FSB FINANCIAL STABILITY BOARD

Stocktake of International Data Standards Relevant to Cross-Border Payments

25 September 2023

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 Twitter: @FinStbBoard
E-mail the FSB at: fsb@fsb.org

Table of Contents

Executive summary 1

1. Introduction 4

2. Stocktake of existing national and regional data frameworks 5

2.1. Findings from the official sector survey 5

2.2. Summary of the written feedback request to industry 7

2.3. Summary of the virtual outreach event with industry 9

2.4. Implications of data localisation 10

3. Suggested areas for improvement 12

3.1. AML/CFT requirements 12

3.2. Cooperation on data privacy issues 14

3.3. Alignment and interoperability of technical standards 15

3.4. Data frameworks and innovation, including digital identity and open banking 17

3.5. Broader alignment and interoperability between data frameworks 18

4. Next steps 20

Annex 1: Respondents to the FSB survey 21

Annex 2: Summary of the stocktake of FSB members 22

Annex 3: Summary of industry written feedback responses 30

Executive summary

The transfer of data across borders is essential to the functioning of the cross-border payments system. These data are subject to a range of data frameworks: the laws, rules and regulatory requirements for collecting, storing and managing data underlying cross-border payments. These frameworks relate to the conditions allowing or restricting data transfer across borders; what data must be stored for regulatory purposes; how data must be secured; what data must accompany an international payment; and technical standards to promote interoperability between bilateral, regional and international payment networks.

The Roadmap for Enhancing Cross-border Payments[1], endorsed by G20 Leaders, seeks to assess frictions that could arise from these frameworks and consider recommendations that would contribute to meeting the G20's commitment to address the challenges of cost, speed, access and transparency in cross-border payments. As set out in the Roadmap, the FSB has taken stock of existing national and regional data frameworks relevant to the functioning, regulation and supervision of cross-border payment arrangements, and to identify issues relating to cross-border use of those data by national authorities and by the private sector. The FSB will use the results of this stocktake as input for taking forward priority actions to facilitating cross-border data exchange and increase the use of standardised messaging formats for cross-border payments under the latest phase of work under the Roadmap which was launched in February 2023.[2]

The FSB surveyed its members and solicited external feedback in writing and through a virtual workshop. Drawing from this work, a number of frictions from data frameworks were identified that pose significant challenges to improving the cost, speed, transparency and access of cross-border payments:

(i) **Fragmentation among data framework requirements and their implementation, most notably across the data needed to accompany a cross-border payment transaction**. Implementation of rules and standards is not always uniform across jurisdictions, the most frequent friction mentioned being divergence in how Financial Action Task Force (FATF) Recommendation 16: Wire Transfers has been implemented. Industry stakeholders also provided information on many different types of jurisdiction-specific requirements for messaging and clearing formats and accompanying legal documentation, requiring manual intervention or resulting in higher incidence of payment rejections.

(ii) **Uncertainty among payment providers on how to balance the various obligations under different data frameworks**, including obligations related to regulatory and supervisory requirements, the use of third-party providers and requirements for data security and privacy. For example, uncertainty may exist as to how to balance obligations related to data privacy and to anti-money laundering and combating the financing of terrorism (AML/CFT) and other regulatory requirements.

(iii) **Challenges arising from restrictions on the flow of data across borders**. Measures that require data to be stored or processed in-country (data localisation) are a significant

1 FSB (2020), Enhancing Cross-border Payments – Stage 3 roadmap, October.

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

cost for firms in terms of fixed overhead and maintenance (including resources to keep such data secure and integrate it into global operations). Market participants argue that these measures could make it more difficult to identify fraud, comply with AML/CFT and other regulatory obligations as well as manage risk on an enterprise-wide basis. Such data localisation measures may also degrade the security of data and the resilience of systems, impede the ability to comply with regulatory and supervisory requirements and may act as a barrier to entry for smaller players, reducing competition in cross-border payments.

(iv) **Frictions may also make innovating in the payment system more challenging.** The lack of a global approach to the many different frameworks acts as a barrier to innovations that could help improve the efficiency of the payments system. Such innovations include full payment traceability, one-time customer verification and pre-payment validation.

A certain degree of friction from data frameworks may be an unavoidable and acceptable consequence of regulations aimed at preserving the security of transactions, meeting AML/CFT objectives and protecting the privacy of citizens. However, the extent of fragmentation in data frameworks across jurisdictions was considered by survey respondents a main contributor to increased cost and inability to automate payments. In light of these observations, the FSB has identified five ways to help reduce the identified impediments while also ensuring that cross-border payments are safe and secure and data is handled appropriately, in line with regulatory objectives:

- aligning AML/CFT related data requirements across jurisdictions, while preserving standards;
- promoting greater cooperation among different approaches to data privacy as well as between data privacy and other policy objectives;
- promoting alignment and interoperability of technical standards;
- exploring how current data frameworks enable, or impede, future developments that may lead to further improvements (e.g. open banking, digital identity, transition to greater real time payments); and
- seeking broader interoperability across data frameworks applicable to cross-border payments.

Work is already underway as part of the Roadmap to address many of these identified issues:

- The FSB is developing recommendations, for public consultation by early 2024, 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 access requirements. The FSB will work with external stakeholders to develop case studies to assess the impact of selected frictions on cross-border payments and identify where action should be prioritised. (Action 7a of the February 2023 Roadmap update.)

- The Committee on Payments and Market Infrastructures (CPMI) established a joint task force comprising technical experts from the CPMI and the Payments Market Practice Group (PMPG) to develop harmonisation requirements for the use of ISO 20022 messages in cross-border payments.[3] The requirements will be finalised in October 2023. The CPMI will also work with payment system operators and market practice industry groups to align market practice guidelines with the ISO 20022 harmonisation requirements. (Actions 8b and 8c of the 2023 Roadmap update.)

- By February 2024, the FATF will enhance Recommendation 16: Wire Transfers to take account of recent and upcoming developments in the architecture of payments systems, including adoption of ISO 20022 messaging standards, with a view to improving the consistency and usability of message data in cross-border payments and facilitate more efficient AML/CFT checks. (Action 6a of the 2023 Roadmap update.)

These actions are priorities for the next phase of the Roadmap.

[3] CPMI (2023), *ISO 20022 harmonisation requirements for enhancing cross-border payments: consultative document*, March.

1. Introduction

The FSB developed the Roadmap, in coordination with the CPMI and other relevant international organisations and standard-setting bodies (SSBs), aiming to address the four main challenges faced by cross-border payments: cost, speed, transparency and access. These challenges vary widely by type of payment, jurisdiction and currency corridor. The flow of data across borders, between payment originator and beneficiary, through intermediaries and the payment infrastructure, is required in any cross-border payment. Data frameworks that govern such data flows in one jurisdiction affect the provision and supervision of cross-border payment services in another. Data frameworks applicable to cross-border payments include the following:

- Frameworks regulating data privacy, security or storage, including data location requirements, electronic communications and data sharing with use of third-party providers.
- Requirements for data retention (e.g. required data items for regulatory compliance).
- Multilateral and bilateral trade agreements covering use and sharing of data across borders.
- Frameworks regulating access to data, such as open banking frameworks.
- Implementation of international standards from the FSB and other SSBs, if not included as part of formal domestic data frameworks.

Building block 6 of the 2020 Roadmap seeks to review the interaction and potential constraints between data frameworks and cross-border payments, with the aim to inform recommendations to address those constraints. To take forward this work, the FSB (in cooperation with CPMI and other SSBs, domestic data protection bodies and other data governance bodies) conducted a stocktake of existing national and regional data frameworks relevant to the functioning, regulation and supervision of cross-border payment arrangements to identify issues relating to cross-border use of those data by national authorities and by the private sector.[4]

The FSB has identified this work as having the greatest potential to contribute to achieving the quantitative targets that have been established for the Roadmap. Building on this stocktake, by early 2024 the FSB will develop recommendations, for public consultation, 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 access requirements.

This report provides a summary of the stocktake (Section 2), discusses identified areas for improvement drawn from the stocktake and other feedback from external stakeholders (Section 3), and sets out next steps for promoting alignment and interoperability across data frameworks applicable to cross-border payments (Section 4).

[4] The expected completion date for this action was extended from December 2021 to September 2022, and subsequent milestones were accordingly also extended by nine months. See FSB (2022), *G20 Roadmap for Enhancing Cross-border Payments: Consolidated progress report for 2022*, October.

2. Stocktake of existing national and regional data frameworks

In 2021, the FSB surveyed its members and requested written feedback from external stakeholders, including industry and non-governmental organisations. The FSB also posted an online survey on its website to solicit feedback from a broader range of external stakeholders, including regulated financial institutions, trade associations representing payment industries, non-bank payment service providers, private financial market infrastructures and messaging network providers. In order to explore in greater detail how data frameworks impact cross-border payments and to allow stakeholders to offer ideas and issues not previously considered, the FSB held an outreach event in February 2022.

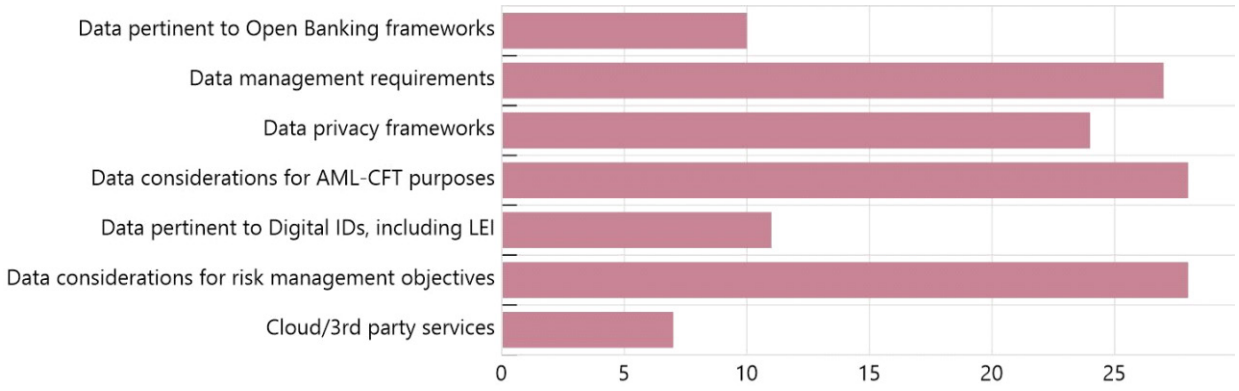
This section of the report summarises: (1) the findings from the survey of FSB members, (2) the written feedback from industry and (3) the outcomes of the virtual outreach event with external stakeholders. It also highlights some specific data localisation issues raised by several private sector participants, such as the rapid increase (and variation) in data localisation measures and mirroring requirements.

2.1. Findings from the official sector survey

The FSB received responses from all 25 member jurisdictions (see Annex 1). The stocktake captured 147 different measures relevant to cross-border payments across the 25 FSB member jurisdictions. A detailed summary of the findings of this stocktake is provided in Annex 2.

The most common policy measures reported were related to AML/CFT requirements; risk management objectives, including cybersecurity and operational resilience; data management requirements[5] and data privacy requirements (Graph 1).

Most commonly reported policy measures **Graph 1**



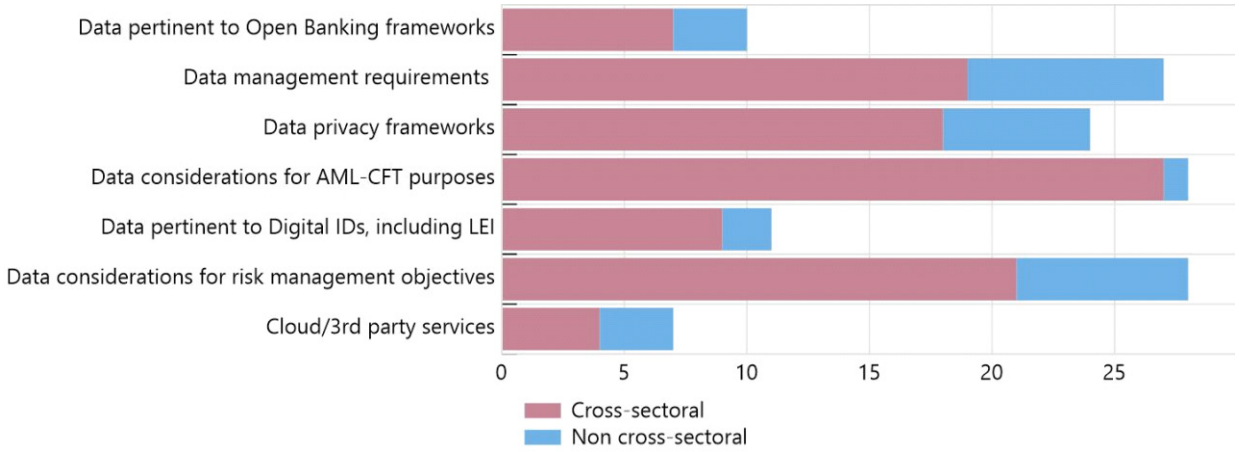
Source: Survey responses

[5] Data management requirements was a broad category, encompassing technical standards for payments (messaging, clearing, etc.), how data needed to be stored or processed, and also frameworks that facilitated the cross-border transfer of data (trade agreements, non-binding arrangements).

Policy measures were often applicable to financial services more broadly, rather than specific to payments or to cross-border payments (graph A1 in Annex 2). The majority of frameworks (71%) were national, though in several cases they could be national implementation of international or regional frameworks, including national implementation of FATF requirements or national implementation of regional frameworks such as the European Union (EU)'s Revised Payment Systems Directive (PSD2).[6]

Another significant finding is that surveyed measures relate to a wide variety of policy objectives, were often cross-sectoral in scope (graph 2 below) and different authorities were responsible for their implementation (graph A2 in Annex 2). Authorities reported some cross-sectoral cooperation mechanisms while responses were more limited with reference to cross-border cooperation mechanisms relevant to the identified data frameworks.

Cross-sectoral measures[7] by policy objective **Graph 2**



Source: Survey responses

Authorities also identified some areas of data frameworks that both positively and negatively affected cross-border payments. Authorities acknowledged that frameworks to implement AML/CFT compliance, data privacy, data management requirements and cybersecurity and risk management requirements could result in costs to financial institutions. In relation to AML/CFT, authorities were aware of fragmentation in the national implementation of international frameworks, notably with respect to FATF Recommendation 16. They also noted that national AML/CFT rules introduced additional requirements for customer due diligence and enhanced monitoring of cross-border correspondent banking based on specific risk and context banking relationships.

Some authorities also stressed the benefits of these policies, including to the security of the payments system and operators.

6 European Central Bank (2018), *The revised Payment Services Directive (PSD2) and the transition to stronger payments security*, March.

7 If a policy objective applied to more than one type of provider, this report classifies it as a "cross-sectoral" measure. Cross-sectoral in this case refers both to across sectors in financial services and economy-wide.

Some jurisdictions highlighted the benefit of regional approaches, like PSD2 and the Single Euro Payments Area (SEPA) on credit transfers, but also noted frictions associated with how this approach was applied to payments involving non-EU jurisdictions.

There was some diversity in views regarding requirements about local data storage or limited data transfers. Authorities acknowledged that these policies required costs to comply, but the marginal impact on the cost and speed of cross-border payments was unclear. One authority noted that localisation of payments data ensures utmost data security, which in turn results in greater transparency and fosters confidence amongst the end-users of payment systems. Another authority assessed that it could improve transparency in the event that the financial institution involved suffered financial difficulties. Other authorities had agreed bilaterally not to impose such measures and indicated that the absence of these policies could have positive effects on the cost and speed of payments.

Frameworks to implement digital identity or open banking were only infrequently reported. One authority reported that if the Legal Entity Identifier (LEI) were to be more widely adopted and used in cross-border payments, efficiency (i.e. cost or speed) could improve, citing the CPMI's Stage 2 report on the building blocks of the cross-border payments Roadmap.[8] Some authorities assessed that open banking could improve domestic market efficiency, cost and/or transparency and that there was the potential to also improve the efficiency of cross-border payments.

Authorities identified a number of areas where data frameworks could be improved. A common suggestion was to harmonise the national implementation of FATF recommendations. Some authorities pointed to the move to ISO 20022 as a positive way to improve interoperability in technical standards as well as adopting a means for interoperable digital identity. Other suggestions included addressing frictions by developing interoperable principles and standards, establishing more adequacy agreements for data privacy, and promoting collaboration between financial authorities and data privacy authorities. These suggestions, along with those from industry, are discussed in Section 3.

2.2. Summary of the written feedback request to industry

The FSB solicited feedback from external stakeholders to better understand how data frameworks shape the provision of cross-border payments, where areas of friction may arise from a provider perspective, and how these data frameworks might enable, or impede, the improvement of the cross-border payment system in line with the G20 objectives. The FSB received 30 responses from a diverse range of payment providers, payment infrastructures, and other interested parties. The responses indicated strong support for the work of the Roadmap and consideration of this building block. A detailed summary of written feedback responses can be found in Annex 3.

Stakeholders noted that capacity to deliver on the Roadmap exists but cautioned that regulatory barriers from data frameworks are a key challenge. Stakeholders frequently had to implement manual or other costly approaches given data fragmentation and regulatory conflicts between data frameworks, impacting cost, speed and access. They further emphasised that global harmonisation of data management and frameworks would support fast and efficient processing

8 CPMI (2020), *Enhancing cross-border payments: building blocks of a global roadmap: Stage 2 report to the G20*, July.

of payments, and some respondents went further to suggest that it was a pre-condition to completing the Roadmap. Most respondents agreed with and emphasised the official sector view, with additional details and examples provided.

Fragmentation between frameworks*:* Industry agreed with official sector responses that certain requirements, in particular those associated with data privacy and AML/CFT regulations, can be a significant driver of costs for cross-border payments. Stakeholders went further to emphasise that the fragmentation in approaches and frequent changes to local requirements increased costs of providing cross-border payments, for example, the lack of alignment in wire transfer reporting rules between payments corridors. One respondent noted that while FATF had issued guidance to address fragmentation and improve information sharing, implementation of that guidance was lacking. Some authorities also mentioned technical challenges with complying with sanctions regimes.

ISO 20022 was welcomed by many stakeholders as a means to address some fragmentation in payment standards. As noted, some challenges could arise from differences in its implementation. Several stakeholders commented on the perception that different payment types and rails[9] had different expectations for data retention for regulatory purposes. Stakeholders welcomed regional approaches but noted that there was fragmentation from differences in national implementation.

The EU's General Data Protection Regulation (GDPR) was cited by several stakeholders as an effective approach to data privacy in the EU and potentially a model for others (see Box 2 for further information). Industry stakeholders in particular appreciated the focus on data rights regardless of the location of data, and that financial data was not inherently treated as sensitive. On the other hand, different stakeholders noted challenges in implementation, including mainly with respect to transferring data to countries outside the EU. A few references were made also to interaction with other regional frameworks, diverging national interpretations and technical implementation (e.g. concerns that industry stakeholders have that GDPR may prevent pre-payment validation efforts).

Conflicts between requirements: Addressing tensions between different data frameworks, notably those associated with data privacy and AML/CFT obligations, was a common challenge. These conflicts are complicated by the situation in which a cross-border payment could be subject to requirements of different frameworks depending on its potential payment path and currency, thus increasing the chances of fragmentation. Stakeholders noted instances where financial institutions would refuse to share relevant information for AML/CFT compliance purposes, citing data privacy. They also noted that even though some jurisdictions had similar frameworks, national implementation was still fragmented and causing conflicts. Some suggested that data privacy obligations may pose a challenge to developing up-front payment validation, which could reduce the risk of payments fraud.

Challenges arising from restrictions on the flow of data across borders: The impact of data localisation and other data restrictive policies was frequently mentioned by industry. Several stakeholders argued that these policies impacted the cost of cross-border payments, made it more difficult to resolve payment exceptions or identify fraud, and caused difficulties in complying

9 A payment rail is a payment platform or a payment network that moves money from a payer to a payee. Either party could be a consumer or business, and both parties are able to move funds on the network. (source: en.wikipedia.org).

with AML/CFT and facilitating regulatory and supervisory access. Some also pointed to data mirroring and regulatory policies for outsourcing as often achieving the same effect as data localisation. They stated that these policies should not focus on the location of data and that alternative approaches, including focusing on appropriate use and access, or leveraging technology (e.g. encryption) were preferred solutions to address authorities' concerns. Stakeholders encouraged the FSB to examine this area, particularly the regulatory and supervisory implications. This area is further discussed in Section 2.4.

Innovating in the Payment System: Stakeholders emphasised that digital identity could be critical to improve AML/CFT compliance. One stakeholder noted the need for e-KYC (Know Your Customer) guidance. Stakeholders also encouraged adoption of IBAN[10] or some other global identifier to increase the efficiency of cross-border payments. Additionally, one stakeholder emphasised the need for enhanced payments traceability to help resolve payment errors and rejections, and address the risk of fraud. One stakeholder noted that the FSB should consider the implications of rich data in payments and the ability to connect payments transactions with underlying use cases, like invoicing or trade financing.

The written feedback also offered numerous suggestions to address cross-border payments, including several suggestions for further harmonisation in frameworks. These suggestions are further discussed in Section 3.

2.3. Summary of the virtual outreach event with industry

In February 2022 the FSB held an outreach event on how data frameworks impact cross-border payments. The event was attended by 27 representatives from banks, financial market infrastructures (FMIs), mobile money operators, international credit card companies and non-bank payment service providers engaged in cross-border e-commerce and remittance activities as well as industry bodies and private sector issuers of guidance. Participation was balanced to ensure a mix of industry and regional representation. The outreach event was divided into two sessions: the first consisting of an exchange of views on the impact of data frameworks on cross-border use of data, focusing on potential areas of friction, and the second featuring a deep dive into the four suggested areas where data frameworks could be improved to facilitate cross-border payment efficiency.

Areas of friction: Participants at the event reiterated the need for harmonisation of cross-border data standards and regulatory frameworks, noting inconsistencies in data standards related to regulatory compliance checks, variations in regulatory treatment depending on the payment type and the rails upon which cross-border payments travel, and a lack of interoperability of various data frameworks. One participant stated that until harmonisation in data requirements is achieved, it would be difficult to see material improvements in cross-border payments.

Most participants also raised concerns regarding data localisation, highlighting how these restrictions undermine participants' ability to conduct AML/CFT/KYC compliance and other regulatory checks while meeting regulatory access requirements, resulting in increased costs and decreased data security. Others highlighted how local restrictions related to data privacy, cybersecurity, procurement and other regulations serve as de facto localisation requirements.

[10] International Bank Account Number.

One participant stressed that this could be more problematic if the financial institution relied on data sharing between affiliates. Another stressed the potential cybersecurity implications of data localisation. Cloud services was seen as a key innovation to make payments cheaper, more resilient and address financial inclusion gaps, but significant regulatory challenges to using these cloud services were mentioned. Participants also highlighted changes in the payments landscape and the importance of ensuring a level regulatory playing field between incumbents and new actors, technologies and system operators.

The move toward the adoption of ISO 20022 messaging formats was also seen as a positive development to be encouraged. However, some participants recommended caution with respect to differences in implementation/interpretation of data fields.

Suggestions for improvement: Participants called for increased engagement between regulators, for example between AML/CFT regulators and data protection/privacy or sanctions authorities, as requirements in these areas are often the source of conflict at a national level. Participants also welcomed international efforts at the World Trade Organization (WTO) and the Organisation for Economic Co-operation and Development (OECD), as well as bilateral efforts. One participant suggested the need for a regulatory license to provide flexibility to store data, particularly for cross-border transactions (i.e. allowing a copy of the domestic component of the transaction to be also stored abroad). A similar suggestion was made to harmonise audit and other oversight frameworks so that payment providers are audited less frequently and according to consistent standards. Inconsistencies in these frameworks can create complexity and uncertainty for payment service providers, impacting their ability to operate efficiently and comply with multiple sets of standards. Participants encouraged the development of digital identities that could really help small payment providers in the context of open finance (see Section 3.4). Others suggested that common standards or common clearing templates could serve to ensure messaging format requirements are applied consistently to existing and emerging payment technologies and providers. Participants also supported measures to improve data sharing among jurisdictions.

Participants suggested several roles that the FSB could play in addressing frictions. They suggested that the FSB could work with regulators to share best practices and encourage FATF to promote implementation of its guidance. The FSB could play a significant role bringing various authorities together including national regulators, data protection/privacy authorities and sanctions authorities, developing standards and best practices particularly in defining baseline standards of data required to complete cross-border payments that could be included in bilateral or multilateral frameworks, and providing an important voice in highlighting this issue to national financial authorities.

2.4. Implications of data localisation

The rapid increase (and variation) in data localisation measures and mirroring requirements were raised as a particular issue by several private sector respondents to the written feedback request. Given the importance of this cross-cutting topic, specific data localisation issues raised by external stakeholders were further explored at the outreach event and are summarised below. The set of policies categorised under data localisation are often intended to achieve a range of underlying public policy objectives (most commonly regulatory and supervisory access, data privacy and cybersecurity). Variations of these policies include:

- Conditional limitations on data export (e.g. for personal data);
- Local copy requirements (sometimes referred to as “data mirroring”) or local processing requirements; and
- Outright prohibitions on data export (or where conditional approvals for export are very challenging to obtain).

Some external stakeholders noted that regulatory requirements not specific to data could result in the same outcome, e.g. requirements applicable to third-party service suppliers, like cloud services. External stakeholders made two arguments against these policies.

First, the implementation of these policies varied significantly or were often not clear (between defining what sensitive data was subject to such requirements and whether the requirements were for local processing or storage), often requiring custom solutions for each implementing jurisdiction. One stakeholder also noted that while the official sector may consider data mirroring as a solution that allows the movement of data beyond borders, such solutions frequently have the same effect as localisation requirements in practice.

Second, localisation policies can have a number of negative effects, sometimes in ways that would be in conflict with their intended purposes. Industry stakeholders argued that data restrictive policies could:

- increase cyber and operational risks by preventing firms from using regionally situated experts to manage operational risks on an enterprise-wide basis and often require patchwork changes to existing data architecture, thus increasing the possible scope for vulnerabilities.
- prevent financial institutions from pooling data from different sources, thereby weakening internal capabilities to effectively manage risk, detect fraud or identify suspicious activities for AML/CFT compliance purposes.
- prevent financial institutions from complying with cross-border regulatory requirements, including AML/CFT compliance, prudential supervision and investor protection requirements.
- increase fixed and variable costs to deliver payments, by often requiring new data centres and systems to accommodate such policies. This acts as a barrier to entry for smaller or new players. They also have potential environmental implications associated with the requirement to establish and maintain additional data centres.

External stakeholders suggested that regulatory approaches should be focused on proper access and usage of data by approved users rather than physical location of data. Participants also suggested that agreements to allow regulators to access data across borders or encryption could be the means to address some of the underlying policy objectives. Some participants suggested that the FSB should issue guidance to help address this issue. Finally, third-party outsourcing requirements were often mentioned alongside data localisation issues and in a similar context. More specifically, policies that restrict outsourcing arrangements often de facto result in data localisation. Some responses specifically highlighted bilateral trade agreements

and non-binding statements that discouraged data localisation as policies that should be adopted more broadly.

This issue was further explored at the outreach event where stakeholders stressed that the trend towards data localisation is increasing, and several considered it to be their top concern. Participants noted that moving towards keeping records on the cloud for small and medium enterprises should reduce costs and increase capabilities, and that requirements that prevented the use of third-party providers could undermine the objectives of the cross-border payments Roadmap and acted as a competition barrier to do business cross-border. Some participants highlighted that new technologies (such as cloud and/or digital ledger technology) would have the potential to support the sharing of information across jurisdictions in a secure and privacy-friendly manner. In this sense, information sharing could potentially facilitate compliance with AML/CFT requirements by facilitating the matching and storage of data across jurisdictions (e.g. for sanction screening purposes). One participant noted that addressing these policies would require addressing the underlying motivation for these policies, e.g. jurisdictional concerns regarding regulatory access or data privacy.

Feedback in writing and at the outreach event revealed some positive developments in this regard with ongoing work at international level, e.g. at the WTO, OECD and Group of Seven (G7), as well as bilateral agreements on certain payment corridors. Participants believed that the FSB could have a positive role to play in encouraging further work in this area.

3. Suggested areas for improvement

Both the FSB member stocktake and stakeholder outreach offered a range of ideas for improving data frameworks to facilitate cross-border payments, resulting in the identification of five possible areas for further consideration.

3.1. AML/CFT requirements

Official Sector*:* Several authorities noted that, while AML/CFT requirements were based on a common set of principles, there was still fragmentation among approaches that could give rise to frictions in cross-border payments, particularly with respect to wire transfer recordkeeping and offered further suggestions to promote convergence and interoperability. One authority suggested that multilateral cross-border mechanisms for reciprocal information sharing, perhaps through a platform safeguarding KYC information available to participating financial institutions could improve frictions in cross-border payments.

Private Sector*:* Addressing fragmentation and costs in complying with AML/CFT requirements was a key priority for many external stakeholders. Many participants mentioned dealing with a lack of clarity on precisely what data needs to be exchanged for AML/CFT compliance purposes.

Participants noted that FATF had issued guidance in many areas raised by participants, including information sharing. Even with such guidance, they still experienced significant issues with fragmentation in national implementation. Aligning national implementation of FATF Recommendation 16 across jurisdictions was a frequent suggestion. Some stakeholders remarked that it appeared that different cross-border payments systems were subject to different requirements and that there should be greater alignment with respect to system requirements.

One participant suggested the possibility of FATF making data sharing part of its mutual evaluation process. One written comment noted that the development of e-KYC guidance would be helpful. Another comment noted that clarity on how suspicious activity reports were being used and their retention requirements would be welcomed.

Similarly, several stakeholders noted that aligning the data that needed to be searched to comply with local and global sanctions requirements would also be welcomed.

Box 1 summarises the ongoing work of the FATF related to applying AML/CFT rules consistently and comprehensively.

Box 1: FATF-Private sector information sharing for AML/CFT purposes

Under the Germany Presidency of the FATF, from 1 July 2020 to 30 June 2022, digital transformation and working with data protection authorities was a priority. In July 2021, FATF completed the first stage of this work, which was two stocktake reports on the use of emerging technologies: (1) to share AML/CFT information between financial institutions while ensuring data privacy and protection;[11] and (2) on opportunities and challenges associated with other emerging AML/CFT technologies[12]. A second stage of this work is to develop guidance or other material, with input from data protection authorities, focusing on how technology or other mechanisms can improve information sharing to enhance AML/CFT functions.

The FATF has completed a number of projects to promote information sharing for AML/CFT purposes, For example, in 2020, FATF released guidance on digital ID,[13] which highlights the role of public and private sector digital ID solutions in the customer due diligence process and sets out a framework for incorporating these solutions within a risk-based framework. In February 2018, FATF amended Recommendation 2 of the FATF standards to require cooperation and coordination between relevant authorities to ensure the compatibility of AML/CFT/CPF requirements with Data Protection and Privacy rules and other similar provisions (e.g. data security/localisation). In November 2017, the FATF released Guidance on private sector information sharing,[14] which identifies key challenges that inhibit sharing of information within and between financial institutions and highlights country examples to facilitate sharing of information.

In October 2021, the FATF published a stocktake of survey results on implementation of FATF Standards.[15] The FATF launched the industry survey in November 2020, in consultation with the Basel Committee on Banking Supervision (BCBS), to identify areas where divergent AML/CFT rules or their implementation cause friction for cross-border payments. The survey and the subsequent technical dialogue with the industry participants revealed that divergent implementation of AML/CFT requirements seems to contribute to challenges for cross-border payments in a number of ways. While some of these issues may not exclusively relate to cross-border aspects, inefficiencies caused by an inconsistent implementation seem to cause friction, leading to increased cost, reduced speed, limited access and reduced transparency. Inconsistent national approaches also seem to create obstacles in identifying and verifying customer and beneficial owners, effective screening for targeted financial sanctions, sharing of customer and transaction information and establishing and maintaining correspondent banking relationships.

---

11 FATF (2021), *Stocktake on Data Pooling, Collaborative Analytics and Data Protection*, July.

12 FATF (2021), *Opportunities and Challenges of New Technologies for AML/CFT*, July.

13 FATF (2020), *Guidance on Digital ID*, March.

14 FATF (2017), *FATF Guidance – Private Sector Information Sharing*, November.

15 FATF (2021), *Cross-Border Payments: Survey results on Implementation of the FATF Standards*, October.

3.2. Cooperation on data privacy issues

Official Sector*:* Two authorities recommended that further efforts to undertake data adequacy assessments of foreign jurisdictions would facilitate cross-border flows of personal data in a manner compliant with their domestic regimes. One of these authorities also recommended greater coordination between data protection authorities and financial supervisors on data breaches to limit overlaps in compliance obligations.

Private Sector*:* Industry stakeholders asked for common principles to be adopted between different privacy frameworks to enable mutual recognition across jurisdictions. Some stakeholders noted that the lack of defined data privacy frameworks in some emerging markets was a challenge to navigate. Like the official sector, some industry participants encouraged adequacy arrangements or other mechanisms to address different approaches to data privacy between major markets.

Stakeholders noted the importance of providing clarity on interactions between data privacy requirements and other frameworks (e.g. AML/CFT, cybersecurity). Some stakeholders noted concerns that data privacy frameworks impede the development of up-front payment validation processes while others noted a lack of clarity associated with different data privacy frameworks and cross-border payments (e.g. whether payment information was in scope of those frameworks or not). One commenter suggested that there should be a data privacy framework for payments that could help resolve the tensions between data privacy and financial sector use cases and regulatory frameworks.

These suggestions were reinforced at the virtual outreach event, with stakeholders highlighting the conflicts between data privacy requirements and AML/CFT regulations. Data privacy and cooperation on this was further raised at the outreach event with conflict between data privacy rules enacted by national data privacy authorities resulting in conflicts with those issued by national financial regulators. Another respondent noted that the key to attaining data standardisation is to reach a common agreement between data privacy and AML/CFT regulatory authorities.

Box 2: Data privacy across borders

The 1980 *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*[16], which were updated in 2013 to the *OECD Privacy Framework*,[17] provides a common understanding for data privacy across borders as well as modernising principles on cross-border data transfer and legitimate restrictions. As recently as October 2021, the G7 Trade Ministers committed to support the OECD's work on developing common principles for trusted government access to personal data with the ultimate goal of facilitating cross-border data flows.

Within the EU, member states transfer data across borders under the GDPR which ensures a harmonised framework for Member States, including for dealing with data transfers to countries outside the EU. The GDPR is based on a set of data protection principles and the need to establish an independent data protection authority. A key element under the GDPR framework is that it applies to companies processing the personal data of data subjects residing in the EU regardless of the data processing location. The EU framework also allows for adequacy decisions for third countries to

16 OECD (1980), *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, September.

17 OECD (2013), The OECD Privacy Framework, July.

facilitate data flows.[18] Other mechanisms to transfer data outside the EU include: (i) binding corporate rules, (ii) standard contractual clauses and (iii) adherence to an approved code of conduct or certification mechanism.

The Asia-Pacific Economic Cooperation (APEC) launched in 2013 and revised in 2015 the Cross-Border Privacy Rules (CBPR) system[19]: a government-backed data privacy certification that companies can join to demonstrate compliance with internationally-recognised data privacy protections. The framework relies on a certification system for data controllers which requires the existence of a privacy enforcement authority and the designation of an accountability agent. Additionally, the framework is based on seven rules consisting of (i) enforceable standards, (ii) accountability, (iii) risk-based protections, (iv) consumer friendly complaint handling, (v) consumer empowerment, (vi) consistent protections and (vii) cross-border enforcement cooperation. As of November 2021, participating economies include Australia,[20] Canada, Japan, Korea, Mexico, the Philippines, Singapore, Taiwan and the United States of America.

Additionally, in January 2021 the ASEAN Model Contractual Clauses were approved, consisting of contractual terms and conditions that may be voluntarily adopted by companies as a legal basis for the cross-border transfer of data. This framework is based on two modules, the first allowing transfers from data controllers (e.g. payment service provider) to data processors (e.g. third-party service provider) and the second focusing on transfers from data controller to data controller (e.g. payment service provider to payment service provider).

3.3. Alignment and interoperability of technical standards

Official Sector*:* Some authorities highlighted the benefits of interoperable data principles and standards to improve data portability and cross-border data flows. Two authorities highlighted the benefits of greater adoption of interoperable data messaging standards, particularly ISO 20022. One authority highlighted its efforts to promote regional integration and information sharing among participating central banks, through the Single Eurasian Payments Space. One authority noted that it would be beneficial for greater adoption of the LEI to be encouraged.

Private Sector*:* In their written feedback, many respondents noted the complexity associated with complying with many different local requirements, resulting in manual intervention and payment rejections. Other points made included:

- Support for interoperable messaging standards, though one respondent suggested that there was too much variation in ISO 20022, and that there was a concern with what would happen to jurisdictions that were lagging in adopting ISO 20022.
- Some suggested that data frameworks needed to be adjusted to allow for upfront payment validation to reduce rejections and allow for payment traceability.

---

[18] Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the United States of America (limited to the Privacy Shield framework under review) have been awarded with adequacy decisions by the European Commission.

[19] APEC (2015), APEC Privacy Framework.

[20] Australia is a participating economy in APEC's Cross-Border Privacy Rules (CBPR) System that requires participating businesses to implement data privacy policies consistent with the framework. At this time, Australia has not formally implemented the system domestically so there are currently no participating Australian businesses or organisations.

- Some encouraged the expansion of regional approaches like the EU's SEPA, though others mentioned the need to address frictions in local variations or with other policy frameworks.
- Several suggested the need for a standard data format for cross-border payments.
- Several noted that it would be beneficial for more jurisdictions to adopt IBAN or develop a common legal entity identifier.

This theme was further explored at the outreach event where standardisation of messaging templates (and in particular clearing templates) was raised as important as well as the need for a common minimum standard of data. While the move to ISO 20022 was frequently highlighted as a positive and welcome development, it was noted that it would be another 3-4 years before it was fully rolled out. Additionally, even within ISO 20022 there remains issues with ensuring consistency and simplified minimum standard requirements, one participant mentioning that there were over 12 ways to insert an "account number" as an example. At the same time, one stakeholder suggested the need to be flexible to allow for new addressing formats, including mobile numbers, email addresses or finding a way to interface with cross-border payments.

Box 3: ISO 20022

The ISO 20022 standard is a standard for electronic data interchange between financial institutions. The standard applies to financial information transferred between financial institutions, including payment transaction information, securities trading and settlement information, and other financial information. It is supported by a central repository, with a data dictionary and a catalogue of messages. Unlike some other standards ISO 20022 is free and open for anyone to use.

Because ISO 20022 covers a broad range of financial services, it enables a common understanding and interpretation of information, as well as the ability to reuse components across all messages regardless of the original application, so that individual components of a message to facilitate securities settlement can be used for payments, for example. It also can facilitate mapping between other standards. Such interoperability enables automated transfer and straight-through processing (STP) across entire processing chains. Another benefit of the ISO 20022 standard is its enhanced payload capacity which provides for richer and more detailed data, as well as more structured reference data relative to proprietary message formats. These features also support compliance screening and STP across processing chains.

Major reserve currency payment systems have adopted, or are in the process of adopting, the ISO 20022 messaging standard (e.g. TARGET2, Fedwire, STP, CHAPS, BOJ-NET). Moreover, many large financial infrastructures and user groups are already using ISO 20022 in payments and securities settlement, and it has become the standard for real-time payments. A spur to global adoption of ISO 20022 has been SWIFT's decision to adopt ISO 20022 for cross-border payments and to end support for the MT (message type) messaging standard in cross-border payments exchanged across its private messaging network by November 2025. More than 70 market infrastructures are in the process of adopting ISO 20022. Thus, even payment systems that have chosen not to adopt the ISO 20022 standard will be seeking to map their proprietary messaging standards to the ISO 20022 standard for cross-border payments.

International work is also currently underway to ensure that the interoperability benefits of the ISO 20022 standard are preserved even as the standard is implemented in slightly different ways in different jurisdictions. In particular, central banks are collaborating with industry through a CPMI task force to standardise ISO 20022 messages and data elements used in cross-border payments. This task force is identifying a set of common elements and attributes (e.g. permitted characters, supported length) that are considered the minimum standard for cross border payments messages to minimise

variances across jurisdictions. To facilitate implementation, the task force is also developing a proposal for how these elements and attributes could be maintained in an online library used to support the conversion and/or mapping of domestic formats to the recommended common elements. The outcome of these efforts has fed into high-level guidance for the harmonised use of ISO 20022 messages and elements in an end-to-end cross-border payment transaction, supporting interoperability and STP.[21]

3.4. Data frameworks and innovation, including digital identity and open banking

Official Sector: In addition to promoting interoperability in technical standards, some stakeholders encouraged consideration for how open banking frameworks should interact at a cross-border level. Additionally, with the move to real time cross-border payments, one authority suggested that there should be multilateral collaboration to address potential fraud risk. Two authorities noted that greater adoption of digital identity solutions could be helpful in reducing time and cost spent on AML/KYC procedures as the customer will have a trusted ID that payment service providers (PSPs) can use to access the necessary information and enabling interoperability between them as they will no longer have to run their own ID processes.

Private Sector: Stakeholders made a number of similar comments, regarding the need to consider open banking and broader interoperability issues across a range of current and future payment systems. One respondent also noted that open banking across borders would only be possible based on clear cross-border legal certainty on data sharing and data portability.

Stakeholders also mentioned other features that needed to be developed in the cross-border payments system, including up-front payment validation and payment traceability that could reduce fraud and payment rejections. Digital identities were considered a significant piece of the puzzle that was missing, especially when sending identification information of both payer and payee in a transaction across payment rails. It was also noted that, from a financial inclusion and remittances perspective, while there is a general tendency for payments to become digital, many migrants are not digitally literate and are therefore being increasingly forced to use informal channels. At the virtual outreach event, participants also highlighted the need to achieve a level playing field across payments providers in terms of requirements.

Box 4: Open banking/open finance

Open banking is an emerging financial services model that focuses on the portability and availability of customer data held by financial institutions. Data-sharing frameworks are critical to shape the open banking/open finance model. An open banking framework comprises three key features: customers having greater access to and control over their banking data; financial institutions being required to share customer data with customers; and, with the consent of customers, financial institutions sharing customer data with accredited third-party providers.

Consumers currently take advantage of data sharing through screen scraping or API. Screen scraping is used to access data stored in closed systems not readily readable by computer applications. This method requires that the customer shares their login credentials with the third-party provider that performs the screen-scraping task so that they can log in and access their account data to import into their systems. Screen scraping does not require the financial institution holding data to develop any

[21] CPMI (2023), *ISO 20022 harmonisation requirements for enhancing cross-border payments: consultative document*, March.

new processes, though it can pose challenges to consumers and financial institutions, in part because consumers may not fully understand what data is being shared.

Alternatively, APIs are a set of instructions that allows two systems or computers to "talk" to each other over a network. There are different models of API frameworks depending on the participants and data access purposes. While some participants might need to access data for read-only (e.g. account information service providers) others might need read and write access (payment initiation service providers). API standards provide specifications (e.g. architecture, format, documentation, versioning) allowing participants to share data in a uniform way that is understood by all parties. This approach requires investment by financial institutions to develop programming interfaces that third-party providers and consumers can use to access data, and by design limits data sharing to what is allowable under the API specifications (which has both benefits and challenges).

Many jurisdictions have now begun to explore open banking in terms of their domestic payment systems. Singapore has adopted an approach towards open banking enabling banks to share data with financial technology and other non-bank firms without enacting legislation. The Banking Act and the Personal Data Protection Act remain the primary statutes regulating banking data in Singapore. The Monetary Authority of Singapore (MAS) has collaborated with the Association of Banks in Singapore to release non-binding guidance on developing and adopting open API-based system architecture.

The Australian Consumer Data Right (CDR) is an economy-wide framework, which allows consumers to consent to securely share data that designated data holders (such as Authorised Deposit-taking Institutions) hold about them with accredited third parties. Data holders and accredited third parties are mandated to comply with the data-sharing rules and standards. Open banking in Australia commenced through the CDR in July 2020, and the CDR expanded to the energy sector in 2022. The Australian Government has introduced legislation into the Parliament to extend the CDR to action initiation, which would enable consumers to instruct accredited third parties to initiate actions, such as payments, on their behalf. The Australian Treasury is undertaking detailed policy and design work on action and payment initiation, focusing on building a strong foundation for future implementation and identifying the highest-priority actions for Government to bring into the CDR to maximise consumer benefits.

In India, the open banking regulation enables third party access to customer-permissioned data, requiring licensing or authorisation of third parties, and implementing data privacy and disclosure and consent requirements. The Reserve Bank of India licenses an Account Aggregator to consolidate financial information of a customer held with different financial entities, based on an explicit consent of the customer.

3.5. Broader alignment and interoperability between data frameworks

Official Sector: One authority recommended more bilateral frameworks in the short-term to facilitate cross-border data flows which among other benefits, could enable effective AML/CFT monitoring. Long-term, a multilateral framework for cross-border data to harmonise rules and standards could be helpful, e.g. the OECD Privacy Guidelines. Another respondent highlighted that common principles and/or agreements between such authorities could be set to address this issue.

Private Sector*:* Beyond concerns solely between AML/CFT and data privacy compliance obligations, industry stakeholders stressed the need to holistically address the range of conflicts among data frameworks applicable to cross-border payments at the international level. Some suggested that international alignment in data principles or data frameworks was a pre-condition to achieving the Roadmap, which could include establishing a minimum set of data that needs to be included when sending a cross-border payment. One stakeholder suggested that this could be accomplished through a framework specific to payments, that would balance between the many

data framework requirements applicable to cross-border payments. Stakeholders also supported more regional and bilateral efforts, including trade agreements and non-binding joint statements, similar to the US-Japan Digital Trade Agreement[22] and the Australia-Singapore Digital Economy Agreement[23]. One stakeholder suggested that standard "gateways" or exceptions to data barriers be established to clarify the circumstances when authorities and financial institutions may make disclosures, and that these gateways could be tailored to business-to-business, business-to-government or government-to-government use cases.

Participants considered this area as an opportunity for the FSB to engage with regulators and consider a whole of government approach to data frameworks. This engagement could be helpful in allowing all national authorities to understand the different actors in a payment chain and the impact of their polices and laws on the financial sector. Some stakeholders encouraged the FSB to engage on specific areas of friction, including data localisation. One stakeholder suggested that the FSB produce a comprehensive list of data requirements applicable to payments, to help identify frictions and assist with international compliance.

Box 5: Promoting cross-border data flows

Regulatory differences in data frameworks across jurisdictions may be fully justified, for example due to different national strategic priorities and values. However, effective cross-border payments rely on access to data residing in more than one jurisdiction. In the absence of a globally accepted standard on cross-border data flows, some regional efforts and multilateral initiatives could provide guidance on key elements for a cross-border data flows framework. Additionally, several approaches in the financial sector may serve as some roadmap.

The concept of 'data free flow with trust' was also launched by heads of governments under Japan's G20 Presidency in 2019. The G7 under the UK's Presidency in 2021 agreed to four areas for cooperation on data free flow with trust (DFFT). In January 2022, while assuming the G7 Presidency, Germany prioritised the goal to promote DFFT across borders, following from work done under prior G7 years.

The World Economic Forum Roadmap[24] is shaped along six elements for economies that voluntarily want to follow the roadmap including: (i) allow data flow by default instead of including unjustified data localisation rules, (ii) establish a level of data protection, (iii) prioritise cybersecurity, (iv) hardwire accountability between nations, (v) prioritise connectivity, interoperability, data portability and data provenance and (vi) future-proof the policy environment.

On 29 September 2021, the United Nations Conference on Trade and Development (UNCTAD) in the Digital Economy Report[25] pointed out that the international debate on the governance of cross-border data flows is at an impasse due to diverging views and positions on their regulation. In order to overcome this problem, UNCTAD proposed the formation of a new United Nations multilateral, multi-stakeholder and multidisciplinary body with the skills for developing a new global data governance approach capable of delivering middle-ground solutions.

Financial authorities have come up with a variety of mechanisms to promote data sharing among government authorities. On the multilateral front, the Egmont Group, the International Organization of

---

22 Office of the United States Trade Representative (2019), Agreement between the United States of America and Japan Concerning Digital Trade, October.

23 Australian Department of Foreign Affairs and Trade (2020), Australia-Singapore Digital Economy Agreement, December.

24 World Economic Forum (2020), *A Roadmap for Cross-Border Data Flows: Future-Proofing Readiness and Cooperation in the New Data Economy*, June.

25 UNCTAD (2021), *Digital Economy Report 2021*, September.

Securities Commissions (IOSCO's) multilateral memoranda of understanding (MMoUs), supervisory colleges and crisis management groups all serve as examples of data sharing among regulatory authorities. In addition, banking, securities and insurance regulators have all established broad networks of bilateral memoranda of understanding. In 2020, under the U.S. G7 Presidency, Finance Ministers and Central Bank Governors discussed the issue of cross-border data flows in financial services, noting the various public policy objectives, like risk management, fraud detection, AML/CFT compliance and financial stability, were furthered by cross-border data flows.

4. Next steps

The FSB has identified a series of significant issues warranting further attention, both by financial authorities and non-financial authorities with responsibilities for data frameworks. In conducting this assessment, the FSB received many suggestions that could help address these frictions. Some are more complex than others and some are not within the sole remit of financial authorities. It should also be noted that some frictions may be legitimate and necessary consequences to achieving other public policy objectives.

As set out in the Roadmap, the next phase of the FSB's work is to identify recommendations, in cooperation with other stakeholders and subject to public consultation, which could address impediments identified in this stocktake. Several suggestions for improvements are already under consideration in the cross-border payments Roadmap. Any recommendations, therefore, will need to be coordinated with other building blocks of the Roadmap.[26] Industry stakeholders stressed that frictions needed to be addressed through alignment of frameworks to enable authorities and industry stakeholders to achieve the goals of the Roadmap. Options for implementing the next phase of this work include:

- Comprehensively mapping differences in approaches requiring bespoke or manual solutions that affect cost, speed, transparency, or access (e.g. differences in messaging or document protocols, wire transfer rules).
- Assessing the impact of selected frictions on cross-border payments, for example through case studies, to identify where action should be prioritised.
- Determining if alternative approaches can be recommended, that would address frictions while preserving appropriate policy outcomes, particularly for policies designed to achieve regulatory and supervisory oversight.
- Identifying and recommending appropriate steps to encourage alignment and interoperability of data frameworks applicable to cross-border payments, including data privacy, operational resilience, AML/CFT compliance, and regulatory and supervisory oversight data access. As alignment and interoperability should not compromise necessary and appropriate policy objectives, such efforts could include coordination with cross-sectoral authorities as necessary, as part of a holistic consideration of the objectives of the Roadmap, the functioning of the cross-border payments system, and the underlying objectives of applicable data frameworks.

[26] This includes the building blocks on common features of Service Level Agreements, AML/CFT rules, KYC and information sharing, adopting a harmonised version of ISO 20022, and establishing unique identifiers.

Annex 1: Respondents to the FSB survey

(Survey was conducted in 2021)

Jurisdiction	Agency
Argentina	Central Bank of Argentina National Security Council
Australia	Department of the Treasury Australia Prudential Regulatory Agency Australian Transaction Reports and Analysis Centre Attorney-General's Department Digital Transformation Agency Office of the Australian Information Commissioner
Brazil	Banco Central do Brasil
Canada	Government of Canada
China	People's Bank of China
EU	European Commission
France	Banque de France
Germany	Ministry of Finance Deutsche Bundesbank Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)
Hong Kong	Hong Kong Monetary Authority
India	Ministry of Finance
Indonesia	Bank Indonesia
Italy	Banca d'Italia Ministry of the Economy and Finance
Japan	Financial Services Agency
Korea	Financial Services Commission
Mexico	Banco de Mexico Comisión Nacional Bancaria y de Valores
Netherlands -	De Nederlandsche Bank
Russia	Central Bank of Russia
Saudi Arabia	Saudi Central Bank
Singapore	Monetary Authority of Singapore
South Africa	South African Reserve Bank
Spain	Bank of Spain
Switzerland	Swiss Federal Department of Finance
Türkiye	Central Bank of the Republic of Türkiye
UK	Financial Conduct Authority
US	Department of the Treasury Federal Reserve Board Office of the Comptroller of the Currency

Annex 2: Summary of the stocktake of FSB members

This annex presents findings from the survey of existing national and regional data frameworks relevant to the functioning, regulation and supervision of cross-border payment arrangements, and to identify issues relating to cross-border use of those data by national authorities and by the private sector. The survey was conducted in 2021.

FSB members were then asked to summarise the objectives of the framework and discuss aspects relevant to cross-border payments, particularly those that affected cost, speed, access or transparency. Finally, the stocktake asked FSB members to (1) identify any areas where data frameworks could be improved to reduce frictions, (2) discuss current or future initiatives for these frameworks and (3) provide information on cross-sectoral cooperation or cross-border cooperation mechanisms and relevant areas for improvement.

Categorisation

Respondents were also asked to identify the intended policy objectives of the framework, from the following list. A single framework could fall under multiple policy objectives, if relevant.

- Data privacy frameworks;
- Data considerations for anti-money laundering and counter-terrorism financing (AML/CFT) purposes;
- Data considerations for risk management, including cybersecurity and operational resilience;
- Data management requirements (retention, deletion, localisation, consent, onward sharing);
- Cloud/third-party services and any interactions that may arise from those;
- Data frameworks pertinent to digital IDs, including LEI; and
- Data frameworks pertinent to open banking frameworks.

The most commonly reported measures were related to (1) data frameworks relevant to AML/CFT requirements; (2) data considerations for risk management objectives, including cybersecurity and operational resilience; (3) data management requirements; and (4) data privacy requirements. The least commonly reported measures were related to emerging topics, including open banking frameworks, digital IDs and cloud/third-party services.

Measures by applicable entity

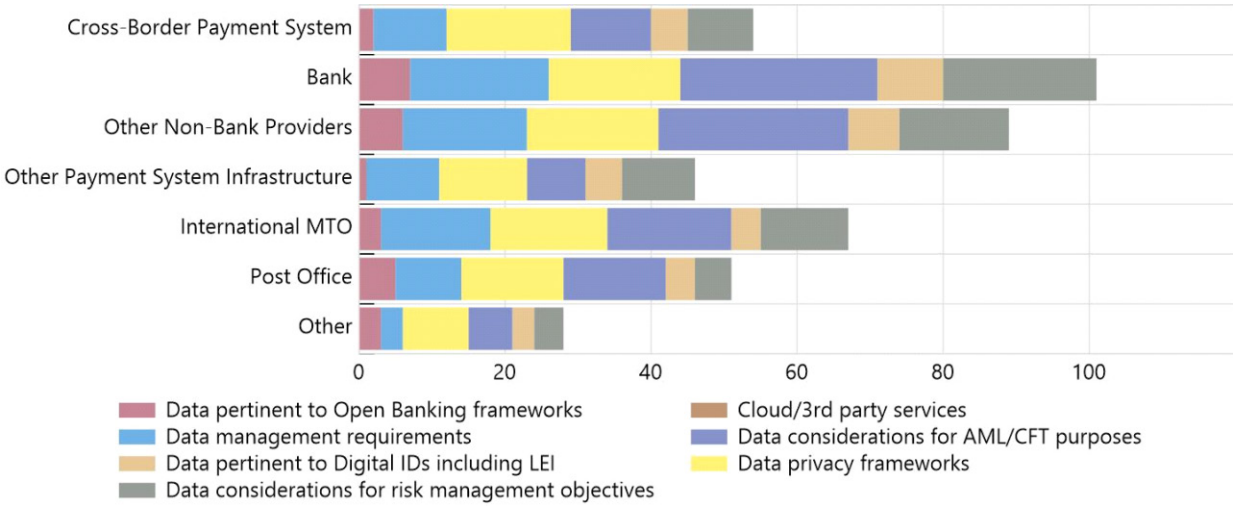
Graph A1 shows that measures were most commonly applicable to bank providers (over 100), followed closely by non-bank providers and international Money transfer operators (MTOs). “Other” entities to which measures applied varied based on the policy objective:

- In the case of data privacy frameworks, “other” often included government authorities or non-financial companies.

- In the case of data considerations for AML/CFT purposes or risk management, “other” could include non-financial professions or specially designated financial companies.

  In the case of cloud and third-party requirements, “other” could include the providers of services to financial institutions.

Measure applicability, by provider **Graph A1**



Source: Survey responses

Measures by competent authority responsible for implementation

Though central banks and financial regulators are often solely responsible for a measure, the stocktake identified other authorities that could have primary authority for implementation. Competent authorities responsible for implementation often varied depending on the framework, as shown in Graph A2:

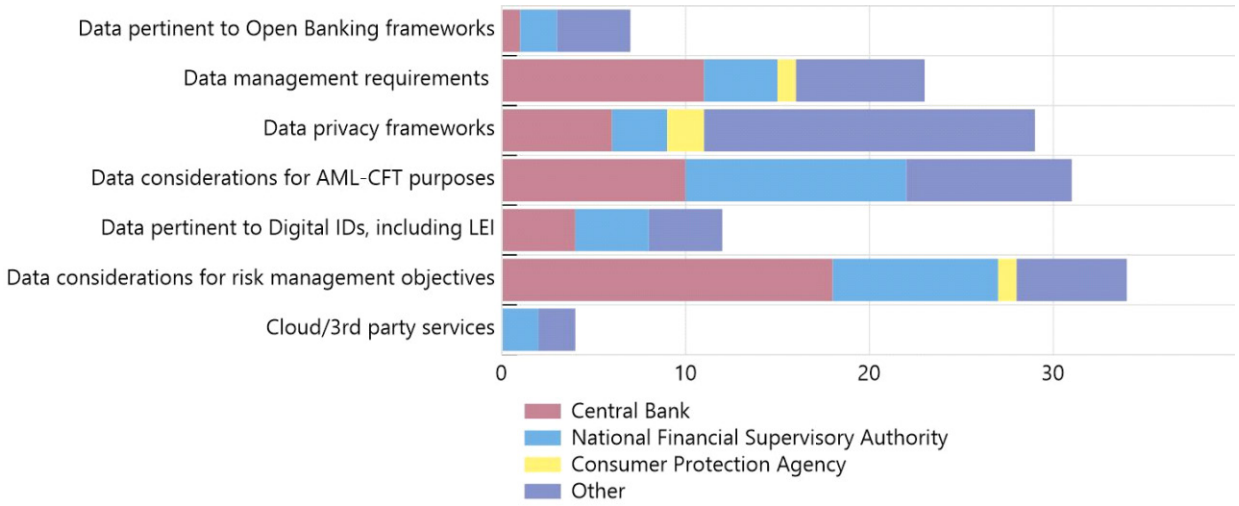
- In the case of data privacy frameworks, data protection authorities were often reported as the competent authority.

- In the case of measures relevant to AML/CFT requirements, ministries of finance and financial intelligence units were reported as a competent authority.

- In the case of cybersecurity requirements, national cybersecurity agencies were reported as a competent authority.

This indicates that in certain instances, engagement with non-financial authorities may be necessary to effect changes that the FSB may recommend.

Measures by competent authority responsible for implementation **Graph A2**



Source: FSB survey responses

Cross-sectoral cooperation

The survey asked FSB members to identify existing cross-sectoral cooperation mechanisms relevant to the identified data frameworks within their jurisdictions.

- Japan and Singapore highlighted cooperation between financial regulators and data protection authorities on potential personal data breaches.
- Saudi Arabia and the United States highlighted cooperation among financial authorities in regard to operational or cyber events.
- Spain, Switzerland, and Türkiye highlighted cooperation between financial regulators and cybersecurity authorities.
- Australia highlighted joint work between the Australian Department of the Treasury, the Australian Competition and Consumer Commission, and the Office of the Australian Information Commissioner to implement legislation related to the Consumer Data Right.

Cross-border cooperation

FSB members were also asked to identify existing cross-border cooperation mechanisms relevant to the identified data frameworks. Responses were more limited. Some respondents identified regional and bilateral engagement on open data and data portability, collaboration on sandboxes and interoperability, existing working groups at the FSB and SSBs on cyber resilience, adequacy assessments of foreign jurisdictions' data privacy requirements and mutual legal assistance around issues related to financial crimes.

Types and examples of measures

Data considerations for AML/CFT purposes[27]

The most common frameworks cited included:

- Implementation of FATF Recommendation 16 on wire transfers.
- National AML/CFT laws, noting additional requirements for customer due diligence and enhanced monitoring of cross-border correspondent.

Two authorities further noted potential requirements for data necessary to sanction/freeze relevant assets in order to combat the financing of terrorism.

This category of measure that had the highest proportion of requirements that were cross-sectoral, i.e. applicable to more than one segment of the financial sector. Some authorities noted that requirements were risk-based. Authorities also discussed the specific information that may be required to be collected and retained, including originator and beneficiary information on cross-border payments.

Data considerations for risk management objectives, including cybersecurity, operational resilience

The most common frameworks cited included:

- Requirements for how financial institutions manage data security and operational risks, including high-level principles asking firms to identify relevant information assets and implement security controls.
- Cyber incident reporting requirements, with respect to reporting either to the financial supervisor or to the relevant cybersecurity authority.
- General frameworks for payment service providers, including the EU's PSD2, which was also identified as a data management and open banking framework, or Canada's Retail Payments Oversight Framework (RPOF),[28] a new regulatory regime being developed to oversee retail payments.

Data management requirements (retention, deletion, localisation, consent, onward sharing)

Authorities identified a wide range of policies as data management requirements, which can be informally subdivided into the following categories:

---

27 See Box 1 for a summary of FATF's work on harmonisation of AML/CFT and KYC requirements among countries.

28 Bank of Canada, About the retail payments supervisory framework.

Data standards and interoperability

- Standards for how credit transfers and direct debits must be processed, as well as aspects of the PSD2 covering information disclosure in international payments.
- ISO 20022 Technical Standards, which govern the generating and reading the messages that form the basis of electronic transactions and ensure a standardised transfer of data (See Box 3 for description).

Requirements for regulatory and supervisory purposes

- Data retention requirements for records though respondents did not indicate whether the recordkeeping needed to be kept in-country and could not be transferred to other jurisdictions.
- Data localisation requirements for regulatory and supervisory purposes.

Requirements implicated by other frameworks, e.g. data privacy

- Frameworks that impose sharing restrictions on credit data with third parties.
- Data management requirements arising out of data privacy frameworks.

Frameworks allowing the transfer of cross-border data

- Commitments under relevant trade agreements, such as the United States-Mexico-Canada Agreement,[29] and the Comprehensive and Progressive Agreement for the Trans-Pacific Partnership (CPTPP),[30] which prohibit measures that prevent the transfer of financial information.
- Commitments under non-binding arrangements, such as the United States-Singapore Joint Statement on Data Connectivity.[31]

Data privacy frameworks

Frameworks primarily included economy wide data privacy laws. Some authorities noted principles or sector-specific requirements. These frameworks often address notice to consumers of how data is processed and shared, and in some cases impose requirements before data can be transferred across borders. Some responses also identified that data privacy requirements can impose data security requirements to safeguard personal data. This policy requirement was by far the most cross-sectoral in nature, and often involved non-financial authorities such as national data protection authorities.

---

29 Office of the United States Trade Representative (2020), United States-Mexico-Canada Agreement, July.

30 Australian Government Department of Foreign Affairs and Trade (2018), Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), March.

31 US Department of the Treasury (2020), United States-Singapore Joint Statement on Financial Services Data Connectivity, February.

Data frameworks pertinent to digital IDs, including LEI

Digital ID frameworks identified largely fell into two categories:

- National requirements related to the LEI or other type of unique.
- National initiatives to develop digital identity.

Data frameworks pertinent to open banking frameworks[32]

Reported open banking frameworks included sector-specific open banking frameworks, as well as economy-wide open data frameworks such as Australia's Consumer Data Right.[33] Features of these frameworks include whether they are read-only or allow providers to initiate transactions, access through APIs, and security requirements such as strong customer authentication. Other authorities noted their intent to consult on such frameworks, or that they had adopted a market-based framework.

Cloud/third-party services and any interactions that may arise from those

Responses focused on financial institution requirements on outsourcing and the use of third-party services, which often focused on data security and data privacy requirements.

Impact of measures on provision of cross-border payments

In general, only a limited number of responses provided an assessment of the impact of these frameworks on the provision of cross-border payments. Some authorities pointed to theoretical impacts on cross-border payments or the supervision of financial entities based on potential increased costs, or benefits to resilience or regulatory access, though noting that it is difficult to quantify or assess the relative degree of potential impact of these frameworks. Many authorities pointed to proportionality as a key aspect of their frameworks. In some areas, there was a high degree of thematic consistency in approaches and assessment, but in the area of data management requirements, some jurisdictions took different approaches and, as a result, assessed the impact of the policy differently. Authorities, where they did provide responses, focused on the impact of their own measures on end-users in their own jurisdiction. The working group is hopeful that further stakeholder input will provide insight on impacts not captured through the stocktake, including:

- Cross-border spill-overs from one jurisdiction's framework to another, e.g. through regional payment corridors;
- The impact of any policies not captured in the FSB-member-only survey, e.g. EMDE policies that may be under-represented;

---

32 See also Box 4.

33 See Australian Government Consumer Data Right

- How existing data frameworks might interact with future actions financial authorities may undertake to improve the cost, speed, access, and transparency of cross-border payments.

The FSB will also consider what further analysis it can itself do to explore these issues within its own membership.

A summary of impacts based on policy type are below.

Data considerations for AML/CFT purposes

Several authorities noted awareness that data retention for implementation of FATF Recommendation 16 (on wire transfers) or other FATF Recommendations was not being implemented consistently or on an interoperable basis across jurisdictions. But other respondents do not believe that this impacts cost, speed, availability, or transparency of payment services.

Data considerations for risk management objectives, including cybersecurity and operational resilience

A number of authorities noted that requirements with the objective of risk management could increase costs, although two jurisdictions noted that the effect might be limited because the requirements did not apply to cross-border payment systems/networks like SWIFT. Some authorities noted that these measures have benefits through improved resilience of payment systems. One authority noted that these measures are important for maintaining the safe transfer of data between supervisor and supervised entity and protecting against data breaches.

Data management requirements (retention, deletion, localisation, consent, onward sharing)

Authorities provided a wide range of views on the impact of data management requirements.

Data standards and interoperability

One jurisdiction highlighted that there was convergence and growing market adoption of interoperable technical standards (e.g. ISO 20022). Some jurisdictions highlighted the benefit of the EU's PSD2 and SEPA regulations on credit transfers but noted frictions with how these standards were applied when only one leg was within the EU.

Requirements for regulatory and supervisory purposes

Authorities with these requirements noted that they could increase costs to payment service providers but did not believe that they had an effect on cost to end-users, or on access and speed. One authority assessed that these requirements would improve transparency in the event of a stress scenario at a financial institution.

Frameworks promoting the transfer of cross-border data

Some authorities assessed that these frameworks, including those that prohibit data localisation and other impediments to cross-border data flows, could have positive impacts on cost and speed, and aid in the ability of entities to comply with regulatory and supervisory requirements and improve the ability to detect fraud and perform other risk management and mitigation.

Data privacy frameworks

Most authorities did not provide an assessment of potential impact of data privacy requirements. Some authorities did note that data protection requirements may lead to greater cost and reduced speed for cross-border payments, noting compliance requirements. Some authorities noted that their frameworks could increase compliance costs, but did not assess that there would be a material effect on frictions in cross-border payments.

Data frameworks pertinent to digital IDs, including LEI:

No authority noted any impact from digital ID frameworks on cross-border payments. Some authorities noted that this is because they were not directly related to or being used in cross-border payments. One authority reported that if the LEI were to be more widely adopted and used in cross-border payments, efficiency (i.e. cost or speed) could improve, citing the CPMI's Stage 2 report on the cross-border payments Roadmap.[34]

Data frameworks pertinent to open banking frameworks:

Some authorities assessed that open banking could improve domestic market efficiency, cost and/or transparency and that there was the potential to also improve the efficiency of cross-border payments.

Cloud/third-party services, and any interactions that may arise from those:

Only one authority provided an assessment of their framework in this area, focused on its domestic application. While the framework did not exclude cross-border payments, they noted that it would be difficult to assess the specific impact on cross-border payments. One authority noted that they had received industry feedback that greater use of cloud services for data processing could improve cost or speed of cross-border payments.

[34] CPMI (2020).

Annex 3: Summary of industry written feedback responses

This annex presents findings from the informal request for written feedback from private sector stakeholders. The written feedback period lasted from early December 2021 to mid-January 2022 with a similar call on the FSB's website as a request for public input.[1] The FSB received 30 responses to the consultation which ended on 14 January 2022 with a small number of late responses after this date (6 respondents provided anonymous responses through the online survey). Identified respondents comprised: regulated financial institutions [6], trade associations representing payment industries [3], non-bank payment service providers [6], private financial market infrastructures [5], messaging network providers [2], others [2].

Summary of responses to consultation questions

Overarching comments:

- A number of commentors noted that the technology to deliver on the Roadmap exists, but regulatory challenges are a key barrier. Respondents noted that the wide range and complexity of existing data frameworks too frequently require manual solutions, impacting cost, speed, and access. Several respondents stated that resolving these disparate frameworks is important, if not a pre-condition to the Roadmap's success, and urged greater harmonisation in data frameworks applicable to payments.

- Commentors cited the need to harmonise data privacy, AML/CFT, cybersecurity, outsourcing and regulatory and supervisory requirements within and across borders.

- Policies that result in data localisation, or otherwise restrict the flow of cross-border data were frequently highlighted as a significant issue impacting payments processing, exception handling, cybersecurity, fraud detection and AML/CFT compliance. Many participants argued that it affected the speed and cost of payments.

- Differences between local data frameworks often result in high costs attributed to the costs to understand and implement solutions to similar, but different requirements, or in situations where requirements are not clear or less developed, or operational costs to implement technical solutions. Several responses noted the difficulty in building technical solutions for messaging requirements to AML/CFT compliance and sanctions screening.

- GDPR in the EU was mentioned as being effective in setting requirements regarding circumstances in which personal data can be processed and by whom and therefore providing certainty and clarity to various actors in the payment chain. Despite support for GDPR-like harmonisation, some commenters expressed concern regarding discrepancies in its implementation and the potential impact on the exchange of payments data, or noted that it could present challenges to processes like upfront payment validation.

- Many participants urged greater international cooperation to address these issues, and that the FSB should take steps to promote convergence in data frameworks applicable to cross-border payments.

1. **How, in your view, do data-specific requirements or objectives of existing national and regional data frameworks, such as those listed above, currently affect (either positively or negatively):**

   a) **the cost and speed of delivering payments,**

   b) **access and transparency (e.g. through compliance costs or through measures enabling or reducing competition) and**

   c) **other aspects that affect the delivery of, or regulatory compliance with respect to, cross-border payments?**

- Commentors noted the importance of data frameworks for a wide range of regulatory objectives, including data privacy, data security and AML/CFT compliance. One respondent noted that "implementing consistent, principles-based, risk-based, horizontal privacy frameworks at the regional and national levels can create the right conditions for data sharing across a region, leading to regional economic growth and harmonised privacy protections for consumers, while helping to reduce friction, reduce cost and increase speed in the cross border payments landscape."

- Many commentors noted the lack of a global harmonised framework across policy objectives results in bespoke requirements that makes developing a more efficient system of cross-border payments difficult, and that an appropriate balance must be struck.

- AML/CFT and privacy issues were highlighted as a top issue, as a lack of legal and regulatory harmonisation of AML/KYC requirements leads to excessive diversity in data retention and transfer requirements for compliance. Some respondents urged for international cooperation to address conflicts related to AML/data protection legislation. In particular, technical challenges were noted with exception handling, payment reconciliation, and transaction screening.

- ISO 20022 was frequently welcomed as a solution in transmitting data in a more structured manner, though one commentor noted that it would still allow for too much variation, and that external pressure was needed to harmonise all means of payments, and another commentor noted issues with interoperability with jurisdictions that did not adopt the standard.

- Commentors also noted the benefits of regional regulatory requirements like GDPR, SEPA and PSD2 in the EU, though some noted that even within these frameworks they continue to face challenges that should still be addressed. For example, frictions within SEPA may arise from divergences between national or regional AML/CFT and data protection regimes, while other respondents cautioned that diverging interpretations of the mandatory provisions of GDPR by national data protection authorities in the EEA may hinder the efficient and effective exchange of certain payment and payment-related data, notably in the context of cyber security and combatting fraud.

- Respondents highlighted a broad range of policy barriers to the use of cross-border data, the resulting impact on payments and financial services, and the need for further clarity on these policies.

- GDPR was highlighted as an important framework that focused on data rights, noting that "the European Union's General Data Protection Regulation (GDPR), which seeks to have a progressive and comprehensive approach to data protection, serves as an illustrative example of a regulation that does not have any data localisation requirements." Though several jurisdictions noted challenges associated with GDPR's interaction with third-countries.

- Commentors also noted perceived differences in data requirements for different types of payments transactions (card payments versus bank transactions).

2. **More specifically, what barriers to cross-border use of data do you see in existing data frameworks that will impede our ability to address the four challenges faced by cross-border payments?**

    - Data localisation requirements were seen as a barrier to the cross-border use of data, causing friction for businesses that operate in multiple jurisdictions. Respondents noted that the adoption of data localisation frameworks increases the overall operating costs faced by firms whose operations span borders, which necessarily includes the majority of institutions supporting cross-border payments.

    - Some commentors also noted that a wide range of policies, including data mirroring and regulatory consent requirements had many of the same effects as data localisation. Many digital finance, fintech, and mobile payment firms are using cloud technology to deliver their services, detect fraud, and improve operations. Policies that restrict outsourcing arrangements often result in the de facto localisation of data onshore, which deters firms from entering or expanding in a market, undermining economic growth and disadvantaging local consumers.

    - Respondents suggested that data privacy requirements might impede the implementation of means to achieve more reliable payments settlement and reduce payment rejections, including payments pre-validation, Confirmation of Payee, or similar initiatives that require data to be exchanged before a payment is consummated.

    - A lack of harmonisation among payments frameworks and consistency in the implementation of data protection requirements acts as a barrier to cross-border payments or will result in the duplication of systems and processes. For example, commenters noted that wherever local legislation imposes specific requirements on the inclusion of data in a payment message that is not standardised cross border, there will, inevitably, be impacts on the ability of payment service providers to meet enhanced expectations for cross border payments. The lack of generalised adoption of IBAN and inconsistent usage of LEIs also add complexity and cost to cross-border payment processing.

    - Several responses noted the challenges in adhering to sanctions screening, and the fragmentation between technical requirements. Batch payments between operators and payments without full information exacerbates this challenge.

    - Bespoke additional payments requirements make it difficult to automate, and if not included, will cause payments to be rejected. Examples include:

        - Required documentation for tax payments, invoices, utility payments

- Inclusion of reason for payment
- Local identification/tax identification numbers, residency, legal status of the customer, no initials in beneficiary name
- Replacement of @ with AT
- Specific account number formatting
- Non acceptance of P.O. Box numbers

3. **What areas of improvement could you suggest in data frameworks in order to overcome these barriers? Are there effective practices you would highlight to the FSB membership?**

- Respondents suggested that global alignment of frameworks, standards and regulations will be most helpful in overcoming the challenges regarding data frameworks. Some commentors suggested that this could be addressed through a payments-specific data framework. One commentor suggested the development of standardised exceptions for B2B, B2G and G2G transfers.

- A number of commenters urged principles-based rules in achieving harmonisation among data frameworks noting that "the development of principles-based data frameworks, which can effectively achieve policy objectives and address potential risks, while also keeping pace with innovation and prioritizing an open, level playing field. Principles-based regulatory frameworks should be underpinned by robust, globally interoperable and internationally recognised technical standards."

- High quality digital trade agreements that facilitate cross-border payments by enabling cross-border data flow were supported by many respondents. Identifying common principles among various data privacy frameworks, or focusing on reciprocal adequacy agreements were also seen as potential solutions.

- A number of recommendations were suggested relative to AML/CFT requirements, including:
  - Resolve conflicts between AML/CFT and data privacy legislations so that companies do not breach one regulation when complying with the other. Clarify legal requirements relating to what data is required to be collected and the instances in which it should be shared with law enforcement;
  - Produce clear rules on electronic customer due diligence/KYC;
  - Clarify requirements related to funds transfer reporting;
  - Prioritise harmonizing requirements concerning AML/CFT information sharing; and,
  - Secrecy and privacy laws should not inhibit the reporting of suspicious activity.

- Many commenters proposed achieving further standardisation in payments requirements like clearing formats, possibly by exporting regional frameworks. One commenter noted that "SEPA is an example of multiple countries adopting a single set of standards based on regional legislation. If the regional model was extended to other

communities, wider harmonisation of payment practices could be expected, which could help bring down costs, improve access, increase speed and improve transparency."

- Some commentors on the other hand, noted challenges when regional frameworks were not globally adopted, noting that it could be a source of friction or impede the development of efficient global payment networks.

- Preferred approaches to data restrictions should focus on access and use; authorities should consider encryption requirements as an alternative means of assuring control of data. Regulatory data access arrangements and intergovernmental agreements could also help address regulatory and supervisory issues.

- Several respondents recommended the global adoption of messaging standards such as ISO 20022, mandating the use of IBANs, and introducing a requirement for the universal global adoption of the LEI regime for correspondent banking, namely a unique global identifier for legal entities participating in cross-border payment transactions. Others suggested that a number of issues could be solved through developing an interoperable system of digital identity.

- Several commenters identified key roles for the FSB. For example, one commenter said, "we suggest the FSB study and provide a public summary of different national and regional data privacy and protection laws and how they apply to payment providers that send and receive payments in key corridors and service providers that provide services to mitigate fraud and compliance risks related to payments."

- Another role for the FSB could be to conduct an inventory of existing requirements, noting that "although there have been prior studies and assessments to quantify the impact of data localisation requirements, the plethora of restrictions on data flows across jurisdictions has grown rapidly, making it suitable and appropriate for the FSB to complete a comprehensive inventory of existing requirements and assess their impact on cross-border payments and how they may exacerbate current challenges in cross-border payments. The FSB could then focus its efforts on harmonisation of and removing cross-border data flow restrictions in restrictive jurisdictions."

- Requiring beneficiary name, city, and country as mandatory information for payments could help facilitate sanctions screening.

- Implementing approaches to Confirmation of Payee (CoP) could reduce payments fraud. However, data privacy issues are often raised and may serve as a barrier.

4. **Can approaches to data frameworks in one jurisdiction impact the provision or supervision of cross-border payments services in other jurisdictions? Are there particular issues that you would like to highlight?**

   - Many commenters agreed that approaches to data frameworks in one jurisdiction could impact the provision or supervision of cross-border payments services in other jurisdictions. One commenter noted that "with different data frameworks and requirements in different jurisdictions, there is always a mismatch between what data is gathered at the remitting jurisdiction against what data is required at the processing jurisdiction."

- Restrictions on data sharing was raised as a particular issue affecting payments, with a commenter suggesting that "where data frameworks place blanket restrictions on the sharing of important information about the beneficiary or originator of a cross-border transaction, they may prevent information known in another jurisdiction from being used to make a risk assessment about that beneficiary."

- Another commenter noted that, "the cross-border payments ecosystem is interconnected and regulations enacted in one jurisdiction will affect all payments to and from that corridor. Today we see that a frequent cause of payment delays is due to requirements to comply with complex regulations and exchange rate controls, not the speed of the payments infrastructure itself or interbank models. The technology used to facilitate cross-border payments within the interbank SWIFT model for example is very fast, with most payments being settled end-to-end within 1 hour. Payments that take longer tend to be due to either issues with opening hours or regulatory requirements."

5. Are there particular payment corridors (especially related to emerging markets) that you wish to highlight to the FSB as facing specific challenges relating to data frameworks?

- While the GDPR was cited as a potential model for framework harmonisation, some commenters cited challenges, noting that in Europe the GDPR makes cross-border data transfer difficult because of the stringent requirements that must be met before data can be transferred to third countries. The European Commission has the power to determine whether a country outside the EU offers an adequate level of data protection. It has so far recognised a limited number of countries (including Argentina, Israel, Japan, New Zealand and the UK). Key trading nations that are likely to generate substantial cross-border payment flows, such as India, China, Mexico and the US (not an exclusive list) are not (currently) recognised.[35] Diverging interpretations in the mandatory provisions of GDPR by national data protection authorities may hinder the effective exchange of payment-related data between payment providers, notably in the context of cyber security and combatting crime.

- A number of survey respondents noted country-specific payment frictions or barriers in the following areas:

  - Australia: Rules requiring maintenance of personal information locally, rules requiring banks to make an assessment that the data privacy law of offshore jurisdictions are equivalent to Australia's.

  - Bangladesh: draft guidelines propose cloud use restrictions and AML regulatory approval for cross-border data sharing.

  - Brazil: Challenges in payments to Brazil, although currency use is limited.

[35] Although Mexico is not yet recognised by the EU as offering an adequate level of data protection, Mexico has acceded to the Council of Europe Convention 108 which is comprised of 46 members, including all 27 EU states.

- China: For personal remittances, the need to send the beneficiary's name mandatorily in Mandarin and adherence to annual compliance limit per individual without any visibility on either.
- India: One country that is highlighted frequently is the India payment corridors whose required supporting documentations continue to impact the process leading to long delays of payments.
- Indonesia: Mandating domestic payment processing and personal data protection bill contains localisation provisions treating financial data as sensitive.
- Korea: Information processing system must be in Korea where PII and personal credit information is being processed.
- Lithuania: Very specific differences in the interpretation of data protection and AML requirements. For example, driving licenses are not valid ID for AML purposes in Lithuania, but they are valid ID for AML purposes in many of the countries where customers of Lithuanian entities reside.
- Mexico: Restrictions on contracting outsourcing services. Regulators have long approval times for changes to core banking systems.
- Pakistan: The need to capture the beneficiary's local ID number for the local regulator database is a challenge. Such data requirements are not enforced locally and so additional system alignments are required in order to ensure compliance.
- Russia: Requires payment codes to formatted as {VOxxxx}, has mirroring requirement.
- Saudi Arabia: Measures being put in place to require Data to be stored locally.
- Türkiye: Imposes outsourcing restrictions and requires banks keep primary information systems situated in country, including all backups.
- UK: Post Brexit payment cost transparency for payments to EU.
- Vietnam: Draft decree on personal data requires original data to be kept locally and approval for cross-border transfer of Vietnamese personal data.
- EU: Instances of payments from Uganda/Jamaica being rejected because of EU funds transfer regulation requirements.
- LATAM: Regulators focused on domestic flows without consideration for cross-border flows. Strict FX controls and strong currency controls require manual processes.
- Indonesia, Malaysia, Vietnam, UAE: Provide less clarity / merely state the types of processes that need to be on-shored without providing guidance on the kinds of data that are in scope and even at times the precise definitions of those processes.
- Thailand (in respect of health data) and China.

6. Other feedback relevant to the Cross-Border Payments Roadmap not captured above.

- Financial authorities should consider the implications of exchanging rich data in payments, to a wide set of transactions, like e-invoicing or supply chain financing.

- The move in various jurisdictions across the world to move to an open payment infrastructure is welcomed, often referred to as open finance or open banking. Open banking will only be possible based on clear cross-border legal certainty around data sharing and data portability.

- CPMI could explore the risks and opportunities of data storage developments.

- Some commentors noted perceived differences in the overall regulation of different types of payment providers.

- Several commentors noted that specific currency requirements (i.e. that certain cross-border payments could not be made in certain currencies) were a driving factor behind the complexity of cross-border payments.

- Jurisdictions' ability to request and access data is not necessarily related to the physical location of where the data is stored or processed, but rather depends on the legal framing and governance structures. Therefore, an appropriate legal and governance process around providing access to data to authorities could address authorities' legitimate policy concerns without the very negative effects of local processing and storage requirements.