Recommendations for Regulating and Supervising Bank and Non-bank Payment Service Providers Offering Cross-border Payment Services

Final report

12 December 2024

The Financial Stability Board (FSB) coordinates at the international level the work of national financial authorities and international standard-setting bodies in order to develop and promote the implementation of effective regulatory, supervisory and other financial sector policies. Its mandate is set out in the FSB Charter, which governs the policymaking and related activities of the FSB. These activities, including any decisions reached in their context, shall not be binding or give rise to any legal rights or obligations.

Contact the Financial Stability Board

Sign up for e-mail alerts: www.fsb.org/emailalert
Follow the FSB on X/Twitter: @FinStbBoard
E-mail the FSB at: fsb@fsb.org

Copyright © 2024 Financial Stability Board. Please refer to the terms and conditions

Table of Contents

Executive summary 1

Introduction 3

Scope of the Report 5

Definition of terms 7

1. The role of banks and non-banks in cross-border payments 10

1.1. Banks 11

1.2. Non-banks 12

1.3. Impacts of regulatory and supervisory inconsistencies 14

2. Cross-Border payment frictions and risks 15

2.1. Interdependencies with other G20 Roadmap workstreams addressing compliance-related frictions 16

2.2. Risks associated with cross-border payments services 17

3. Principles for developing recommendations 22

4. Recommendations for improving alignment of PSP regulatory and supervisory regimes 23

Annex 1: Survey of existing standards, recommendations, and guidance 30

Annex 2: Survey of domestic regulatory and supervisory frameworks 35

Executive summary

This report sets out policy recommendations to strengthen consistency in the regulation, supervision and oversight of banks and non-banks in their provision of cross-border payment services in a way that is proportionate to the risks associated with such activities. Greater consistency in the treatment of payment services across payments service providers (PSPs) supports an environment that facilitates reduced costs, increases delivery speed, and improves financial access and transparency by establishing a level playing field, to the extent possible given differences in business models and risk profiles, for both banks and non-bank PSPs. This approach reduces the prospect of regulatory arbitrage. This work forms part of the Financial Stability Board's (FSB) work programme for enhancing cross-border payments.

Advances in technology have shaped and will continue to reshape the cross-border payments landscape, increasing the number and variety of PSPs and services they offer. In response to these changes, legal, regulatory, and supervisory frameworks that govern PSPs have had to rapidly adapt and evolve. In the absence of comprehensive international standards applicable to non-bank PSPs' provision of cross-border payment services, jurisdictions have taken varying approaches to regulating and supervising bank and non-bank PSPs offering these services.

The FSB has analysed existing standards, recommendations, and guidance relevant to cross-border payments developed by international standard-setting bodies (SSBs) and other organisations. It has also reviewed the regimes currently in place in a small sample of jurisdictions to better understand the different approaches being taken. Taken together, these reviews highlight an opportunity for policy adjustments to strengthen consistency both within and across jurisdictions, while maintaining flexibility to accommodate the wide variety of national regulatory and supervisory frameworks applied to cross-border payments activities conducted by both banks and non-banks. This report has been revised to reflect the feedback received on its public consultation issued in July 2024.[1]

The six policy recommendations in this report are directed at competent authorities. Recommendations 1 to 3 detail steps that should be taken to identify, understand, and assess risks across the PSP sector; to evaluate the effectiveness of existing laws, regulations, and supervisory frameworks in addressing these risks to identify needed adjustments; and to ensure the protection of consumers who use cross-border payment services. Recommendation 4 addresses the need for clear guidance on supervisory expectations across the sector to promote the safe and efficient provision of cross-border payment services. Recommendation 5 covers the role of licensing or registration requirements in ensuring a risk-proportionate level playing field from the time a PSP enters the sector. Recommendation 6 emphasises the need to foster expanded information and data sharing both within and across jurisdictions, which is critical to conducting comprehensive risk assessments and, as needed, taking regulatory or supervisory actions.

This report completes priority action 4(a) and paves the way for the following next steps that were agreed under the Roadmap implementation plan (priority actions 4(b), 4(c), and 4(d)). As

---

[1] A list of public responses to the consultation report and an overview of responses, including how the feedback was reflected in this final report, can be on the FSB website.

part of further work, the FSB will organise a workshop in the first half of 2025 with the private sector to exchange practices in the regulation, supervision and oversight of non-bank PSPs and to support implementation of the BNBS policy recommendations, while further exploring the need for international guidance, principles or standards for the regulation, supervision and oversight of non-bank service providers. Upon completion of priority actions 4(b), 4(c), and 4(d), in 2027 the FSB will take stock of the progress in implementing the BNBS recommendations, to learn from experiences and support further jurisdictional implementation.

Introduction

The G20 Leaders endorsed the Roadmap for enhancing cross-border payments at their November 2020 Summit to address four challenges that cross-border payments face relative to domestic payments: high cost, low speed, and insufficient access and transparency.[2] In 2021, the FSB published targets for addressing these four challenges across three payment market segments: wholesale, retail, and remittances.[3] The Roadmap takes a comprehensive and holistic approach to addressing these challenges by evaluating potential solutions and promoting practical actions from both the private and public sectors.

In February 2023, the FSB published the G20 Roadmap for Enhancing Cross-border Payments: Priority actions for achieving the G20 target*s,* that identified the actions and projects determined to be the best way to achieve the G20 quantitative targets set for addressing the identified challenges.[4] Based on FSB analysis and feedback received through industry outreach events, the FSB Working Group on Bank and Non-Bank Supervision (BNBS) was tasked with developing recommendations for advancing priority action 4(a) to strengthen consistency in the application of regulation, supervision and oversight to banks and non-banks providing cross-border payment services proportional to their respective risks.[5] This final report reflects responses received to a consultation report[6] published earlier this year and completes priority action 4(a).

Differences in the coverage or application of legal, regulatory, or supervisory regimes to banks and non-banks that provide cross-border payment services have been identified as adversely affecting efforts to successfully address the identified Roadmap challenges and meet the G20 targets.[7] Inconsistencies can arise in a variety of areas such as licensing, consumer protection requirements, and the implementation of anti-money laundering/combating the financing of terrorism (AML/CFT) measures, including compliance with economic sanctions requirements, as well as data protection and privacy measures. For example, actual or perceived differences in the scope and application of regulation, supervision and oversight regimes to banks and non-banks can contribute to the complex processing of compliance checks that in turn results in higher costs and lower speeds for cross-border payments. The impact of these on cross-border payment costs may therefore be significant, driven in part by the need to organise and maintain a level of resources sufficient to meet compliance obligations.

---

[2] G20 (2020), 2020 Riyadh Summit Leaders' Declaration (paragraph 16), 21 November. FSB (2020), *Enhancing Cross-border Payments - Stage 1 report to the G20*, April. CPMI (2020), *Enhancing cross-border payments: building blocks of a global roadmap Stage 2 report to the G20*, July. FSB (2020), *Enhancing Cross-border Payments - Stage 3 report to the G20*, October.

[3] FSB (2021), *Targets for Addressing the Four Challenges of Cross-Border Payments*, October.

[4] FSB (2023), *G20 Roadmap for Enhancing Cross-border Payments: Priority actions for achieving the G20 targets*, February.

[5] The FSB Stage 1 assessment report identified seven underlying frictions contributing to the four challenges. The CPMI's Stage 2 report identified 19 "building blocks)" in four focus areas to address the identified frictions. One of the building blocks focused on the alignment of regulatory and supervisory frameworks applied to banks and non-banks in focus area B: Regulatory, supervisory and oversight frameworks. See CPMI (2020*), "Enhancing cross-border payments: building blocks of a global roadmap Stage 2 report to the G20",* July.

[6] FSB (2024), *Recommendations for Regulating and Supervising Bank and Non-bank Payment Service Providers Offering Cross-border Payment Services: Consultation report*, July.

[7] FSB (2022), *G20 Roadmap for Enhancing Cross-border Payments: Priorities for the next phase of work*, October. The report identifies three priority themes: payment system interoperability and extension; legal, regulatory, and supervisory frameworks; and cross-border data exchange and standards. With respect to the second identified theme, it also identifies a series of actions for each of the identified themes to take these themes forward. Strengthening the consistency in the regulation, supervision and oversight of bank and non-bank providing cross-border payment services is one of the actions in the second theme.

Regulatory frameworks, including those imposed through licensing regimes, for non-banks differ widely across jurisdictions, and the impacts of such differences may become more pronounced as new technologies continue to expand consumer access to, and facilitate the provision of, cross-border payment services. For example, inconsistent implementation of, or variations on, the application of AML/CFT measures, including customer due diligence (CDD) requirements, across jurisdictions can reduce the processing speed and increase the cost of cross-border payments. More effective and consistent implementation of the standards issued by the Financial Action Task Force (FATF), including those relating to CDD, correspondent banking, money or value transfer services, new technologies, and wire transfers, among others, across jurisdictions could help reduce the identified challenges associated with the provision of cross-border payment services. Differences in the requirements applied to banks and non-bank PSPs and the resultant variations in risk management practices, may not only impact banks' willingness to provide services to non-bank PSPs, but more generally could impact the reliability, security, and efficiency of cross-border payment services. This in turn could limit speed and access, while increasing costs.

The recommendations presented in this final report promote the G20 targets to enhance cross-border payments by ensuring quality and consistency in the legal, regulatory, and supervisory regimes for PSPs and promote greater alignment between those applicable to banks and non-banks in their cross-border payment activities. Focus areas include differences in the application of regulatory requirements related to the management of risks, including money laundering and terrorist financing (from now on defined as "financial crimes") risks, as well as how the real-or-perceived adequacy of related supervision in managing operational risk and resilience may affect banks' willingness to provide cross-border payment related services to non-banks.

In addition to improved risk management resulting from increased alignment, and more effective information sharing and collaboration across competent authorities, public policy objectives such as increasing transparency related to service terms, conditions, and pricing, as well as supporting consumer access may also be achieved.

The report is organised as follows:

- Section 1 provides a brief overview of the role of banks and non-banks in cross-border payments;
- Section 2 discusses the relevant frictions and risks;
- Section 3 defines the principles identified based on the analysis conducted in the report, which frame the boundaries of the report's recommendations, and on the discussions in the previous sections;
- Section 4 proposes specific recommendations for strengthening consistency in regulating and supervising banks and non-banks in their provision of cross-border payment services.

The Annexes provide information on existing work conducted by the FSB, SSBs, and relevant international organisations; and examples from a few jurisdictions to highlight various approaches for regulating and supervising banks and non-banks in their provision of cross-

border payment services. These have all informed the development of the recommendations in this report.

In addition, the FSB published the proposed recommendations for public comment in July 2024 and received feedback from 21 respondents, from North America, Asia-Pacific and Europe. The responses received spanned various entities in the cross-border payments ecosystem such as banks, non-bank payment service providers (PSP), credit card schemes and clearing houses. The recommendations were revised to account for these public comments.[8]

The completion of this priority action paves the way for the next steps agreed under the Roadmap and the implementation timeline described below.[9]

According to priority action 4(b), in 2025 SSBs should adapt their regulatory, supervisory and oversight standards or guidance, as needed, in line with the FSB recommendations.

In the first half 2025 the FSB will organise a workshop with the private sector to exchange practices in the regulation, supervision and oversight of non-bank PSPs and to support implementation of the BNBS policy recommendations, while further exploring the need for international guidance, principles or standards for the regulation, supervision and oversight of non-bank PSPs. Moreover, based on the findings of the workshop, in 2025 the FSB and Committee on Payments and Market Infrastructures (CPMI) will review whether to develop recommendations for reducing legal or regulatory barriers to non-bank PSPs' participation in payment systems, while ensuring that risk mitigation measures are proportionate (Action 4(c)), having regard to this report and earlier work conducted through the CPMI, including through the sharing of views in the CPMI Community of Practice on Payment Systems (COPS).

In 2026 national authorities should evaluate what changes to make to their frameworks consistent with the FSB and (if developed) CPMI recommendations and international standards and guidance, and report on any such changes (Action 4(d)).

In 2027 the FSB will take stock of the implementation of the recommendations set forth in this report, to learn from experiences and support further jurisdictional implementation.

Scope of the Report

The absence of a single, comprehensive set of international standards governing the provision of cross-border payment services has resulted in jurisdictions applying various approaches to regulating and supervising banks and non-banks. Both banks and non-banks are subject to the FATF Standards for combating financial crime (money laundering, terrorism financing and other illicit financial activities).[10] Banks are subject to comprehensive international prudential

---

[8] FSB (2024), *Recommendations for Regulating and Supervising Bank and Non-bank Payment Service Providers Offering Cross-border Payment Services: Consultation report*, July. A list of the public responses and an overview of how the feedback was reflected in this final report can also be found on this FSB webpage.

[9] For further Priority Actions on improving consistency of bank and non-bank regulation, supervision and oversight see, FSB (2022), *G20 Roadmap for Enhancing Cross-border Payments: Priorities for the next phase of work*, October

[10] FATF (2023), *The FATF Recommendations*, November. The FATF Recommendations set an international standard, which countries should implement through measures adapted to their circumstances. The FATF standards comprise the Recommendations themselves and their interpretive notes, together with the applicable definition in the Glossary.

supervisory standards set by the Basel Committee for Banking Supervision (BCBS); and financial market infrastructures (FMIs) are subject to the standards set by the CPMI and the International Organization of Securities Commissions (IOSCO) to promote their safety and efficiency and that of related arrangements. However, there are currently no comprehensive, globally agreed international standards that fully govern either the supervision and oversight of the provision of payment services to consumers and businesses generally, or prudential supervision and oversight of non-bank PSPs in their provision of such services.[11]

The recommendations in this report seek to strengthen consistency (within and across jurisdictions) between the regulatory and supervisory regimes for banks and non-banks concerning the provision of cross-border payment services and are focused on providers of services to end-users. They also recognise that there is a range of regulatory and supervisory approaches currently being applied across jurisdictions with respect to these activities. Furthermore, banks' provision of these services is subject to prudential regulation, to supervision and to oversight that is typically applied at a consolidated or entity level. The banks themselves are subject to robust governance, capital, liquidity, and risk management frameworks. While noting differences across jurisdictions, capital adequacy-related prudential requirements applied to cross-border payment providers such as those related to credit, liquidity, and other related risks, are not within the scope of this report. Furthermore, the proposed recommendations are not intended to apply to FMIs, the international standards for which are in the *Principles for Financial Market Infrastructures*[12] (PFMI) issued jointly by the CPMI and IOSCO.

The recommendations are not intended to weaken the current model for regulating and supervising banks, given their important role in financial stability, nor to raise the bar unjustifiably for non-banks, but rather to aid in identifying and addressing gaps resulting from inconsistencies in how banks and non-banks are regulated and supervised that contribute to the underlying frictions and resulting challenges the Roadmap is seeking to address. The recommendations are addressed to competent authorities (e.g. central banks, financial supervisory authorities, consumer protection authorities, ministries of finance, financial integrity units, conduct authorities).

Improving the consistency of the frameworks relevant to the provision of cross-border payment services does not mean that banks and non-banks should be subject to the same regulatory or supervisory regimes, particularly given that the Basel framework, which governs the broad range of activities banks undertake, has been broadly implemented across the globe and is important in maintaining financial stability. Instead, the objective is to ensure that the same cross-border payment services when undertaken by both banks and non-banks are subject to similar regulation, supervision, and oversight that are aligned with, and proportional to, the risks present in their cross-border-payment-related business models and organisational structures, while also

[11] Standards such as those established by the European Union's *Payment Services Directive 2 (PSD2)* and the United Kingdom's Wire Transfer Regulations, may be consistently applied at regional levels governing the supervision or oversight of cross-border payment services.

[12] CPMI, IOSCO (2012), *Principles for Financial Market Infrastructures*, April.

considering national policy priorities.[13] This is consistent with an approach of "same activity, same risk, same rules".

This report is focused primarily on addressing the identified Roadmap challenges that result from the complexities in meeting compliance requirements, including those related to AML/CFT, while acknowledging that addressing this underlying friction may impact other frictions, such as fragmented and truncated data formats, weak competition, and long transaction chains. It focuses on retail funds transfers and does not address asset transfers or related services (including technologies or platforms that support crypto-asset or other digital asset-related activities, which are already covered in other publications).[14] Further, this report does not focus on non-bank direct access to central bank operated payment systems, as the CPMI has done work on this topic[15] and this issue will be further considered as part of in Action 4(c). Finally, while considerations of data framework alignment and interoperability, data localisation and data protection and privacy have implications for consumers and for exchanging information to meet AML/CFT and other compliance obligations, these issues are also not the focus of this report. However, where appropriate, this report notes the connections with the report and recommendations simultaneously being finalised by the FSB, with a specific focus on data frameworks.

The analysis and resulting recommendations in this report are intended to complement the relevant existing body of work in this area and to be flexible so they can be incorporated into the wide variety of national regulatory and supervisory frameworks that are applicable to cross-border payments activities conducted by both banks and non-banks. To this end, the BNBS reviewed work conducted by the FSB and relevant SSBs and brief summaries of these reviews are included in Annex 1 (Survey of existing work).

Definition of terms

The definition and use of terms vary across jurisdictions, often reflecting the different legal and regulatory frameworks under which banks and non-banks offering payment services are organised and operate. As a result, SSBs such as the FATF, BCBS, and the CPMI have sought to standardise definitions and this section draws on these efforts to improve consistency and better inform the discussion contained in this report.

Activity-based regulation

As used in this report, activity-based regulation refers to the consistent application of regulatory requirements directly applicable to activities on a stand-alone basis that generally does not vary

---

[13] The Financial Stability Institute's (FSI) (2021), Fintech regulation: how to achieve a level playing field*, 2021 Occasional Paper,* provides a helpful analytical framework for considering how achieving a level-playing field fits within jurisdictions' policy priorities and how it might be achieved through a combination of activity- and entity-based rules.

[14] FSB (2023), *Global Regulatory Framework for Crypto-asset Activities*, July, which consists of the FSB (2023), *High-level Recommendations for the Regulation, Supervision and Oversight of Global Stablecoin Arrangements: Final report*, July, and the FSB (2023), *High-level Recommendations for the Regulation, Supervision and Oversight of Crypto-asset Activities and Markets: Final report*, July.

[15] Moreover, the CPMI has done work on best practices for the self-assessment whenever considering improving access to payment systems for cross-border payments (CPMI (2022), "*Improving access to payment systems for cross-border payments: best practices for self-assessments*", May). Based on that, work is currently being brought forward by the COPS and the CPMI's payments interoperability and extension (PIE) taskforce.

with the type of entity that performs the activity or other activities that the entity performs. Compliance with activity-based regulation may be ensured by sanctions and other enforcement actions applied by the regulators and supervisors that facilitate oversight of such activities by competent authorities. For example, the FATF standards include a requirement that jurisdictions implement a funds transfer rule to capture information associated with payments activity, regardless of entity type.

Entity-based regulation

Entity-based regulation strengthens the resilience of activities indirectly, as it is calibrated at the level of the entities that perform them, and may include governance, prudential, and conduct requirements that are supported by supervisory activities. Since an entity's resilience hinges on the mix of its activities, entity-based regulation imposes constraints on the combination of those activities and is core to financial stability regulation.[16] Competent authorities may also adopt a hybrid approach that combines elements of both activity- and entity-based regulation depending on the nature of each jurisdiction's regulatory structure.

Payments

These are defined as an act to place, transfer, or withdraw funds denominated in a fiat currency (e.g. a monetary claim) from a payer to a payee. Typically, such funds take the form of cash (i.e. physical form of currency such as bank notes or coins) or deposit balances or electronic money held at a financial institution. For purposes of this report, payments will cover all types of electronic funds transfers and instruments (e.g. cheques, credit transfers, direct debits, card payments, e-money). Cross-border payments are funds transfers for which the payer and the payee are in different jurisdictions.[17]

Payment service provider (PSP)

As used in this report, the term PSP includes all entities (banks and non-banks) that provide payment services, including. prepaid transfers (e.g. prepaid cards or traveller's checks) and pay later transfers such as credit card transfers, and individuals providing payment services,[18] services enabling cash to be placed on or to be withdrawn from an account, the issuing of payment instruments and the acquiring of payment transactions, payment initiation services, and, in certain jurisdictions, account information services.[19] This report focuses on PSPs that offer services directly to end users such as consumers and businesses.

---

16 Borio, C, S Claessens and N Tarashev (2022), Entity-based vs activity-based regulation: a framework and applications to traditional firms and big techs, *FSI Occasional Paper*, no.19. August.

17 FSB (2024), *Annual Progress Report on Meeting the Targets for Cross-border Payments: 2024 Report on Key Performance Indicators*, October.

18 Committee on Payment and Settlement Systems and the World Bank (2007). *General principles for international remittance services*, January.

19 "PSP" includes the terms "remittance service providers" (RSPs), "money services businesses" (MSBs) and "other providers of money or value transfer services" (MVTS) that are used in other contexts.

Payment system

This is defined as a "set of instruments, procedures and rules for the transfer of funds between or among participants, the system includes the participants and the entity operating the arrangement." [20] Payment systems can facilitate wholesale payments between participants, who are typically financial institutions, sometimes including central banks, or retail payments [21] between customers of those participants and which are mainly high volume, low value transfers. Participation in payment systems can be direct, or indirect. Indirect participation generally involves a direct participant as intermediary, thus offering an alternative to access payment systems. [22] The focus of this report is retail payments.

Proportionality and risk-based approach

Proportionality is the principle of applying appropriate levels of regulatory or supervisory measures commensurate with risk profile and systemic importance of a given entity or activity. The concept of proportionality is intended to facilitate the application of regulatory and supervisory requirements to a wide range of activities and/or entities that create different types or levels of risk to financial systems, entities, or end users. A "Risk-based approach" (RBA) is a related concept in which regulatory and supervisory measures are applied based on the risks posed by the activities or entities taking into account limited supervisory resources. In the context of financial inclusion, the application of a RBA requires appropriate identification of the risks presented by individual transactions, users, or PSPs to mitigate the risks sufficiently to continue to ensure the access of legitimate parties to those services. For purposes of this report, proportionality and RBA are used interchangeably unless specifically noted.[23]

Regulation, supervision and oversight

Although generally referenced together, there is a distinction between these types of activities that may fall under the scope of separate authorities in a jurisdiction. "Regulation" references the rules set by regulators under governing laws that are applicable to entities and activities within specific financial sectors, groups of institutions, and individual entities, as well as customer types. "Supervision" references the strategies and resulting measures that competent authorities may apply in monitoring and enforcing compliance with regulations. In some jurisdictions supervisors may exercise discretion in interpreting and applying rules established by other competent authorities within their jurisdictions, but changing those rules may be beyond their scope of authority. Furthermore, supervisory approaches usually reflect the principle of proportionality and may also differ depending on whether the regulations are activity- or entity-based. PSP oversight is generally focused on assessing success or progress in complying with certain requirements or meeting outcomes or targets such as greater operational and risk-management efficiency and effectiveness and financial stability.

---

20 CPSS, IOSCO (2012), *Principles for financial market infrastructures*, April.

21 Retail payments are described as low-value payments (FSB (2020), *Enhancing Cross-border Payments - Stage 1 report to the G20*, April).

22 CPMI (2022), *Improving access to payment systems for cross-border payments: best practices for self-assessments*, May.

23 For additional discussion of proportionality, see BCBS (2022), *High-level considerations on proportionality*, July.

1. The role of banks and non-banks in cross-border payments

Advances in digital technology are playing a key role in improving the efficiency and effectiveness with which funds are transferred across borders. New service providers supplying more delivery channels based on new technologies offer consumers access to more convenient, cheaper, and faster options for conducting transactions such as paying bills, purchasing goods and services, and transferring cash to others. While this trend was on the rise before the COVID-19 pandemic, demand for digital payment services and the number of service providers participating in the cross-border payments ecosystem increased significantly during the pandemic.[24] Within the realm of cross-border payments, both banks and non-banks are critical in facilitating global trade, contributing to economic growth and development, and providing access to essential financial services.

Banks have historically held the predominant role in the provision of cross-border payment services; however, non-bank PSPs entering the cross-border payments market have generated significant changes in the market structure and have, in some jurisdictions, become competitors to banks and expanded the range of payment options available to consumers while assuming a complementary function to banks in other important domains, often leveraging new technologies.

Bank and non-bank PSPs cover a broad range of cross-border operating market domains, including e-commerce, mobile payments, person-to-person payments, business-to-business payments, and remittances. The specific roles they assume in each of these ecosystems are determined by the regulatory environment in which they operate and their specific business models. Nevertheless, in the context of engagement with the public, both bank and non-bank PSPs expressed concerns about complying with AML/CFT requirements that vary across jurisdictions and the differences in regulatory and supervisory frameworks that govern the provision of cross-border payment services in jurisdictions worldwide. In addition, non-bank PSPs also raised their interest in directly accessing payment systems and infrastructures.

While the role of banks and non-banks in the cross-border payment space has evolved over time, in some circumstances, banks have limited or decreased the provision of account and other services to non-bank PSPs as part of their risk tolerance and risk management strategies, as well as in response to changes in bank business models or profitability concerns. The changing business models of non-bank PSPs, combined with the potential inconsistency or uncertainty in the regulation, supervision and oversight of non-bank PSPs in some jurisdictions, may raise concerns about whether all the risks posed by their business models are addressed sufficiently, both at the level of the entity as well as in the context of partnerships with banks. For example, there could be concerns by banks and by authorities with respect to non-bank PSPs' management of operational risk (e.g. fraud, cyber risks) and resilience. These factors could affect the ability of non-bank PSPs to access and maintain necessary banking and payment services that could, in turn, impact cost, speed, and access related to cross-border payments. This is covered in greater detail in section 1.3.

---

[24] World Bank (2022), *COVID-19 Drives Global Surge in use of Digital Payments*, June.

1.1. Banks

Banks play a multifaceted role in cross-border payments that reflects their deep integration in the global financial system. In addition to offering depository and lending services, banks also provide both front- and back-end cross-border payment services to consumers and businesses, thereby facilitating economic growth and trade internationally, and supporting expanded access to financial services in underserved and underbanked communities. Banks with direct participation in payment systems also provide indirect participation possibilities for non-bank PSPs. For example, banks can provide payment services directly to customers and other end-users, increasing convenience and improving the overall customer experience. They can also provide payment services to other banks and non-bank PSPs, for example enabling them to establish and maintain deposit accounts or to access domestic and cross-border payment infrastructures.

Banks that provide correspondent banking services play a unique and critical role in the context of cross-border payments. Correspondent banking is "an arrangement under which one bank (correspondent) holds deposits owned by other banks (respondents) and provides payment and other services to those respondent banks," including processing foreign currency transactions.[25] Respondent banks often rely on correspondent banking relationships to facilitate payments with jurisdictions in which they do not themselves operate. Correspondent banking relationships are essential to the stability, economic growth, and inclusion of emerging markets and developing economies (EMDEs), especially in those jurisdictions that rely heavily on trade, foreign direct investment, and remittances and which may otherwise be unable to readily access international trade and financial markets.

With respect to retail cross-border payments, banks operate on behalf of the payer, or the payee and provide a range of payment services directly to end users, including electronic funds transfers and currency conversions as well as, online and mobile banking and ATM services. The levels and nature of risk exposure may vary with the roles that banks may play in the payment chain. Banks may also operate as intermediaries to other banks. Banks facilitate access to critical payment infrastructures to enable consumers, businesses, and other financial institutions to participate in payment networks and securely use payment services. In addition, in the context of global card networks, banks act as card issuers and merchant acquirers, the latter being a critical role connecting merchants to the card network.[26]

Finally, banks' access to payment systems and settlement accounts enables them to act as key intermediaries in the clearing and settlement of cross-border transactions. In payment systems that settle in central bank money, banks are typically direct participants with settlement accounts. This direct participation allows them to function as intermediaries for non-bank PSPs and other financial institutions that do not hold settlement accounts with a central bank, which is the case for non-bank PSPs in most jurisdictions. According to the World Bank's 6th global payment systems survey of October 2023, non-bank PSPs' access to payment systems and settlement

[25] Committee on Payments and Market Infrastructures (2016), *Correspondent banking*, July.

[26] The Committee on Payment and Settlement Systems defines acquirer as "the entity or entities that hold(s) deposit accounts for card acceptors (merchants) and to which the card acceptor transmits the data relating to the transaction. The acquirer is responsible for the collection of transaction information and settlement with the acceptors", CPSS (2003), *A glossary of terms used in payments and settlement systems*, March (updated in June 2015).

accounts is slowly rising but remains generally low. The report notes that "direct access of supervised non-bank financial institutions (NBFIs) including access to central bank credit is more common in high-income economies, while access to a settlement account only is more common in [low and middle-income countries]. In contrast, unsupervised NBFIs typically do not have direct access to real-time gross settlement (RTGS) systems. In only four cases direct access was reported, all of them without access to central bank credit, the same as in the 2018 iteration."[27,28]

The crucial role of banks in cross-border payments is further exemplified by the functions they perform in wholesale cross-border payments, wherein they facilitate large-value transactions between financial institutions, and which creates additional responsibilities in liquidity management and risk mitigation with respect to credit, liquidity, and currency risk. In addition, banks are typically required by regulation, supervision and oversight to ensure that provision of banking services to and via other financial institutions, including non-bank PSPs, are appropriately managed from a risk management perspective. Therefore, banks are generally expected to implement robust risk management strategies to safeguard the integrity of wholesale payment systems and are subject to comprehensive regulatory and supervisory standards.

1.2. Non-banks

Non-bank PSPs include a wide range of providers, reflecting the range and complexity of the retail payments[29] service offerings available to consumers. Non-bank PSPs differ significantly in size and complexity, and in how comprehensively they may be regulated and supervised by different competent authorities. Non-bank PSPs span a spectrum of risks and do not uniformly present a higher financial crime risk than banks. Non-banks' growing involvement in the payments ecosystem has increased competition by offering alternative payment channels encouraging technological innovations in the payment industry.[30] Their presence and involvement in the global retail payments can be considered in some respects as alternatives to the roles that banks play and in others as complementary to those roles. They offer benefits by extending financial services to more consumers and encouraging competition, thereby potentially reducing costs for end-users, and promoting financial inclusion.[31] The number of non-bank PSPs and their market presence has risen in part due to the increase in the demand for digital payment services during the COVID-19 global pandemic, but also due to consumers'

---

27 The World Bank (2023), *A Snapshot Payment Systems Worldwide - Summary Outcomes of the Sixth Global Payment Systems Survey*, October, p. 27-28. According to the *World Bank* for the 2025 fiscal year "low-income economies are defined as those with a gross national income (GNI) per capita, calculated using the *World Bank Atlas method*, of USD 1,145 or less in 2023; lower middle-income economies are those with a GNI per capita between USD 1,146 and USD 4,515; upper middle-income economies are those with a GNI per capita between USD 4,516 and USD 14,005; high-income economies are those with more than a GNI per capita of USD 14,005."

28 The World Bank defines NBFI as "a financial institution that does not have a full banking licence and cannot accept deposits from the public," which includes, but is broader than just non-bank PSPs, including "insurance firms, venture capitalists, currency exchanges, some microloan organisations, and pawn shops." See World Bank (2016), *Global Financial Development Report 2015/12015*.

29 Retail payments "describes all payments which are not included in the definition of large-value payments. Retail payments are mainly consumer payments of relatively low value and urgency" (CPSS (2003), "*Glossary of terms used in payments and settlement systems*", March, updated in June 2015).

30 For example, according to Boston Consulting Group's (BCG) *Global Payments Report 2024* published in September 2024, payment-focused FinTechs numbered 6,500 globally, attracting more than USD 125 billion in equity funding over the past 25 years.. The BCG's *Global Payments Report 2023* anticipates they could command a revenue pool worth USD 520 billion by 2030.

31 FSI (2021), Fintech and payments: regulating digital payment services and e-money, *FSI Insights*, No. 33, July, p.9.

increased demand for faster, cheaper, and more convenient payment options. Technological developments have expanded the types of services available to customers to meet this demand, accompanied by the proliferation of non-bank PSPs delivering these services and the technology providers supporting the provision of these services and, in some markets, the introduction of specific supervisory regimes for non-bank PSPs.

Like banks, a variety of non-bank PSPs now offer payment services to consumers and businesses directly, as well as offering white-label payment and related back-office services to financial institutions. This is driven in part by technological developments that have facilitated the entry of large technology companies with established platforms (e.g. BigTechs) and other FinTech companies (e.g. large non-bank merchant acquirers,[32] payment processors, and device manufacturers) into a market in which banks had been the predominant providers.[33]

The growth in the number of non-bank PSP has resulted in increased competition in the global payments market. While banks have traditionally served as the primary channel for remittances, non-bank PSPs have emerged as an alternative cross-border channel for the transfer of funds and, in some markets, have become the dominant providers of payment services. Some of these PSPs may be linked to established technology platforms; others may offer services through multiple technology providers and platforms. Often, non-bank PSPs rely on banks for access to payment infrastructures. However, some non-bank PSPs provide services to other PSPs, for example, to issue payment instruments, acquire and process payment transactions, manage ATMs and terminals, conduct fraud risk management, and provide digital banking services, some of which may be enabled by open banking models.

While there has been an increase in the number of non-bank PSPs, banks continue to provide payments services directly to their customers and many provide clearing and settlement services to non-bank PSPs. This synergy has resulted in an increase in partnerships between non-bank PSPs and banks to provide payment services and financial products. In many of these arrangements, the underlying transaction account that is used to make and receive payments may be held by a bank, making it highly likely that a bank is involved in either the customer-facing "front-end" of a payment transaction or the clearing and settlement processing "back-end". However, in some jurisdictions non-banks can also offer payment accounts and provide white label front-end solutions to banks, as well as offer clearing and settlement services. Local laws may require non-banks offering payment services to maintain segregated accounts for client funds with commercial banks, leading them to set up and maintain a complex architecture of accounts with commercial banks to enable the transfer of their clients' funds. Additionally, as banks seek to better manage associated risks, they may consider limiting or decreasing the provision of account and other services to non-bank PSPs.[34]

---

[32] For example, according to the Nilson Report, the eight largest merchant acquirers in 2022 conducted 225,87 billion transactions, representing 48% of the top 150 acquirers worldwide, and six of the eight were non-banks. See Nilson (2023), *Nilson Report 1242*, May

[33] For purposes of this report, FinTech is defined as technology-enabled innovation in financial services. See FSB (2017), *Financial Stability Implications from FinTech. Supervisory and Regulatory Issues that Merit Authorities' Attention*, June.

[34] In its opinion dated January 5, 2022, the European Banking Authority (EBA) found that "de-risking" occurred across the European Union and often included entire categories of bank customers, including payment and e-money institutions. EBA (2022), *Opinion of the European Banking Authority on 'de-risking'*, January. In the context of this Opinion 'de-risking' is defined as the decision of a financial institution to refuse to enter into, or to terminate, business relationships with individual customers or categories of customers associated with higher financial crime risks.

By leveraging technology, non-bank PSPs have developed products and services that address gaps in existing retail payments systems. Those gaps are often the result of weaknesses in legacy infrastructures and limited access to financial services. In general, innovative payment solutions developed by non-bank PSPs have led to increased processing speed and cost-efficiency. Some wallet service providers, for instance, have been able to easily connect underlying bank accounts or facilitate strong customer authentication in a convenient manner. Increased access to and availability of cross-border payment services have been linked to improvements in financial inclusion, with developments in mobile banking enabling these services to reach populations that are typically underserved by traditional banking services or that banks consider insufficiently profitable.

These new business models, as well as potential inconsistency or uncertainty in the regulation, supervision and oversight of non-bank PSPs in some jurisdictions, may raise concerns about whether all the risks posed by their business models are addressed sufficiently, both at the entity level as well as at the level of the partnerships with banks.

Box 1: Varying approaches to regulating, supervising and overseeing PSPs

In the absence of comprehensive international standards, except for the FATF's AML/CFT standards, jurisdictions have taken a variety of approaches to regulating and supervising PSPs in their provision of cross-border payments. Jurisdictions often use a mix of activity-based and entity-based approaches to this regulation, supervision and oversight, and in some cases with the express intent of promoting a level playing field between banks and non-banks in their provision of cross-border payment services.

For example, Indonesia's framework is activity-based, applying the principle of same activity, same risk, same rule, and defining PSPs to include both banks and non-banks providing services to facilitate payment transactions to users. All PSPs are subject to licensing and minimum capital requirements. The Payment System supervision framework comprises a combination of on- and off-site supervision, based on a risk-based approach that is proportionate to the risk profile of the PSP and its systemic importance which will determine the application of supervisory focus.

Comparatively, the United States takes a mixed approach. Banking entities are generally supervised at the federal level by the Federal Reserve, the Financial Deposit Insurance Corporation (FDIC), National Credit Union Administration (NCUA), and the Office of the Comptroller of the Currency (OCC), (collectively referred to as the federal banking agencies or FBAs). The FBAs examine banks not only for safety and soundness, but also compliance with applicable laws and regulations, including AML/CFT and certain consumer protection requirements. Non-bank PSPs generally fall within the definition of money transmitters, which are a type of Money Services Business (MSB) and are subject to licencing and other requirements in the states in which they operate and supervisory oversight by state authorities. However, all banks and many non-bank PSPs are subject at the national level to the provisions of the Bank Secrecy Act (BSA) and its implementing regulations that require financial institutions to establish AML/CFT compliance programs, file certain reports, and keep certain records of transactions.

Annex 2 (Survey of domestic regulatory and supervisory frameworks) provides more detail and additional examples from a few jurisdictions to highlight these different approaches.

1.3. Impacts of regulatory and supervisory inconsistencies

Inconsistencies in regulatory frameworks can create significant challenges for both banks and non-banks in their provision of cross-border payment services. Such inconsistencies could increase the risk of regulatory arbitrage which may, in turn, reduce regime effectiveness and

create opportunities for fraud, money laundering, terrorist financing, and other illicit financial activities. Inconsistencies could also increase the cost and complexity of compliance programs and operations leading to delays in payment processing times.

As institutions that hold end users' deposits from the public, extend credit, and facilitate large-scale payments, often filling multiple roles in the payment chain, banks are generally subject to stricter regulation than non-banks. In contrast, non-banks, which may engage in selected activities but do not cover the full spectrum of banking activities, typically operate under lighter regulatory regimes and supervisory scrutiny. However, banks remain accountable for their own compliance with regulatory requirements regardless of whether the banks are providing services to non-bank PSPs (e.g. use of correspondent accounts) or partners (e.g. white labelling, outsourcing service provider). This may result in increases to large banks' compliance costs and could be perceived by banks as an excessive regulatory accountability that limits their ability to innovate in the cross-border payments space.

Notwithstanding that non-bank PSPs offer many of the services that banks provide, particularly with respect to front-end services, they continue to rely to a large degree on banking channels to conduct their activities, including to segregate and safeguard client funds. Risk management considerations may lead banks to decline or stop providing banking services to non-bank PSPs, including by refusing to provide payment accounts, which may result in adverse consequences for those non-bank PSPs.

In most jurisdictions, non-banks PSPs rely directly on participating banks for indirect payment system access causing them to establish and maintain banking relationships that may be subject to regulation, supervision and oversight unrelated to the specific payment activities conducted by the non-bank PSP customer. Whenever non-bank PSPs maintain banking relationships they may be prompted by their banking services provider to meet bank regulatory requirements that may improve risk mitigation, but at the same time this may increase compliance costs or reduce transaction processing speeds, potentially affecting two of the G20 Roadmap's four challenges. Some non-bank PSPs may choose to not directly access payments infrastructures in jurisdictions where they are able to do so, because of the investment costs needed to meet regulatory, technical, and operational requirements or other reasons.

Inconsistency or uncertainty regarding the regulatory and supervisory frameworks applicable to non-bank PSPs in some jurisdictions may raise concerns about whether all risks posed by their business models are addressed sufficiently in these relationships to satisfy requirements under bank regulatory and supervisory regimes.

2. Cross-Border payment frictions and risks

The CPMI and the FSB identified seven frictions that contribute to the four challenges that the Roadmap seeks to address.[35] This report focuses primarily on the friction related to the

[35] FSB (2020), *Enhancing Cross-border Payments – Stage 1 report to the G20*, April, and CPMI (2020), *Enhancing cross-border payments: building blocks of a global roadmap. Stage 2 report to the G20 – technical background report*, July. The identified frictions are the following: Legacy technology platforms that rely on batch processing that is characterised by low data process capability and a lack of real-time monitoring; Long payment chains that result in costly development of connections needed to

complexities of meeting compliance requirements, including those designed to counter financial crime, fraud, and operational risks, such as cybersecurity, and strengthen resilience. It is important to note that the frictions do not operate in isolation. For example, long payment chains may involve increased numbers of intermediaries that could affect exposure for PSPs, including potentially increasing financial crime risks. A level playing field resulting from increased alignment of bank and non-bank regulation, supervision and oversight may reduce barriers to entry for intermediaries, facilitating stronger competition. Similarly, fragmented or truncated data formats could exacerbate legacy platform issues or have adverse implications for effective activity monitoring and screening for economic sanctions compliance. These and other issues are being addressed under the comprehensive set of priority actions under the G20 Roadmap.[36]

2.1. Interdependencies with other G20 Roadmap workstreams addressing compliance-related frictions

This report is part of the work under the G20 Roadmap priority theme that focuses on establishing and maintaining a legal, regulatory, and supervisory environment for cross-border payments. This theme promotes the safety, efficiency, and integrity of cross-border payments and recognises the limitations that inconsistent or unaligned legal, regulatory, and supervisory frameworks can place on achieving this objective. The other two action items under this priority theme are priority action 5 on enhancing information to end-users and priority action 6 on updating the application of AML/CFT rules.[37]

Under priority action 5, the FSB has engaged with various SSBs and international organisations to evaluate ways in which transparency in cross-border payments could be effectively incorporated into standards, frameworks, or guidance covering consumer protection, payments, or both. For example, the FSB worked with the G20/Organisation for Economic Co-operation and Development (OECD)Task Force on Financial Consumer Protection to introduce specific references to cross-border payments into the G20/OECD High-Level Principles on Financial Consumer Protection.[38]

Priority action 6 is led by the FATF and focuses on harmonising the application of AML/CFT international standards. Complexity resulting from the divergence in how these standards, such as those related to customer identification and verification, are implemented across jurisdictions can increase costs and reduce speed.[39] Progress on this action includes FATF adopting revised standards and guidance on beneficial ownership of legal persons; strengthening its Mutual Evaluation Programme; holding a Private Sector Consultative Forum to continue to develop awareness of emerging technologies, information sharing and data privacy and protection in relation to AML/CFT compliance; ongoing work on harmonising the application of Recommendation 16 to improve payment transparency and incorporate ISO 20022 messaging

transmit cross-border payments in multiple currencies; Funding costs resulting from pre-funding needs to access foreign currency markets or settle multi-currency transactions; Weak competition due to barriers to entry for intermediaries; Limited operating hours that cause delays especially in payment corridors that are subject to differences in time zones; Fragmented and truncated data formats that lower the rate of straight through processing and automated reconciliation; and Complex processing of compliance checks focused on the complexities of meeting compliance requirements including those related to AML/CFT.

[36] *Ibid.*

[37] FSB (2024) *G20 Roadmap for Enhancing Cross-border Payments: Consolidated progress report for 2024*, October.

[38] OECD (2022), *G20/OECD High-Level Principles on Financial Consumer Protection*, December.

[39] FATF (2021), *Cross Border Payments. Survey Results on Implementation of the FATF Standards*, October.

standards; and conducting potential follow on activities such as developing guidance on payments transparency to promote consistent implementation of the revised FATF standards across the global FATF network.

In addition, priority action 7 on enhancing the interaction between data frameworks and cross-border payments is closely related to this report. Lack of standardisation with respect to data formats, data elements, and information sharing, including due to data protection and privacy concerns, and different supervisory approaches to monitoring PSPs adversely affect sending and receiving customer and transaction information. To further work on this priority action, the FSB has developed recommendations for promoting alignment and interoperability across data frameworks applicable to cross-border payments, including data privacy, operational resilience, AML/CFT compliance, and regulatory and supervisory cooperation and data sharing.[40]

This report recognises that actual or perceived differences in the scope and application of regulatory and supervisory regimes applied to banks and non-banks can contribute to the complex processing of compliance checks that in turn results in higher costs and lower speeds. Reducing such actual or perceived differences could, for example, support non-banks' access to payment systems. Additionally, effective implementation of the FATF Standards, including those relating to CDD, correspondent banking, money or value transfer services, new technologies, wire transfers, and information sharing, among others, across jurisdictions will also help reduce challenges in providing cross-border payment services.

2.2. Risks associated with cross-border payments services

In addition to the identified frictions that contribute to the four challenges that the G20 Roadmap seeks to address this report also considers certain other risks associated with the provision of cross-border payment services. While these risks are not the primary focus of the report, PSP exposure to them is linked to regulatory and supervisory regimes that govern both bank and non-bank PSPs. For example, weak or non-compliance with AML/CFT requirements or inadequate and inconsistent regulation, supervision and oversight of PSPs could potentially increase a PSP's exposure to financial crimes. Similarly, a failure to protect consumers from unfair practices or ensure the operational resilience of offered services may adversely impact public policy goals, such as increasing transparency and access to cross-border services or maintaining payment services' safety and efficiency. In addition, the introduction of other intermediaries such as agents and third-party providers of new and innovative payment products associated with a PSP may not be subject to the same regulation or security standards.

Inconsistencies in legal, regulatory, and supervisory frameworks between and within jurisdictions can provide further opportunities to engage in regulatory arbitrage, undermining the frameworks intended to mitigate different risks, and thereby potentially increasing systemic risk and weakening market integrity. Supervisory gaps and differences in regulation may be exploited to circumvent stricter regulations and exacerbate risks related to cross-border payment services, such as consumer harm and operational and financial crime risks.

---

[40] FSB (2024), *Recommendations to Promote Alignment and Interoperability Across Data Frameworks Related to Cross-Border Payments*, December.

Consumer protection

Existing and emerging technologies have increased consumer access to payment services that may be cheaper, more convenient, faster, and more accessible to segments of the population that have traditionally confronted obstacles to access. PSPs offering fast payment services increasingly allow consumers to conduct transactions via a variety of domestic and international channels. However, there are risks that may accompany these benefits. Consumers may be generally unfamiliar with the products they are using and the related distribution technologies. They could also be exposed to a higher prevalence or new types of fraud or unauthorised payments. Measures such as effective disclosure, due-diligence relating to customer on-boarding and enrolment, increased customer communication and education, and the application of technologies that facilitate secure transaction authorisation and adequately protect consumer data and privacy could help address unauthorised access to or the use of personal data, data breaches, and other incidents that could result in considerable consumer harm.

Operational-related risks

Operational risk is generally considered to include risks to financial condition and resilience arising from inadequate or failed processes or systems, human errors or misconduct, or adverse external events.[41] Operational risk is inherent in all payment products and activities and risk concentrations can accumulate within and across products, business lines, geographies, legal entities, and third-party providers. Fraud can be considered a form of operational risk that can exist in any part of the payment process (e.g. customer on-boarding, enrolment authentication tools and/or software, distribution of payment instruments, transaction authorisation, processing) that may lead to unauthorised transactions and/or transactions resulting from the manipulation of the payer. Emerging technologies, increased use and availability of alternative payment methods and products, and cyber threats are some of the factors contributing to operational risk exposure. For example, in the case of faster payments, the irrevocability of such payments emphasises the importance of strong customer authentication, fraud protection, and the proper identification of payees.

Financial crimes (money laundering, terrorism financing and other illicit financial crimes)

There are two levels at which inherent financial crime risk is present in the PSPs sector: risks associated with payment service characteristics (activity-based risk) and risks associated with the characteristics of the PSPs that offer those services (entity-based risk). In general, payment transactions are conducted in large volumes and at high speeds and the underlying technologies that support payment product and service offerings may also reduce the level of transparency associated with those transactions thus potentially increasing financial crime risk exposure. Although the business model may be changing, non-bank PSPs are more likely to engage in "occasional transactions" rather than transactions originating from established customer relationships that are subject to AML/CFT controls. In some cases, the use of agent networks, in the absence of appropriate supervision or oversight, can increase financial crime risk exposure in cross-border situations. Previous analyses by the FSB and the World Bank have highlighted

---

[41] BCBS (2021), *Revisions to the principles for the sound management of operational risk*, March.

the challenges facing non-bank PSPs, particularly those that process remittance payments, in certain jurisdictions that may be designated as higher risk: variations in practices, characteristics, and levels of supervision of non-bank PSPs may result in decisions by other financial institutions to reduce their exposure to non-bank PSPs.[42] These analyses also indicate that consistent supervision of these non-bank PSPs could counteract such decisions. The FSB's 2018 report included 19 recommendations in four main areas that, if implemented, might contribute to greater access by remittance service providers (RSPs) to banking services.

Box 2: Financial crime risks associated with payment institutions

In June 2023, the European Banking Authority published a report on financial crime risks associated with payment institutions.[43] Among its findings, the report noted that AML/CFT supervisors across Europe considered payment institutions as a sector to represent inherent financial crime risks and that controls put in place to mitigate these risks were not always effective. It also noted that not all AML/CFT supervisors based the intensity and frequency of on-site and off-site supervision on a payment institution's ML/TF risk profile. As a result, payment institutions with weak AML/CFT compliance programs could potentially take advantage of such inconsistencies to establish themselves in jurisdictions where the authorisation process is perceived to be less stringent and then engage in cross-border payment activities from that base of operation. The report also noted that there was no common EU-level approach to the AML/CFT supervision of agent networks or of PSPs' use of agents. Such use may present significant inherent risks, especially in the cross-border context.

The FATF Standards require jurisdictions to ensure that their financial institutions conduct CDD on their customers, as well as ongoing transaction and suspicious activity monitoring. They also require jurisdictions to take measures to ensure that natural or legal persons that provide payment services are licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations. Thus, while a jurisdiction's regulatory requirements for CDD and suspicious activity monitoring generally will apply to both banks and non-bank PSPs, the supervisory approaches for enforcing such compliance often vary, especially if the AML/CFT and prudential supervisors are different or if the jurisdiction does not require licensing of all non-banks PSPs. Since most non-bank PSPs currently access domestic payments systems through banking relationships, a bank's exposure to financial crime risk may be increased in those circumstances where the transactions it is processing on behalf of its non-bank PSP customer do not originate from established account relationships that are subject to effective CDD or AML/CFT controls are not otherwise effective. Supervisors in turn may view those increased risks as not sufficiently mitigated by controls established under the processing bank's AML/CFT compliance programs.[44]

There are also geographic risks associated with cross-border payment services that affect both bank and non-bank PSPs. The geographies where PSPs are located or do business may be considered higher financial crime risk, and this may be especially the case for non-bank PSPs that provide financial services in locations where banks are unlikely to have a presence or do

[42] FSB (2018), *Stocktake of remittance service providers' access to banking services*, March and FSB (2019) *Remittance Service Providers' Access to Banking Services: Monitoring of the FSB's Recommendations*, May.

[43] European Banking Authority (2023), *EBA Report on ML/TF Risks Associated with Payment Institutions* June (EBA/REP/2023/18).

[44] Ensuring effective CDD and transaction monitoring is made more challenging when PSPs issue virtual account numbers, such as virtual IBANs. This issue is discussed in a recent report from the EBA, (2024) *Report on virtual IBANs*, May.

business. Such payment services may be critical to EMDEs in conducting trade and other commercial activities and supporting the flow of remittances and humanitarian assistance.

The types of products and services offered by both bank and non-bank PSPs are often based on new and emerging technologies for which potential financial crime risks have either not been sufficiently identified or appropriately addressed. Identifying and addressing financial crime as part of the product design process, identification of potential delivery channels and arrangements, introduction of new technologies for pre-existing products and similar activities can reduce potential risk exposure on roll-out.

Other risks associated with bank and non-bank PSPs' involvement in the payment chain

Changes in technology are not the only drivers of change in national payment landscapes. Business arrangements could also affect regulation and produce accompanying changes in supervisory strategies. Increases in partnerships between banks and non-bank PSPs to provide services can potentially change risk profiles and shift supervisory focus to third-party oversight to ensure effective risk management and compliance, including compliance with AML/CFT requirements, and cyber and operational risk management (see Box 3 for an example). Furthermore, for larger PSPs, expansion into new services and products may change their mix of product types that may require regulatory changes and corresponding supervisory strategy adjustments.

Similarly, an expansion of large mixed-activity groups (e.g. BigTech firms, telecom providers) into payment services, may lead to intragroup interdependencies, where the supervisory approach would need to consider group-wide interdependencies that may lead to new requirements on governance, conduct of business, operational resilience and, where appropriate, financial soundness.[45]

Not all PSPs present the same level of risks, so it is important to understand the risks associated with each PSP, considering its customer base, the markets within which it operates and the types of payment products and services that it offers, as well as its business model, and adjusting supervisory approaches as appropriate. Perceptions about both a non-bank PSP's risk profile and the rigor of its supervision or oversight can affect its ability to access and maintain necessary banking and payment services.[46] The examples of current regimes in Annex 2 indicate that in some jurisdictions, bank and non-bank PSPs are subject to similar regulatory and supervisory regimes based on the services they offer, and proportionality as a principle is, in many cases, already applied in the supervision of both PSP types. Proportionality is also integrated into the BCBS Core Principles for banks and the FATF Standards that require countries to assess risks and apply a risk-based approach, noting that where countries identify higher risks, they should

---

[45] Ehrentraud, J, J L Evans, A Monteil and F Restoy (2022), Big tech regulation: in search of a new framework, *FSI Occasional Paper*, no 20, October.

[46] For example, the World Bank's 2015 *Report on the G20 survey on de-rising activities in the remittance market* found that only 48% of banks that responded to the survey agreed with the statement that "Banks can rely on adequate supervision of to inform their risk-based decisions on opening/maintaining accounts for [non-bank remittance service providers] customers." This compares with 84% of the responses from government respondents. In total, 13 governments and 25 banks completed the survey.

ensure that the regimes related to financial stability, operational resilience, and AML/CFT adequately address such risks.

Finally, in the cross-border context, other risks for PSPs could also, for example, include currency exchange risks, credit risks (e.g. cards, buy-now-pay-later, fraud, counterparty risk), liquidity risks (e.g. operational incidents, delayed payments), money settlement risk, general business and business model risks, governance risk, and reputational, compliance and legal risks (e.g. complexity of dealing with various legal frameworks).

Box 3: Banking/Licensing-as-a-Service (BAAS)

BAAS is a growing form of third-party arrangements in which banks or other licensed financial service providers provide licensed activities (e.g. banking, payments or investment services) via non-bank intermediaries[47] that act, depending on the regulatory regime, as agents or outsourcing partners.[48] Such cooperation can potentially be beneficial for the BAAS provider as it may offer an opportunity to access new sales channels, payment systems, card networks, and customers, and may increase efficiency and access to innovative solutions. It may also foster competition in the market. However, such intermediation can also introduce risks. Like third-party outsourcing, BAAS introduces dependencies between banks, other licensed financial service providers and other firms, although the nature of these dependencies and the risks they create are different. In the context of payments, some of the most prominent risks include conduct risks, information security risks, liquidity risks, operational risk (including cyber risks), legal risks, business model risks, interconnection risks, reputational risks, resolvability risks, agency problems, and adverse selection. For example, there have been incidents where intermediaries have comingled or defrauded funds or failed to comply with know your customer or third-party risk management obligations. In classic BAAS partnerships (e.g. co-branded credit card issuance) the BAAS provider would be legally liable for providing the services as well as responsible for performing all important technical front- and back-office services. However, new non-bank intermediary relationships have emerged where the non-bank intermediary runs the front-office, typically via an application programming interface (API) and may be the main counterparty for the payment service user, while the PSP/BAAS provider may only responsible for conducting back-office-related process and regulatory compliance. Some non-bank intermediaries have established BAAS relationships with multiple licensed payment service providers and other financial service providers. In complex cases, the total set of services offered by the non-bank intermediary may replicate the economic functions of a bank, providing access to deposit services, payments, trading, credit and in some cases even crypto asset custody services, or insurance as a broker.

As a result, in more complex cases, the licensed provider for the individual service may no longer have the full picture and control over the interdependencies emerging from various services provided in the non-bank intermediaries application that links up services from various financial service providers. Once the non-bank intermediary's/distributor platform expands, their PSPs may become dependent on the non-bank intermediary, resulting in concentration risks. Thus, existing third-party risk-management requirements and agent registration may not address complex BAAS models in the absence of and more detailed supervisory guidance, cooperation among competent authorities and consideration of additional licensing or registration in particularly complex cases.

[47] The intermediary may also be a regulated institution which does not hold authorisation for a specific service (e.g. deposit taking).

[48] BCBS (2024), *Digitalisation of finance*, page 15, May.

3. Principles for developing recommendations

The principles described below were developed based on analysis of the identified frictions related to differences in the application of regulatory risk management requirements, focused on financial crime risks as well as operational risks (e.g. fraud, cyber) and resilience described earlier in this report. These principles define the areas and establish a framework for the development of the recommendations in section 4. The principles and the recommendations that follow are intended to be high-level and recognise that national regulatory and supervisory frameworks are influenced by a range of considerations.

Cross-border payment supervisory and regulatory regimes should be designed to promote safe, resilient, and efficient payment services. Safe and efficient payments are essential for a well-functioning economy. It is thus important that regulatory and supervisory requirements consider the entire payment chain and the role of all actors involved and clarify the respective responsibilities and expectations in a transparent and consistent manner. The recommendations should be made and implemented in ways that do not jeopardize the robust entity-level regulation, supervision and oversight to which internationally active banks are subject.

The supervisory and regulatory regimes applicable to cross-border payment activities should be proportionate to the risks that they present. Proportionality refers to the principle that the level of regulatory requirements and scrutiny should be commensurate with the risks associated with a particular activity or entity and thus avoid imposing unnecessary regulatory or supervisory burden on banks or non-banks. Applying proportionality in the context of cross-border payments ensures that measures are tailored to the specific characteristics and risks presented by participants and transactions. It can be applied to specific groups of supervised entities or segments within those groups based on business models, permitted activities, complexity, risk profile, and other considerations.[49] It is important for authorities to consider the impact of regulation, supervision and oversight, if any, on the wider payment ecosystem, including domestic payments.

Proportionality could warrant greater consistency in the treatment of similar payment services across PSPs, for example, in the consistent application of regulatory requirements and resulting supervisory measures to bank and non-bank PSPs in cases where they are providing similar or the same payment services with similar or equal risks. Applying this principle would support an environment that promotes fair competition and innovation by establishing a level playing field to the extent possible, given differences in business model and risk profile, for both banks and non-bank PSPs in the provision of cross-border payments, and would reduce opportunities and incentives for engaging in regulatory arbitrage.

Proportionality is an already widely practised approach for exercising regulation, supervision and oversight. For banks, the concept of proportionality ensures that applicable rules and supervisory practices are consistent with banks' systemic importance and risk profiles, as well as appropriate for the broader characteristics of a particular financial system. Furthermore, proportionality can support the achievement of other national policy goals that may vary across jurisdiction, such as promoting financial inclusion or facilitating access to payment systems for non-bank PSPs.

---

[49] World Bank and BCBS (2021) *Proportionality in bank regulation and supervision – a joint global survey*, July.

The supervisory and regulatory regimes for PSPs should respond to changes in national and international payment services landscapes. This principle acknowledges that as PSPs expand their business into foreign markets and merge with, acquire, or are acquired by other types of entities, changes to national regulatory and supervisory regimes may be required to adapt quickly to address risks which were previously not accounted for and accommodate changing services and activities. Payment services may also change based on new technologies. Therefore, alignment of regulation, supervision and oversight should take a technology neutral approach.

The supervisory and regulatory regimes for PSPs should be clearly articulated. Clear articulation of regulations and supervisory expectations that includes avenues for industry consultation on proposed regulatory changes and resulting supervisory processes for cross-border payments is essential to foster trust among stakeholders and to promote fair competition.

The regulatory and supervisory regimes for cross-border payments should facilitate cooperation, coordination, and information sharing within and across jurisdictions. Regular dialogue and collaboration between and among relevant regulatory and supervisory authorities, as well as with and between private sector entities, are important for identifying, understanding, and addressing the risks and challenges in the fast-changing and complex cross-border payment ecosystem. Fostering consistency and other improvements for cross-border payments requires, to the extent possible, sharing information across jurisdictions to enable a system-wide perspective.

4. Recommendations for improving alignment of PSP regulatory and supervisory regimes

These recommendations are focused primarily on addressing the identified Roadmap frictions that result from the complexities in meeting compliance requirements, including those related to AML/CFT. Such consideration included the application of activity- or entity-based regulation and the principle of "same activity, same risk, same rule," as well as moving toward the ideal outcome of establishing a level playing field between bank and non-bank PSPs in their provision of cross-border payment services that pose similar risks. The recommendations should be implemented in ways that do not jeopardise jurisdiction-specific policy goals, such as the robust entity-level regulation, supervision and oversight to which internationally active banks are subject. To avoid duplication, additional consideration was given to the work underway in other FSB workstreams, including the efforts of other workstreams described in section 2 and the ongoing work to revise relevant FATF Standards and to ensure the effective implementation of these standards. The resulting recommendations apply to all relevant competent authorities and to standard setting bodies, consistent with their respective mandates.[50]

Recommendation 1: Competent authorities should conduct risk assessments of the cross-border payments sector, the aim of which should be to identify, understand and assess the risks associated with PSPs active within the authorities' jurisdiction in cross-border payment services.

[50] According to Action 4(b) in 2025 standard setting bodies should adapt their regulatory, supervisory and oversight standards or guidance, as needed, in line with the FSB recommendations.

Moving towards the objective of a level-playing field between bank and non-bank PSPs that reflects the principle of "same activity, same risk, same rule", while considering the differences in risk profiles, requires a comprehensive and sophisticated understanding of PSPs' activities and their risks as well as of potential mitigants to ensure the safety and efficiency of cross-border payment services. The nature and level of risks associated with a PSP providing one type of service may differ from that of PSPs offering a combination of services (i.e. payments, payment accounts, non-bank lending, other financial and non-financial services, or a combination of activities from different sectors such as payments and data-related services), or a group of entities or platforms linking services of several financial institutions. Such combinations may introduce a range of complexities, additional risks (e.g. concentration risk, contagion risk) that should be assessed to ensure effective risk management. Additional requirements and supervisory approaches may be warranted to assess risks holistically and require coordination of supervisory and oversight activities and prudential consolidation for groups with significant financial activities, in addition to addressing the risks of each activity or group entity in isolation.[51]

Risk assessments should be tailored to the specific risks or categories of risk present in the sector and comprise, among other things, PSPs' business models, operational resilience, the types of services (including ancillary services) and products that they offer and their target customers and market segments as well as dependencies from and interdependencies with third parties and the potential impact of such activities on the safety and efficiency of the payment services provided. The analysis should consider the entire payment flow including implications for domestic payment legs, the risks of the payment instruments, nature of transaction (e.g. individual or bundled),[52] the payment activities and channels (e.g. ATM, point of sale terminal, internet, or distance communication), platforms and underlying technologies, and agents and other intermediaries. For example, partnerships between bank and non-bank PSPs or unlicensed entities, or PSPs' engagement in non-bank lending may present new risk challenges. The analysis should also consider how ease of access by non-bank PSPs to payment accounts at banks and the availability of foreign exchange services for non-bank PSPs may impact risks.

Assessments should consider both inherent risks and residual risks after applying mitigating actions. Assessments should be supported by timely and relevant data, and competent authorities should review their programmes for collecting relevant data to effectively monitor, understand, assess, and mitigate risks. Moreover, competent authorities are encouraged to engage continuously with market participants and industry stakeholders to stay abreast of market developments and emerging risks.

To ensure that payment sector risk assessments are sufficiently responsive, they should be periodically reviewed and updated to reflect market developments.

Recommendation 2: Based on the findings of the payment sector risk assessments, competent authorities should review existing regulatory, supervisory, and oversight regimes to ensure that the regimes: 1) address all the key risks identified; 2) are proportional to the risks identified, with particular

[51] EBA (2022), *Joint European Supervisory Authority response to the European Commission's February 2021 Call for Advice on digital finance and related issues: regulation and supervision of more fragmented or non-integrated value chains, platforms and bundling of various financial services, and risks of groups combining different activities*, January. Recommendation 7: Ensure the sufficient coverage of mixed activity groups (MAGs) by sectoral prudential consolidation/group structured supervision rules.

[52] Bundled payments is also part of the discussion within FATF.

attention to operational risks (e.g. fraud, cyber and third-party risks), resilience and financial crime risks, and 3) are applied consistently and in coordination with all relevant competent authorities across the sector. Competent authorities should consider undertaking or seeking adjustments to laws, regulations, and supervision and oversight models as needed.

Competent authorities should use the findings from their payment sector risk assessments to review and ensure that their regulatory, supervision, and oversight regimes address all the key risks identified, particularly those related to cross-border payment activities, and that those regimes are proportional to the risks and are consistently applied.

These reviews should include operational risks related to payment services. Considerations could include whether PSP regulatory, supervisory, and oversight regimes sufficiently support the establishment of safe and efficient processes for customer onboarding, authentication, communication, and data security; tracing of payment transaction processing; management of other operational risks (e.g. cyber, business continuity, fraud, third-party risk) and reporting operational and security incidents in a standardised manner to the authorities.

General issues that should be considered include the appropriate use of activity- or entity-based regulation; consistency of application both within the jurisdiction and internationally and effective supervision and oversight of PSPs, agents, and other intermediaries, whether through supervision or other means of reviewing and ensuring compliance. This may include, for example, considerations of increased information sharing and cooperation between and among competent authorities; consideration of whether to introduce more rigorous or comprehensive regulatory, supervisory, and oversight approaches, such as requirements on organisational group structures for non-banks with significant financial activities or consideration of potentially enhanced risk management requirements in areas such as operational resilience or recovery planning for non-financial groups expanding into cross-border payment activities.[53]

In jurisdictions that have multiple relevant competent authorities, those authorities should jointly consider ways to better promote proportionality and consistency within the jurisdiction, which could include, for example, coordinating the reviews of their relevant regulatory and supervisory regimes, subject to applicable legal constraints,[54] as well as harmonising reporting requirements and templates where possible.

In considering proportionality, competent authorities should keep in mind the importance of maintaining a balance between the jurisdiction's priority public policy goals and preserving the integrity of the financial system and the PSPs and other financial institutions that operate within it. Such public policy goals often include, among others, the safety and efficiency of the payment system, financial inclusion, supporting sound competition, and protecting national security, including through the application of economic sanctions.

In conducting their reviews, competent authorities should also consider relevant existing international standards and guidance such as the FATF Standards, which apply to both banks and non-bank PSPs, and the BCBS standards with respect to bank supervision. As the regimes applied to banks and non-bank PSPs move towards greater alignment, regulatory changes with

[53] FSI Occasional Paper No.20 (2022).

[54] This does not necessarily entail competent authorities issuing joint regulations or guidance.

accompanying adjustments to supervisory and oversight strategies and models may be necessary. This is especially likely for risk areas associated with non-bank PSPs that are not currently addressed under existing international frameworks and may not be subject to consistent supervision. However, care should be taken in this process to avoid placing unnecessary regulatory or supervisory burden on PSPs by rigorously applying the principles of proportionality and consistency in the context of a risk-based approach.

In considering consistency, a key decision for competent authorities is the appropriate implementation of activity- or entity-based regulation, supervision and oversight. In many cases, a combination of the two approaches may be needed to achieve outcomes that are consistent, proportionate and effective. Competent authorities should have a framework to guide this decision.[55] Relatedly, supervision and oversight regimes with respect to cross-border payment services should be tailored to whether the regulatory requirements are activity- or entity-based or support the application of a hybrid approach.

Recommendation 3: Competent authorities' regulatory and supervisory regimes related to cross-border payments should be designed to promote consumer protection and address consumer harms.

According to the G20/OECD High-Level Principles on Financial Consumer Protection,[56] "the integration of financial consumer protection policies into regulatory and supervisory frameworks contributes to strengthening financial stability, addresses information asymmetries and ensures that consumers are treated fairly and adequately protected from harms."[57] Competent authorities should adopt and implement regulatory and supervisory regimes with adequate consumer protection requirements, including measures to detect and prevent payment fraud. Those consumer protections should include ensuring transparency with respect to payment service delivery and pricing of services, e.g. foreign exchange margins, as well as timely error and dispute resolution procedures to prevent or address consumer harm. Consumer protections should be aligned across the PSP sector, whether the jurisdiction places consumer protection issues under the scope of prudential supervisors, conduct authorities or as a shared responsibility between prudential and conduct authorities. In reviewing their supervisory frameworks, competent authorities should consider the G20/OECD High-Level Principles on Financial Consumer Protection and the targets of the G20 Roadmap.

Recommendation 4: Competent authorities should develop, publish, and communicate payments-related supervisory and oversight expectations to promote safe and efficient payment services, including the guidance relating to application of the risk-based approach.

Promoting transparency through the publication of supervisory and oversight expectations supports achieving a level-playing field in at least two important ways. First, it fosters consistent

---

[55] For example, the FSI suggests that activity-based regulation is appropriate when 1) the risks presented by a particular activity could be significant in the context of the overall national financial system even though failure to manage such risks may not necessarily affect the overall safety and soundness of the entity conducting the activity and 2) the activity can be addressed directly and in isolation. While regulation focuses on establishing rules either for specific activities based on the risks they present or for entities that offer a combination of services based on combined or overall risk, supervision and oversight focus on the application and enforcement of those rules. See FSI (2022), *Occasional Paper No. 19*, August. Another helpful discussion of activity-and-entity-based regulatory approaches is, IMF (2022), *BigTech in Financial Services: Regulatory Approaches and Architecture*, January.

[56] *Ibid.*

[57] *Ibid.*

awareness and understanding among PSPs that enhances their ability to meet those expectations and promotes compliance with legal and regulatory requirements. Second, it can help to improve the consistency and understanding of supervision and oversight, including those applied to non-bank PSPs. Strengthening the consistency of requirements applicable to, and the practices of, non-bank PSPs, as well as the clear communication of such consistency, may reduce instances where banks are unwilling to provide services to non-bank PSPs and could also improve the reliability, security and efficiency of cross-border payment services. Publishing and maintaining updated lists of licensed or registered non-bank PSPs by competent authorities, consistent with domestic law or regulation, could contribute to increased transparency, consumer protection and fraud prevention, while promoting trust and stability in the global financial system.

Where relevant, supervisory and oversight expectations may differentiate between domestic and cross-border payments, given potential differences in related risk exposure (i.e. fraud, non-compliance with economic sanctions, or financial crime risks might be higher for cross-border transactions). In developing guidance, competent authorities should consider and establish appropriate approaches for consulting with PSPs and other stakeholders and incorporating relevant feedback. Moreover, competent authorities should consider providing dedicated assistance (e.g. seminars, focus group discussions, workshops) for PSPs to achieve compliance as new rules or supervisory expectations are introduced or new PSPs are established. Supervisors are also encouraged to share their supervisory practices and insights with other jurisdictions or international organisations.

Recommendation 5: Competent authorities should: 1) review licensing or registration criteria for risk-proportionate requirements, including measures to promote consumer protection and address new services such as account information services, payment initiation services, digital wallets, and the provision of services through agents and other intermediaries; and, if necessary, 2) adjust the licensing or registration processes for PSPs to incorporate requirements such as conducting fit and proper tests, reviews of AML/CFT compliance programs and oversight of agents and other intermediaries.

Improving consistency with respect to licensing or registration across the PSP sector is a key step in successfully aligning bank and non-bank PSP regulatory and supervisory regimes, because many licences or charters issued to PSPs, or registration requirements, identify specific activities or combination of activities that they can offer and may also establish the supervisory and oversight regime that should be applied. Currently, authorisation processes can vary across jurisdictions. Licences can be issued in most jurisdictions for specific services based on activity- or entity-based rules, or a hybrid approach that combines activity-based and entity-based regulation. Applying the activity-based principle of same activity, same risk, same rule may not exclude additional entity-based regulation. In most jurisdictions, banks are required to be licensed or chartered and, with respect to AML/CFT compliance, the FATF Standards allow jurisdictions the flexibility of either registering or licensing PSPs. The focus of the licensing or registration process depends on the determination of whether to apply either or both activity- or entity-based regulation for ensuring effective outcomes. While maintaining neutrality, competent authorities could consider the continuation of benefits such as expanded access or improved technology offered by non-bank PSPs by establishing, maintaining, and enabling regulatory and supervisory frameworks that seek to appropriately balance these benefits with the potential risks associated with products and services offered by non-bank PSPs, differentiating between a

business' inherent and residual risks. Moreover, authorities should also consider a consistent approach across the payment sector for the registration and oversight of non-bank PSP agents.

Recommendation 6: Competent authorities both within and across jurisdictions should, where applicable, implement or expand cooperative arrangements for information sharing to support access to relevant information and data for comprehensively assessing risks as well as the sources of frictions and, when appropriate, supporting regulatory or supervisory action.

The cross-border payments ecosystem is multifaceted and complex. Fully understanding the nature, scope, and magnitude of relevant risks typically requires information from across the payments chain, from all relevant authorities within a jurisdiction, and from multiple jurisdictions. This is particularly true in the context of enforcing effective AML/CFT and sanctions compliance.[58]

Competent national and international authorities should consider establishing suitable international channels to facilitate collaboration and coordination to support access to information for global PSPs that operate across multiple jurisdictions and, where applicable, implementing or expanding information sharing arrangements to support access to relevant information and data for comprehensively assessing risks and, when appropriate, supporting regulatory or supervisory action. Moreover, PSPs should be allowed as appropriate to share information among themselves for purposes such as preventing payment fraud, consistent with jurisdictional privacy laws.

For entities active in cross-border payments, or entities that belong to a group that is active in cross-border payments, relevant competent authorities within and across jurisdictions should consider establishing information sharing arrangements with each other, subject to applicable legal constraints.

Within jurisdictions, competent authorities should consider establishing an interagency task force that includes all authorities, including all AML/CFT supervisors, involved in the regulation, supervision and oversight of the PSP sector.[59] In addition to assisting in conducting, updating, and implementing risk assessments, the group may also support regular outreach to and communication with the PSPs to share information on topics such as on fraud patterns, consumer protection trends, financial crime typologies, and economic sanctions compliance practices that PSPs can incorporate into their risk management strategies.

In jurisdictions where non-bank PSPs are supervised by different competent authorities depending on location or licence-or-registration type, the task force could facilitate improved coordination of supervisory efforts. For example, it could serve as a forum for members to better understand each other's respective supervisory authorities, expectations and activities, as well as for developing strategies to identify inconsistencies to promote greater alignment.

---

[58] Supervisory cooperation, both domestic and international, is highlighted as a key requisite for an effective system. See FATF (2022), *Report on the State of Effectiveness and Compliance with the FATF Standards*, April, pp 22-25.

[59] BCBS (2020), *Sound management of risks related to money laundering and financing of terrorism*, January (revised July 2020). Annex 5 notes that "effective cooperation and exchange of information among prudential supervisors and AML/CFT supervisors that are responsible for banks (hereinafter "supervisors") are essential to address and mitigate ML/TF risk, to maintain the integrity of the banking system and ensure the prudential soundness and stability of banks."

At the international level, competent authorities should consider establishing groups similar to cooperative arrangements[60] or BCBS supervisory colleges to include PSP regulators and supervisors for the purposes of developing a common understanding of the risks associated with internationally active non-bank PSPs, promoting a shared agenda for addressing risks and vulnerabilities as well as frictions associated with cross-border payments, such as those resulting from differences in national economic sanctions regimes, and providing a platform for communicating key supervisory messages among members.[61]

To the greatest extent possible, cooperative arrangements among regulators should be transparent to PSPs, other financial institutions and third parties so they can understand the regulatory environment and meet their customers' expectations and regulatory obligations, as well as those of consumers in general.

---

60 Ibid. Responsibility E: Cooperation with other authorities, page 133.

61 BCBS (2014) *Principles for effective supervisory colleges*, June.

Annex 1: Survey of existing standards, recommendations, and guidance

This annex provides a brief overview of the existing standards, recommendations, and guidance relevant to cross-border payments developed by SSBs and international organisations such as the FSB. The following are key findings from the review that inform the proposed set of principles discussed in section 3 of the report and the proposed recommendations in section 4. The proposed recommendations in this report are intended to be complementary to this existing body of work.

Financial Stability Board (FSB)

In 2018, the FSB conducted a stocktake of RSPs' access to banking services.[62] The report identified a decline in the number of correspondent banking relationships impacting RSPs' ability to access banking services, which posed a major challenge to the provision of remittance services to certain regions of the world, and particularly to EMDEs, where remittance flows are a key source of funds for households.

The stocktake identified a variety of intertwined drivers for the termination of banking services to RSPs, including considerations of profitability, the perceived high financial crime risk associated with the remittance sector, the supervision of RSPs that ranged from active and effective to completely absent and, in some jurisdictions, weak compliance with international standards, particularly those relating to AML/CFT.

Overall, the report concluded that while the FATF Standards relevant to RSPs appeared sufficient, there also appeared to be a lack of understanding of some of their key tenets, such as the application of the RBA. To address the issues identified, the FSB report set out 19 recommendations in the following four areas:

- Dialogue and communication between the banking and remittance sectors.
- Application of the FATF Standards and oversight of the remittance sector focusing on areas such as, coordination and information sharing practices, and guidance on applying the RBA.
- The promotion and use of innovation in the remittance sector and its possible role in enabling RSPs greater access to banking services focusing on promoting new technologies to support customer identification, increasing end user access to transaction accounts and other activities.
- Technical assistance on remittance-related topics that included strengthening RSP regulation, supervision and and oversight conducting national risk assessments of the RSP sectors.

[62] FSB (2018), *Stocktake of remittance service providers' access to banking services*, March.

In 2019, the FSB published a report following up on progress made in implementing the recommendations contained in its 2018 report.[63] The report found that progress had been made against some of the recommendations, but that further work was needed. With respect to the actions undertaken, the report noted for example that some jurisdictions had adopted or implemented several good practices and procedures to improve their supervisory frameworks and enhance coordination.

At the same time, many jurisdictions still did not appear to have established robust supervision for RSPs and quite a few jurisdictions did not effectively supervise RSPs at all. Dialogue between RSPs, banks, and authorities responsible for supervision of the remittance sector was useful but had not resulted in tangible next steps. While innovation was a helpful solution to the challenges faced by RSPs, it was likely only part of a broader solution. The report also noted that significant amounts of technical assistance had been directed to the remittance sector, but there was a need for better coordination of this assistance and more focus on oversight of the remittance sector and the development of national risk assessments.

Standard-Setting Bodies (SSB)

Basel Committee on Banking Supervision (BCBS)

The BCBS is the primary global standard setter for the prudential regulation of banks and provides a forum for cooperation on banking supervisory matters. Its mandate is to strengthen the regulation, supervision and practices of banks worldwide with the purpose of enhancing financial stability. It establishes and promotes global standards for the regulation and supervision of banks as well as guidelines and sound practices on a wide range of topics relevant to its mandate.

The BCBS' Basel Framework is the full set of standards that cover governance, capital, liquidity, leverage, as well as risk management, supervision, and disclosure.[64] The Basel standards are expected to be implemented in full for internationally active banks in BCBS member jurisdictions. The BCBS also established the Core Principles for Effective Banking Supervision (Core Principles) that are the *de facto* minimum standard for sound prudential regulation and supervision of banks and banking systems.

In 2020, the BCBS updated its *Guidelines on the* s*ound management of risks related to money laundering and financing of terrorism*, intended to enhance the effectiveness of supervision of banks' AML/CFT risk management, consistent with and complementary to the goals and objectives of the standards issued by the FATF and principles and guidelines published by the Basel Committee.[65] While not limited to cross-border payments, these guidelines are applicable in the context of the provision of payment services. The role of bank supervisors in the context of cross-border payments broadly described below:

---

[63] FSB (2019), *Remittance service providers' access to banking services: Monitoring of the FSB's recommendations*, May.

[64] The Basel Framework is the full set of standards of the BCBS, which is the primary global standard setter for the prudential regulation of banks.

[65] BCBS (2020), *Guidelines on the sound management of risks related to money laundering and financing of terrorism*, July.

- Establishing effective cooperation mechanisms between prudential and AML/CFT supervisors to ensure that financial crime risks are adequately supervised in the domestic and cross-jurisdictional context for the benefit of the two functions.

- Ensuring full cooperation and assistance between home and host country supervisors in verifying a bank's compliance with the group-wide AML/CFT policies and procedures.

- Providing appropriate legal frameworks to facilitate the flow of information required for customer risk management from jurisdictions hosting foreign banks to head offices or parent banks and home country supervisors. Cooperation and exchange of information between prudential and AML/CFT supervisors should include coverage of the following:

  - bank authorisation processes (i.e. license applications, fit and proper assessments);

  - ongoing supervision, including assessment of governance, risk management, and internal control systems of a bank, business model and profitability drivers, operational risks, and compliance with AML requirements;

  - enforcement actions and/or revocation of banking licences.

Bank supervisors should also establish and maintain official channels to facilitate and structure ongoing dialogue, information exchange and cooperation between prudential and AML/CFT supervisors at the national and international levels (e.g. bilateral or multilateral exchanges, prudential or dedicated AML/CFT colleges).

Prudential and AML/CFT supervisors should:

- exchange information periodically and when necessary, as relevant for their respective tasks;

- consider whether and, if so, in which situations to cooperate (e.g. coordinated or joint inspections);

- consider taking measures to facilitate cooperation and information exchange with all relevant parties (e.g. memoranda of understandings (MOUs));

- include, to the extent legally possible, confidentiality and data protection provisions when putting in place mechanisms in relation to the exchange of information and cooperation among authorities.

Committee on Payments and Market Infrastructures (CPMI)

The CPMI promotes the safety and efficiency of payment, clearing, settlement, and related arrangements, thereby supporting financial stability and the wider economy. The CPMI monitors and analyses developments in these arrangements, both within and across jurisdictions. It also serves as a forum for central bank cooperation in related oversight, policy, and operational matters, including the provision of central bank services.

The CPMI is a global standard setter in this area. It aims to strengthen regulation, policy and practices regarding such arrangements worldwide. The CPMI and the IOSCO have issued the Principles for financial market infrastructures (PFMI) that are the international standards for financial market infrastructures, i.e. payment systems, central securities depositories, securities settlement systems, central counterparties, and trade repositories. They are part of a set of 12 key standards that the international community considers essential to strengthening and preserving financial stability.

Financial Action Task Force (FATF)

FATF is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF standards[66] set out a comprehensive and consistent framework of measures which countries should implement to combat these threats.

The FATF Recommendations apply to banks as well as non-banks. This includes Recommendation 14, which requires countries to take measures to ensure that natural or legal persons that provide MVTS are licensed or registered, and subject to effective systems for monitoring and ensuring compliance with the FATF Recommendations. Additionally, Recommendation 16 requires countries to ensure that financial institutions include required and accurate originator information and required beneficiary information on wire transfers and related messages and that the information remains with the wire transfer or related message throughout the payment chain. FATF is currently considering revisions of Recommendation 16 to reflect changes in the cross-border payments ecosystem. Proposed revisions under consideration include, among others, modifying the required originator and beneficiary information in cross-border transactions; narrowing the current exemption for credit, debit, or prepaid cards and requiring beneficiary financial institutions to check that the beneficiary information in cross-border payment messages aligns with what they have on file.

As the FATF Recommendations are high level and apply across a wide range of national financial crime risk profiles and AML/CFT regimes, implementation may differ across jurisdictions, including in how certain terms are understood and how the requirements for information and data accompanying cross border payments are implemented.

In 2016, the FATF published its *Guidance for a Risk Based Approach for Money or Value Transfer Services* to ensure effective AML/CFT compliance by providers of MVTS.[67] The guidance was aimed at 1) jurisdictions and competent authorities, 2) PSPs operating in the MVTS sector, and 3) banks that had or were considering PSPs operating in the MVTS sector as customers. The recommendations contained in the guidance included:

- Licensing or registration of financial institutions providing MVTS that should also be subject to effective systems for monitoring to ensure compliance with national AML/CFT requirements and the FATF Standards. Any natural or legal person acting as an agent

---

66 FATF (2023), *The FATF Recommendations*, November.

67 FATF (2016), *Guidance for a Risk-Based Approach for Money or Value Transfer Services*.

of a PSP should also be licensed or registered by a competent authority, or the PSP should maintain an up-to-date list of its agents, which can be consulted by the competent authorities in the countries where the PSP and its agents operate.

- Liaising between competent authorities of the PSPs and host authorities to address any financial crime concerns.
- Providing guidance and training to supervisors and their staff to understand the PSP sector and assess the associated financial crime risks and liaising with other relevant domestic regulatory and supervisory authorities to ensure a coherent interpretation of legal obligations and promote a level playing field.
- Fostering domestic and international cooperation and information exchange between supervisors, law enforcement agencies, central banks, intelligence agencies, and financial intelligence units (FIUs) for effective monitoring and supervision of the sector.
- Providing guidance on the effective implementation of an RBA and coordinating with different supervisors to ensure consistent expectations and approaches to the RBA.

In 2021, the FATF published its *Guidance on Risk-Based Supervision* to further promote effective implementation of the RBA for supervision across financial institutions and designated non-financial businesses and professions (DNFBPs).[68] The guidance addressed special considerations for the MVTS sector, such as the use of MVTS sector risk assessments by AML/CFT supervisory authorities to identify low risk activities. The MVTS sector risk assessments provided sufficient transparency for banks and non-banks to continue facilitating financial services to the MVTS sector while appropriately managing financial crime risks using a RBA.

---

[68] FATF (2021), *Guidance on Risk-Based Supervision*, March.

Annex 2: Survey of domestic regulatory and supervisory frameworks

Introduction

Jurisdictions globally take a variety of approaches to regulating and supervising banks and non-banks in their provision of cross-border payment services. This section provides examples from a few jurisdictions to highlight these different approaches, which include a combination of entity and activity-level regulation, supervision and oversight.

The Bahamas

In The Bahamas, a PSP is a payment institution licensed under the Payment Instruments (Oversight) Regulations, 2017.[69] They can include a bank, a bank and trust company, a trust company, a money transmission service provider licensed, or a money transmission agent registered, pursuant to the Banks and Trust Companies Regulation Act, 2020 (Ch. 316) and the Banks and Trust Companies (Money Transmission Business) Regulations, 2008. It can also include a co-operative credit union pursuant to The Bahamas Co-operative Credit Unions Act, 2015; and any other provider licensed to provide payment services under any other relevant law. It should be noted that entities licensed under the Regulations are not permitted to engage in foreign exchange transactions in the absence of a separate licence or prior approval from the Central Bank, or other domestic regulatory authority.

Licensing

All entities that provide payment services in The Bahamas must obtain the proper licensing, according to the scope of services provided, as per the Payment Instruments (Oversight) Regulations, 2017.

Supervisory approach

Supervisory focus for monetary transmission businesses (MTBs) and PSPs is heavily centred on reputational risks, including AML/CFT risk, and operational risk management. In this vein, the Central Bank works to ensure that all key exposures are being effectively identified, measured, monitored and mitigated. Therefore, the Central Bank uses a risk-based approach in the effective supervision of these entities. It is important to note that in this regard, banks and non-banks are not treated differently when it comes to supervisory oversight.

Risk management

All financial institutions in The Bahamas are required to adhere to the rules and regulations laid out in the Financial Transactions Reporting Act, 2018.[70] The Act stipulates how financial institutions should conduct themselves when it comes to exercising customer due diligence, record keeping, internal controls, and assessing risk.

---

[69] Central Bank of The Bahamas (2017), *Payment Instruments (Oversight) Regulations*. July.

[70] Compliance Commission (2018), *Financial Transactions Reporting Act, 2018*.

Minimum capital requirements

According to the Guidelines for Non-Bank Money Transmission Business, all providers should establish and maintain an unimpaired minimum capital of USD 50,000 or such other sum as the Governor may require.

AML/CFT considerations

The domestic approach to regulation, supervision and oversight is largely grounded in AML/CFT and Countering Proliferation Financing (CPF) considerations and is therefore aligned with international regulations set forth by the FATF and other standard-setting and multilateral bodies. In May 2009, the Central Bank issued its first iteration of Guidelines for Supervised Financial Institutions on the Prevention of Money Laundering, Countering the Financing of Terrorism and Proliferation Financing[71] ("AML/CFT Guidelines"), which incorporates both the mandatory minimum requirements of the AML/CFT laws in The Bahamas and industry best practices. Both banks and non-banks are expected to adhere to these Guidelines, and therefore face varying sanctions for non-compliance.

Regarding domestic and cross-border payments, the Bahamas implemented Recommendation 16 under the FATF Recommendations, which seeks to enhance the transparency of cross-border and domestic electronic funds transfers (wire transfers or transfers). The Recommendation was implemented via the Financial Transactions Reporting (Wire Transfers) Regulations, 2018, (FTRR) and is intended to cover any transaction carried out on behalf of a payer through a financial institution by electronic means; it therefore covers both banks and non-bank payment service providers.

European Union

In the European Union, payment services are regulated by several harmonised legislations. The payment services directive (PSD2)[72] and electronic money directive (EMD2)[73] are two key, interconnected directives. PSD2 is the main directive on the authorisation requirements for non-bank PSPs and clarifies the use of agents/distributors. It regulates conduct related aspects for any PSP such as transparency of conditions and information requirements, rights and obligations in relation to the provision and use of payment services requirements, the security of payment transactions, fraud and incident reporting as well as operational risk management. The June 28th, 2023, proposal for the revision of the PSD2[74] envisages a new directive (PSD3), for

[71] Guidelines for Supervised Financial Institutions on the Prevention of Money Laundering, Countering the Financing of Terrorism & Proliferation Financing - https://www.centralbankbahamas.com/viewPDF/documents/2023-04-06-17-20-05-CBOB-AML-CFT-Guidelines-Revised-6-April-2023.Final.pdf.

[72] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

[73] Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC.

[74] Published on 28 June 2023.

the authorisation and supervision of PSPs and electronic money institutions, and a regulation on the provision of payment services (PSR) which primarily sets the conduct-related rules.[75]

PSPs can be credit institutions[76], electronic money institutions regulated under EMD2, payment institutions regulated under PSD2, post office giro institutions, and certain public authorities and central banks. Payments Institutions (PIs) can provide payment services, including placing and withdrawal of cash, execution of payment transactions, issuing of payments instruments[77] and acquiring of payments transactions[78], money remittance[79], payment initiation services[80], and account information services[81]. They can also provide limited short-term credit in connection with the execution of payment transactions as well as other non-licensed activities in accordance with EU or national law.[82] E-money Institutions (EMIs) can in addition issue electronic money and e-money tokens[83] subject to redemption at par. PI and EMIs are subject to prior authorisation based on comprehensive documentation and ongoing supervision by the competent authority. Their initial capital requirements relate to the activities. Account information services are only required to hold a professional indemnity insurance. For money remittance a minimum of EUR 20,000 is required. Payment initiation services require EUR 50,000. All other payment services under a PI licence require EUR 125,000. EMIs need at least EUR 350,000 in initial capital. PIs must hold whatever is higher, the initial capital or own funds based on the harmonised own funds calculation methods depending on the business model and determined by the national competent authorities (NCAs). Own funds for electronic money activities shall amount to at least 2% of the average outstanding electronic money.

In addition, all EU PSPs are subject to regulation on digital operational resilience[84] and strict data protection requirements.[85] Charges are further regulated in the rules on cross-border payments and on the transparency of currency conversion charges within the Union[86] and for card-based payment transactions in the interchange fee regulation.[87] The revised regulation on

---

[75] The PSR will include rules on transparency as well as those on rights and obligations relating to the provision and use of payment services. Additionally, the proposal includes clarifications on open banking by further harmonising requirements for application programming interfaces as well as some updates on fraud prevention including secure authentication.

[76] Regulated under the Capital Requirements Regulation (CRR) /Directive (CRD), CRR3/CRD6 implementing the final Basel III reforms will become applicable as of January 2025.

[77] A payment service provided by a PSP contracting to provide a payer with a payment instrument to initiate and process the payer's payment transactions.

[78] A payment service provided by a payment service provider contracting with a payee to accept and process payment transactions, which results in a transfer of funds to the payee.

[79] A payment service where funds are received from a payer, without any payment accounts being created in the name of the payer or the payee, for the sole purpose of transferring a corresponding amount to a payee or to another payment service provider acting on behalf of the payee, and/or where such funds are received on behalf of and made available to the payee.

[80] A payment service to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider.

[81] An online service to provide consolidated information on one or more payment accounts held by the payment service user with either another payment service provider or with more than one payment service provider.

[82] Payment institutions that engage solely in account information service only need to be registered.

[83] As of 30 June 2024, in accordance with EMD and the Regulation (EU) 2023/1114 (Markets in Crypto Assets Regulation).

[84] Regulation (EU) 2022/2554 on digital operational resilience for the financial sector

[85] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[86] Regulation (EU) 2021/1230 of the European Parliament and of the Council of 14 July 2021 on cross-border payments in the Union

[87] Regulation (EU) 2015/751 of the European Parliament and of the Council of 29 April 2015 on interchange fees for card-based payment transactions

instant payments,[88] which amends the single euro payments area (SEPA) regulation of 2012 on standard credit transfers, aims to make instant payments more secure and fully available to consumers and businesses. It removes legal obstacles for PI and EMIs to become direct participants to payment systems ensuring settlement finality, including to systemically important payment systems[89] and requires them to establish a winding-up plan.

On AML/CFT, the fifth anti-money laundering directive[90] entered into force in June 2018. The more general travel rule obligation for fund transfers were already established previously in 2015[91] but further enhanced with the Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto assets.

Indonesia

As part of payment system regulatory reform, Bank Indonesia (BI) has issued The Bank Indonesia Regulation No. 23/6/PBI/2021 concerning PSPs that uses an activity-based approach (same activity, same risk, same rule) where all PSPs – banks and non-banks – will be subject to regulatory requirements, licensing, and supervision when providing services to facilitate payment transactions to users.

Licensing

Any party acting as a PSP must obtain a licence from the central bank.

Supervisory approach

The Payment System supervision framework comprises a combination of on- and off-site supervision, based on a risk-based approach that is proportionate to the risk profile of the PSP and its systemic importance. The level of regulatory requirements and scrutiny should be commensurate with the risks associated with PSP. To allow for effective offsite supervision, all PSP are required to submit periodic and incident reports to the supervisor.

Minimum capital requirements

All PSPs must meet the provision on the obligation to provide two kinds of capital, (i) initial capital as licence requirements, and (ii) ongoing capital during implementation of business activities.

---

[88] Regulation of the European Parliament and of the Council amending Regulations (EU) No 260/2012 and (EU) 2021/1230 and Directives 98/26/EC and (EU) 2015/2366 as regards instant credit transfers in euro.

[89] By amending the Settlement Finality Directive 98/26/EC.

[90] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU.

[91] Directive 2015/849 Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.

Minimum information system risk management

The PSPs risk management and information system security standard obligations include policy and standard on risk management, the establishment of separate units for audit, compliance and risk management, data and disaster recovery centres, a fraud management system, compliance with cyber security standards, an information technology audit and penetration test, financial audit by a registered public accountant, and standard certificate on security of information on the main Payment System activities.

A framework for controlling financial crime risks

In line with regulation for banks, the regulation for non-bank PSP covers obligations and scope of AML/CFT such as duties and responsibilities of the Board of Directors and Active Supervision of the Board of Commissioners, Policy and Procedures, Risk Management Process, Internal Control System, Customer Due Diligence (CDD) including Simplified CDD and Enhanced Due Diligence (EDD), and Action on The List of Suspected Terrorist and Terrorist Organizations and The List of Funding of the Proliferation of Weapons of Mass Destruction, in accordance with FATF Recommendations and supervises its implementation.

Consumer protection

All PSP have obligation to implement consumer protection principles, in accordance with G20/OECD High Level Principles on Financial Consumer Protection, such as equality and fair treatment, transparency, education and literacy, data protection, and responsible business conduct.

Collaboration and coordination

Regular dialogue and collaboration are essential elements in addressing the challenges and fostering improvements in payment activities, including cross-border payments. In Indonesia, the Financial System Stability Committee consisting of Ministry of Finance, Bank Indonesia, Financial Services Authority, and Indonesia Deposits Insurance Corporation meet regularly to discuss about financial stability concerns. In terms of cross border payments, BI has signed MOUs with authorities from other jurisdictions to enhance cooperation, coordination, and sharing information.

Singapore

The Monetary Authority of Singapore (MAS) is the integrated financial regulator and regulates banks, insurers, capital market intermediaries, financial advisor, stock exchanges, and PSPs.

PSPs are regulated under the Payment Services Act 2019 (PS Act)[92] for seven key payment services: account issuance, domestic money transfers, cross-border money transfers, merchant

[92] Monetary Authority of Singapore (2019), *Payment Services Act 2019*, January.

acquisition, e-money issuance, digital payment token dealing and exchanges, and money-changing.

Supervisory approach

MAS practices risk-based supervision where they aim to reduce the risk and impact of failure of financial institutions or of inappropriate behaviour through increased supervision where it is both appropriate and likely to be effective.

Specific to the PSPs, the intensity of MAS' supervision varies based on an understanding of their risk profiles. The variation is mainly in terms of the frequency of on-site inspections and supervisory engagements with board and senior management. All PSPs are subject to standard, base-level monitoring such as the monitoring of their regulatory returns. MAS also conducts regular industry engagements to raise awareness and foster better understanding of key risks (e.g. AML/CFT) and requirements.

Risk management (including AML/CFT)

Both banks and PSPs are required to develop risk management practices that are commensurate with their business and risk profiles. They are also expected to adopt business practices that deal fairly with their customers and counterparties and to put in place AML/CFT controls that are commensurate with their business activities and risk profile.

The AML/CFT requirements and expectations on financial institutions, including for banks and PSPs are set out in MAS' AML/CFT Notices, Guidelines, and other Guidance issued by MAS. MAS requires all financial institutions to have sufficiently robust controls to detect and deter illicit activities.

Engagement and coordination

MAS monitors international developments in the payments and digital assets space, including ongoing international regulatory practices of major jurisdictions and the work of international organisations and SSBs. MAS has also signed MOUs with other regulators to allow for mutual assistance and facilitation of exchange of information between authorities. This allows the parties to the MOU to strengthen the supervision of the cross-border operations of the financial institutions.

United States

Payment activities and systems in the United States can involve multiple parties, arrangements, and intermediaries, which can add complexity depending on the nature of the payment service being used. Payment services can be offered in the United States by both banks and non-banks.

Banking entities are generally supervised at the federal level by the Federal Reserve, the Financial Deposit Insurance Corporation (FDIC), National Credit Union Administration (NCUA), and the Office of the Comptroller of the Currency (OCC), collectively referred to as (the federal banking agencies (FBAs). The FBAs examine banks not only for safety and soundness, but also

compliance with all applicable laws and regulations, including consumer protection and AML/CFT.

Legal framework

Numerous federal statutes and regulations govern U.S. payment, clearing, and settlement activities. Federal laws include requirements related to AML/CFT and sanctions compliance, responsibilities of participants in electronic funds transfer activities and consumer protection.

Regulatory, supervisory and enforcement framework

Banks

The FBAs are responsible for the oversight of the various banking entities operating in the United States, including U.S. branch offices of foreign banks. The FBAs are charged with chartering, insuring, regulating, and supervising banks and credit unions. In addition to banking supervision, the Federal Reserve System is the central bank of the United States and has other core missions, including conducting the nation's monetary policy, promoting the stability of the financial system, and fostering payment and settlement system safety and efficiency. The FBAs may use their authority, as granted under section 8 of the Federal Deposit Insurance Act or section 206 of the Federal Credit Union Act, to enforce compliance with appropriate banking rules and regulations, including compliance with AML/CFT laws. Treasury's Financial Crimes Enforcement Network (FinCEN) retains overall authority for administration, enforcement, and compliance with U.S. AML/CFT laws.[93] The Consumer Financial Protection Bureau (CFPB) is the Federal government's primary regulator of consumer financial products and services, with a mission to protect consumers in the financial marketplace.

Non-bank PSPs

Non-bank PSPs in the U.S. generally fall within the definition of money transmitters which are a type of Money Services Businesses. Money transmitters are generally defined as persons who engage as a business in the transfer of currency, funds, or value that substitutes for currency from one person to another location or person by any means. Whether a person is a money transmitter is a matter of facts and circumstances. Many FinTech companies that meet these criteria hold money transmitter licenses. Money transmitters are required to register with FinCEN at the federal level but do not have a primary federal regulator. They are subject to licensing and other requirements in the states in which they operate and supervisory oversight by state authorities. In 2021, the Board of Directors of the Conference of State Bank Supervisors voted to adopt the Model Money Transmission Modernization Act, a single set of nationwide standards and requirements to modernise the supervision and regulation of money transmitters. Money transmitters are also subject to examination for Bank Secrecy Act (BSA) compliance by the Internal Revenue Service or state authorities, if applicable. They also come under the jurisdiction

[93] The FBAs have both delegated authority from FinCEN for examinations and separate authority for compliance and enforcement with U.S. AML/CFT laws.

of the Consumer Financial Protection Bureau (CFPB) for purposes of compliance with federal consumer protection laws and regulations.

Broadly, FinCEN's definition of "money services business" includes check cashing, currency exchange, money transmitting, or remittance services and issuance or redemption of money orders, travellers' checks, and other similar instruments. Money transmitters also include any person who engages as a business in an informal money transfer system or any network of people who engage as a business in facilitating the transfer of money domestically or internationally outside of the conventional financial institutions system.

AML/CFT

All banks and many non-bank PSPs are subject to the provisions of the BSA and its implementing regulations, which require financial institutions to establish AML/CFT compliance programs, file certain reports and keep certain records of transactions. BSA regulations require both banks and certain non-banks, including money transmitters, to collect, pass on and retain information on certain funds transfers and transmittals of funds for domestic and international payments. Banks are separately required to have appropriate risk-based procedures for conducting ongoing CDD and complying with beneficial ownership requirements for legal entity customers as set forth in regulations issued by FinCEN. FinCEN has delegated authority for supervising and enforcing compliance by banks with AML/CFT requirements to the FBAs, who also have independent legal authority to examine for BSA compliance in addition to safety and soundness. FinCEN has also delegated similar examination authority to the IRS for supervising the AML/CFT compliance of non-bank financial institutions, including PSPs considered money transmitters under the BSA. The FBAs and IRS supervise their respective financial institutions for compliance with U.S. economic and trade sanctions. The U.S. Treasury's Office of Foreign Assets Control (OFAC) administers sanctions programs and maintains civil enforcement authority for violations of U.S. sanctions laws.

Consumer protection

The CFPB has rulemaking authority with respect to the Electronic Fund Transfer Act and its implementing Regulation E that protects individual consumers engaging in electronic funds and remittance transfers. Remittance transfers generally describe electronic transfers of more than USD 15 sent by consumers in the U.S. to individuals or companies located in foreign countries through a remittance transfer provider. A remittance transfer provider is an entity that provides transfers for consumers in the normal course of its business, and money transmitters, banks and FinTechs may fall within this definition.