A requesting AI will therefore only be permitted to send requests for information to other AIs where the requesting AI has reasonable grounds to believe that those AIs will be able to provide information that will assist the requesting AI in preventing or detecting financial crime, including in deciding whether to file an STR. Requests will also have to be specific and identify the subject of the request, relevant transactions and reasons why the activity observed may be involved in financial crime. General "fishing expeditions" will not be permitted. The HKMA will issue appropriate guidance to the industry on these aspects.

8.6 Similarly, AIs will only be permitted to request information from other AIs, or to disclose information for the purpose of alerting other AIs (other than in response to a request), where they have observed activity that may indicate that a person, account or transactions may be involved in fraud or ML/TF. In other words, sharing will be on a need-to-know basis, while it may involve sharing with multiple AIs, for example in cases where funds are being transferred from an identified mule account and may potentially be sent to a number of AIs.

8.7 The HKMA will issue guidance under the Banking Ordiance requiring AIs to have appropriate systems and controls for handling information shared. These will include requirements on confidentiality and for information to be dealt with by dedicated staff within the AI.

[18] Five AIs currently participate in FINEST: Bank of China (Hong Kong) Limited, Standard Chartered Bank (Hong Kong) Limited, The Hongkong and Shanghai Banking Corporation Limited, Hang Seng Bank, Limited and Industrial and Commercial Bank of China (Asia) Limited. Additional AIs may join in future.

8.8 Another area where the HKMA sees a need for safeguards relates to "de-risking". This term refers to a global phenomenon whereby banks may decline or discontinue business relationships with customers or categories of customers to avoid the risks involved, rather than properly managing those risks. If the "safe harbour" provisions are introduced in Hong Kong, the HKMA will issue corresponding statutory guidance to AIs on the need to adopt a risk-based approach with regard to information shared under the "safe harbour" provision. AIs should not terminate a relationship under the proposed arrangements merely because the customer is included in information shared, or in a request for infomation; instead they should conduct an appropriate risk assessment before taking any appropriate action.

8.9 In fact, the HKMA believes that the proposals to facilitate information sharing should help reduce the likelihood of de-risking in cases where customer activity that raises concerns with one AI may be explained and addressed by fuller information provided by another AI(s) in response to a request via the "safe harbour".

8.10 Moreover, AIs will be subject to supervision by the HKMA for this as for other aspects of their operations. We propose to introduce enforcement provisions in relation to the circumstances in which information may be shared and confidentialityrequirements, which would include powers to impose appropriate penalties on AIs that fail to comply.

Consultation Questions:

Q7 Are the proposed safeguards appropriate?

Q8 Do you have any other suggestions for safeguards that may be imposed to protect the interests of legitimate customers?

9. Implementation and timing

9.1 Depending on responses to this consultation, the HKMA will issue a consultation conclusions document with a view to preparing necessary legislative amendments in the second half of 2024.

Annex

OVERSEAS PRIVATE-TO-PRIVATE INFORMATION-SHARING FRAMEWORKS FOR THE PREVENTION AND DETECTION OF CRIME

United States

Legislation: 2002 regulations implementing section 314(b) of the Patriot Act (2001)

Scope: Money laundering and terrorist financing. Allows voluntary information sharing among FIs regarding "individuals, entities, organizations and countries for purposes of identifying and, where appropriate, reporting activities that may involve possible terrorist activity or money laundering" [19]. Covers FIs, including banks, that are subject to an anti-money laundering program requirement under FinCEN[20] regulations.

Safe Harbour: Provides FIs with the ability to share information with one another, under a safe harbour that offers protections from liability, in order to better identify and report activities that may involve money laundering or terrorist financing activities. Under section 314(b), FIs sharing information "shall not be liable to any person under any law or regulation of the United States"[21] or individual States "or under any contract or other legally enforceable agreement"[22].

An FI may share information if it "has a reasonable basis to believe that the information shared relates to activities that may involve money laundering or terrorist activity, and it is sharing the information for an appropriate purpose under Section 314(b) and its implementing regulations"[23].

19 https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf

20 The Financial Crimes Enforcement Network, which serves as the Financial Intelligence Unit in the US, which receives Suspicious Activity Reports from FIs.

21 Section 314(b), https://www.govinfo.gov/content/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf

22 Ibid.

23 Section 314(b) Fact Sheet, https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf

United Kingdom

Legislation:

(a) Criminal Finances Act 2017 that introduced new sections 339ZB – 339ZG into the Proceeds of Crime Act 2002 (POCA), and new sections 21CA – 21CF into the Terrorism Act 2000 (TA)

Scope: Money laundering and terrorist financing. Allows "banks and other businesses in the regulated sector to share information with each other on a voluntary basis in relation to a suspicion that a person is engaged in money laundering, suspicion that a person is involved in the commission of a terrorist financing offence, or in relation to the identification of terrorist property or its movement or use" [24] . Institutions sharing information are required to notify the National Crime Agency.

Safe harbour: Section 339ZF of the POCA and section 21CE of the TA respectively provide that sharing of information in good faith under the relevant provisions does not breach any obligation of confidence owed by the person making the disclosure, or any other restriction on the disclosure of information, however imposed[25].

(b) Economic Crime and Corporate Transparency Act 2023

Scope: Economic crime. Allows banks and certain other specified businesses in the regulated sector to share customer information with each other, either directly or indirectly through a third-party intermediary, for the purposes of preventing, detecting or investigating economic crime. The disclosing institution must be satisfied that the information disclosed will assist (direct or indirect) recipients in relation to customer due diligence and determining risk-mitigating actions with regard to business relationships or products and services. Unlike under the POCA and the TA described above, businesses can share information amongst themselves without having to involve LEAs.

Safe harbour: Sections 188 and 189 provide that the "disclosure of information will not give rise to breach of obligations of confidence nor to any civil liability to the person to whom the information relates, albeit that

[24] UK Home Office Circular, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/679032/HO_Circular-_Sharing_of_information_within_the_regulated_sector_1.0.pdf

[25] Ibid.

data protection obligations in relation to data accuracy, integrity, purpose, storage and accountability will continue to apply."

Singapore

Legislation: Financial Services and Markets (Amendment) Act 2023[26] (FSMA 2023)

Scope: Money laundering, terrorist financing and financing of proliferation of weapons of mass destruction (proliferation financing). Permits sharing of information via a dedicated electronic platform[27] solely for the purposes of mitigating money laundering, terrorism financing and proliferation financing risks based on pre-determined red flags and subject to controls to safeguard information security and confidentiality. Covers banks and other financial institutions (prescribed FIs).

Safe Harbour: FSMA 2023 provides statutory protection from civil liability for FIs in respect of their disclosure of risk information, provided that the disclosure was made, among others, with reasonable care and in good faith[28]. Relevant provisions of the Personal Data Protection Act 2012 do not apply to prescribed FIs sharing information under the framework[29].

[26] Financial Services and Markets (Amendment) Act 2023, https://sso.agc.gov.sg/Acts-Supp/19-2023/Published/20230628?DocDate=20230628#:~:text=29%20May%202023.%20An%20Act%20to%20amend%20the,Singapore%2C%20as%20follows%3A%20Short%20title%20and%20commencement%201

[27] Called COSMIC – Collaborative Sharing of ML/TF Information & Cases.

[28] See section 28I of the FSMA 2023.

[29] See section 28M of the FSMA 2023.