FSB FINANCIAL STABILITY BOARD

# Recommendations to Promote Alignment and Interoperability Across Data Frameworks Related to Cross-border Payments

Final report

12 December 2024

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

---

Contact the Financial Stability Board

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

# Table of Contents

# Executive summary

The transfer of data across borders is essential to the functioning of the cross-border payments system. Financial institutions, payment service providers (PSPs) and third parties involved in cross-border payments, collectively "cross-border payments market participants" in this report, are subject to a range of laws, rules and regulatory requirements for collecting, storing, and managing data, collectively "data frameworks" in this report. These frameworks relate to the conditions that allow or restrict data handling and its transfer across borders; which data must be stored for regulatory purposes; how data must be secured; what data must accompany an international (cross-border) payment; and technical standards to promote interoperability between bilateral, regional, and international payment networks.

Enhancing the interaction between data frameworks and cross-border payments is a priority action to move forward the G20 Roadmap for Enhancing Cross-Border Payments.[1] The G20 Leaders endorsed the Roadmap at their November 2020 Summit as a means of addressing the challenges that cross-border payments face relative to domestic payments, namely: high costs, low speed, limited access, and insufficient transparency. Greater alignment and interoperability of data frameworks would improve efficiency in transferring payments data across borders and contribute to reaching the Roadmap's targets while improving the safety of payments.

The Financial Stability Board (FSB) took stock of national and regional data frameworks relevant to the functioning, regulation and supervision of cross-border payments.[2] The stocktake identified a number of frictions across data frameworks that pose significant challenges to improving the cost, speed, transparency and accessibility of cross-border payments. A certain degree of friction between data frameworks may be an unavoidable and acceptable consequence of regulations seeking to preserve the security of transactions, meet anti-money laundering and countering the financing of terrorism (AML/CFT) and sanctions objectives, and protect the privacy of individuals. Nevertheless, the stocktake considered the extent of fragmentation in data frameworks across jurisdictions to be a major barrier to enhancing cross-border payments.

Drawing from the findings of the stocktake and following further engagement with government authorities and the private sector, the FSB developed recommendations for promoting alignment and interoperability across data frameworks applicable to cross-border payments. The development of these recommendations has been informed by engagement with the Financial Action Task Force (FATF), the Global Privacy Assembly (GPA),[3] the Organisation for Economic Co-operation and Development (OECD), the Bank for International Settlements' Committee on Payments and Market Infrastructures (CPMI), sanctions experts and a range of financial authorities beyond the FSB's membership. Careful attention has been given to the involvement of authorities beyond the financial services domain, in recognition of the importance of protecting

---

1 FSB (2020), *Roadmap for Enhancing Cross-border Payments,* October; FSB (2023a), *G20 Roadmap for Enhancing Cross-border Payments: Priority actions for achieving the G20 targets*, February.

2 FSB (2023b), *Stocktake of International Data Standards Relevant to Cross-border Payments*, September.

3 The Global Privacy Assembly brings together data protection and privacy authorities from local, national and international levels.

the overarching public policy objectives of the relevant data frameworks. This Report has been revised to reflect the feedback received on its public consultation issued in July 2024.[4]

The recommendations aim to address the identified frictions from data frameworks that pose significant challenges to improving the cost, speed, transparency and accessibility of cross-border payments, while maintaining their safety and security. These include: (i) addressing uncertainty about how to balance regulatory and supervisory obligations; (ii) promoting alignment and interoperability of regulatory and data requirements as well as promoting their consistent and widespread implementation; (iii) mitigating restrictions on the flow of data across borders; and (iv) reducing barriers to innovation. Implemented together, these recommendations should materially enhance data flows for cross-border payments and contribute to progress towards the Roadmap objectives. These actions and best practices include clear legal pathways to transfer payments-related data across borders as well as more effective collaboration among stakeholders involved in payments and in data protection and privacy.

To help ensure that the recommendations are taken forward in a coordinated manner, the FSB, along with its partners, will establish a Forum on Cross-Border Payments Data ("the Forum"). Setting up the Forum responds to strong interest by both the private and public sectors to address unnecessary fragmentation in, and frictions among, data frameworks, as broadly supported by the public consultation. The Forum will be comprised of the diverse set of public sector stakeholders relevant to cross-border payments, including payments, AML/CFT, sanctions, and data privacy and protection stakeholders. The Forum will be charged with coordinating and reporting on the implementation of the recommendations set out in this report and identifying emerging issues that should be addressed. The Forum will also establish a private sector Advisory Group.

Implementation of some of the work related to the recommendations in this report has already begun, including FATF's revision of Recommendation 16 and the adoption of the CPMI's harmonised ISO 20022 data requirements. The recommendations are intended to be the start of a process for jurisdictions globally to identify actions and best practices that would help to foster a more efficient cross-border transfer of payments-related data while respecting public policy objectives around how data are used, stored and secured by the payment industry.

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

# Introduction

In October 2020, the FSB published the Roadmap for Enhancing Cross-border Payments,[5] developed in coordination with the Bank for International Settlements' Committee on Payments and Market Infrastructures (CPMI) and other relevant international organisations and standard-setting bodies (SSBs) to address the four challenges faced by cross-border payments of high costs, low speed, limited access and insufficient transparency and the frictions in existing processes that contribute to these challenges. The Roadmap was endorsed by G20 Leaders.

The FSB, CPMI and partner bodies subsequently identified priority themes to take the Roadmap forward. These included enhancing the interaction between the laws, rules and regulatory requirements for collecting, storing and managing data, referred to as "data frameworks". In support of this priority theme, the FSB conducted a stocktake of data frameworks relevant to cross-border payments and identified a number of frictions arising from these frameworks that pose significant challenges to improving the cost, speed, transparency and accessibility of cross-border payments.[6] The findings of the stocktake have been augmented by FSB engagement with public and private sector stakeholders, including the Financial Action Task Force (FATF), the Global Privacy Assembly (GPA), the Organisation for Economic Co-operation and Development (OECD), the Bank for International Settlements' Committee on Payments and Market Infrastructures (CPMI), sanctions experts, and a range of financial and non-financial authorities beyond the FSB membership.

Based on the cumulative findings of this work, a set of recommendations was developed to promote alignment and interoperability across data frameworks applicable to cross-border payments. While a certain degree of friction from data frameworks may be unavoidable, these recommendations aim to mitigate unnecessary frictions without compromising on the objectives underlying anti-money laundering/countering the financing of terrorism (AML/CFT), sanctions and data protection and privacy rules. Achieving this result would materially enhance data flows for cross-border payments and support progress towards the objectives of the Roadmap and the quantitative targets established under it.

The FSB published the proposed recommendations for public comment in July 2024 and received 34 public comments, including six confidential comments. Respondents included banks, card networks, non-bank payment service providers, financial industry trade associations, private sector entities providing corporate registration services, public sector entities, and data privacy and protection advocacy groups. The responders are geographically diverse, including entities located in the United Kingdom, the United States, Asia, Australia, European Union and Africa. This Report was revised to account for these public comments, where appropriate.

---

5 FSB (2020).

6 FSB (2023b).

The recommendations are in four broad categories:

- **Addressing uncertainty about how to balance regulatory and supervisory obligations.** Cross-border payments market participants[7] encounter difficulties in balancing their various obligations under different data frameworks (e.g. AML/CFT and data protection and privacy), which impedes progress towards achieving Roadmap targets. The recommendations aim to address conflicting requirements and support cross-border payments market participants to navigate different rules.

- **Promoting the alignment and interoperability of regulatory and data requirements related to cross-border payments.** The implementation of rules and standards concerning the data needed to accompany a cross-border payment transaction is not always uniform across jurisdictions. Fragmentation has been observed in the inconsistent implementation of FATF standards, messages and clearing requirements, as well as data requirements to implement sanctions regimes. Recommendations in this area also include promoting the interoperability of data protection and privacy regimes and appropriate cross-border transfer mechanisms for payments-related data.

- **Mitigating restrictions on the flow of data related to payments across borders**. Measures that require data to be stored or processed in-country (data localisation) or require maintenance of the data in the local jurisdiction (data mirroring) can undermine Roadmap objectives. While such data-related requirements may have legitimate public policy objectives, they may also make it more difficult to identify fraud, comply with AML/CFT and sanctions obligations, and manage risk on an enterprise-wide basis. The recommendations aim to open up trusted avenues for the cross-border flow of data related to payments.

- **Reducing barriers to innovation**. Technological innovations that may offer solutions to data frictions could help improve the efficiency of the payments system but appear to be difficult to implement. The recommendation aims to encourage progress on promising innovations and developing frameworks that support public and private sector work.

**Recommendation 1:** The FSB, in collaboration with the OECD, FATF and the GPA, should establish a Forum for collaboration on policymaking, with a view to resolving data framework frictions and facilitating exchanges of ideas and analysis, on cross border payments and related data issues. The Forum would also include relevant stakeholders from international organisations (IOs), SSBs, data protection and privacy authorities (DPAs) and regulatory agencies. The Forum should develop channels for regular engagement with industry stakeholders involved in cross border payments.

[7] An evolving and increasingly diverse set of industry stakeholders are involved in facilitating cross-border payments, including financial institutions, PSPs and third parties. For the purposes of this report, financial institutions include entities such as banks, financial market infrastructure (FMIs) and other entities providing financial services in payments. PSPs are defined as banks and non-banks that are permitted to provide payment services and includes remittance service providers (RSPs), money services businesses (MSBs) and other providers of money or value transfer services (MVTS) as well as providers of prepaid transfers (e.g. prepaid cards or traveller's cheques), pay later transfers such as credit card transfers, and individuals providing payment services, services enabling cash to be placed on or to be withdrawn from an account, the issuing of payment instruments and the acquiring of payment transactions, payment initiation services and account information services. (See also FSB (2024), *Recommendations for regulating and supervising bank and non-bank payment service providers offering cross-border payments services,* December.) Third parties include but are not limited to entities that may be involved in the storage, transmission, analysis or other activity related to data relevant for cross-border payments.

The recommendation to establish the Forum responds to strong interest by both the private and public sectors in addressing unnecessary fragmentation in, and frictions among, data frameworks related to cross-border payments. In light of the broad support received from the public consultation, the FSB has started to work with key stakeholders to develop an appropriate and agile organisational structure and plan for the initial work of the Forum.

The objective of the Forum will be to identify and discuss practical ways of mitigating frictions arising from different approaches to implementing laws, rules and regulatory requirements for collecting, storing and managing payment-related data without compromising on the overarching objectives of such data frameworks. The Forum will support implementation of the recommendations related to data frameworks and will also act as a hub to promote and support the exchange of information and policy research on the intersection of data governance and payment services. This may include, for example, fostering collaboration between domestic authorities, Forum stakeholders, and academic experts, commissioning studies to gather data and insights from experts in the field.

The Forum will identify areas of inconsistency in data frameworks related to cross-border payments and facilitate discussion among authorities on how to mitigate frictions while preserving the security of transactions, meeting AML/CFT and sanctions objectives, preventing fraud and protecting the privacy of individuals. Greater alignment of approaches to data frameworks related to cross-border payments is also essential to support innovation. As described in Recommendation 2, the Forum will also consider a process to ensure that potential newly emerging divergencies and inconsistencies in data frameworks related to cross-border payments in policymaking are identified and addressed.

The Forum will be comprised of public sector experts in payments, AML/CFT, data protection and privacy, and sanctions as well as supervisory and regulatory authorities from FSB and non-FSB members. Coordination *within* and *beyond* the Forum will be critical to its effectiveness. Each organisation that is a member of the Forum would work under its own governance arrangements with respect to possible policy actions but coordination will be ensured among organisations leading the work on a recommendation.

In order to ensure the work of the Forum is informed by the experiences and expertise of cross-border payments market participants, a group of private sector stakeholders will be identified to serve in an advisory capacity to the Forum and, if relevant, to specific working groups.[8] The Forum will make efforts to ensure that the private sector advisory body is composed of representatives of a range of cross-border payments market participants to achieve diversity in terms of geography (extending beyond G20 jurisdictions), size and business model.

[8] The Advisory Group could include participation by existing groups such as the FSB's Taskforce on Legal, Regulatory and Supervisory matters (LRS Taskforce) as well as by other private stakeholders who are not members of the LRS. For additional information on the LRS Taskforce, please see the FSB website.

# 1. Addressing uncertainty about how to balance regulatory and supervisory obligations

Uncertainty among cross-border payments market participants on how to balance the various obligations under different data frameworks was seen as a barrier to achieving the Roadmap targets. Challenges arising from implementation of different data frameworks, including possibly conflicting requirements, are not unique to cross-border payments. Many sectors with a cross-border dimension have been confronted with this issue and have successfully reduced fragmentation and promoted the alignment of regulatory requirements. Examples are the combination of data privacy and protection laws with regulatory frameworks related to international civil aviation or clinical trials and health research, among others. There are similar examples in the payments area, including regional arrangements. Key examples include the Joint Chiefs of Global Tax Enforcement (the J5)[9] as well as payments systems such as Single Euro Payments Area (SEPA) and Buna.[10]

Identifying successful use cases and learning from these experiences may enable them to be replicated as solutions in cross-border payments at a global level.

**Recommendation 2:** Relevant authorities, international organisations and standard-setting bodies should work within the Forum to identify, map and address possible areas of divergence and inconsistency in data frameworks relevant to cross-border payments and facilitate discussion among authorities on how to make these requirements more consistent while meeting AML/CFT and sanctions objectives, preventing fraud, and protecting data privacy objectives. Forum participants should take into consideration successful examples from other areas. The Forum should also consider a process to ensure that new potentially emerging divergences and inconsistencies are addressed as they arise.

Undertaking a comprehensive mapping exercise would be helpful to understand the extent of divergence across approaches to data frameworks affecting the speed and cost of cross-border payments. In addition, the mapping exercise would serve as a resource to provide further clarity on data requirements relevant to cross-border payments in different jurisdictions and would help to identify specific areas where frameworks diverge or conflict. This could serve as a basis for concrete discussions between regulators on how to make requirements more consistent, recognising that some of those differences may be needed due to different risks and contexts prevailing in each jurisdiction. This mapping exercise could be augmented by gathering the guidance that private sector organisations provide to their clients to help them navigate between the various transactional data formats required by jurisdictions. Such guidance helps payees adhere to the required format and provide the right input at cross-border payment initiation. This contributes to reducing the occurrence of payment returns or delays resulting in an overall increase in speed.

Balancing the requirements related to data privacy and protection authorities with AML/CFT rules is an example of the work that could take place under this Recommendation. This issue

---

9 The J5 are committed to combatting transnational tax crime through increased enforcement collaboration. See the Internal Revenue Service website: Joint Chiefs of Global Tax Enforcement.

10 For further information on SEPA and Buna, please see the European Central Bank website: Single Euro Payments Area (SEPA) and the Buna website: The Organisation.

has been repeatedly highlighted by the private sector and confirmed by respondents to the public consultation.

A range of respondents to the public consultation also highlighted the increasing prevalence of fraud in cross-border payments as a significant concern, with broad recognition of the importance of enhancing data flows for use in prevention and detection controls. Regulatory requirements and approaches to fraud prevention may significantly diverge from one jurisdiction to another, which results in adverse impacts on the financial security of cross-border transactions, in a context of heightened fraudulent activity on a cross-border basis boosted by technology and the growing digitalisation of exchanges.[11] Cross-border fraud is a multifaceted issue and the work envisioned to implement the data frameworks recommendations may contribute in many ways to fraud prevention. More generally, sharing best practices and exploring further harmonisation of requirements and approaches to fraud prevention, in balance with the G20 Roadmap objectives, should lead to greater effectiveness in fraud prevention and mitigation at the global level. The FSB and Forum will consider how to respond to this challenge, including which international bodies are best positioned to lead further work.

## 2. Promoting the alignment and interoperability of regulatory and data requirements related to cross-border payments

The 2023 stocktake report highlighted that the implementation of rules and standards concerning the data needed to accompany a cross-border payment is not always consistent across jurisdictions.

The most frequently mentioned friction was divergence in how FATF Recommendation 16 (Wire Transfers) has been implemented by jurisdictions.[12] Stakeholders also highlighted many different types of jurisdiction-specific requirements for technical standards for messaging formats and accompanying legal documentation. Some authorities also described challenges in complying with sanctions obligations, including challenges that arise from differences in the formats of data provided for sanctions screening.

These frictions can impact cross-border payments in several ways. Different approaches to data requirements create a greater need for manual intervention, which reduces the speed of payments and increases the cost of providing cross-border payments. Inconsistent implementation of requirements can also lead to a higher incidence of payment rejections in cases in which the data accompanying a payment message does not meet specific local standards. These issues can increase operational costs and divert resources away from activities that could support more effective AML/CFT and sanctions compliance.

The following four recommendations therefore aim to promote harmonisation, standardisation and more consistent implementation of payments-related data requirements across jurisdictions. Respondents to the consultation widely supported these recommendations, noting, however,

---

11 INTERPOL (2024), INTERPOL Financial Fraud assessment: A global threat boosted by technology, March.

12 FATF is considering revisions to Recommendation 16 and published proposed revisions in February 2024. See FATF (2024), *Public Consultation on Recommendation 16 on Payment Transparency*, February. This work is identified as priority action 6a in FSB (2023a).

that their effectiveness will depend on the consistent implementation of these data standards across different jurisdictions, particularly in addressing variations in local data protection regulations and compliance requirements.

**Recommendation 3:** National authorities should encourage the adoption by market participants, including central banks and payment system operators, of the Bank for International Settlements' Committee on Payments and Market Infrastructure (CPMI)'s harmonised ISO 20022 data requirements for cross-border payments.[13]

The G20 cross-border payments programme identified the fragmentation of payment messaging standards (e.g. due to use of different messaging standards or even different implementations of the same messaging standard) as one of the major frictions contributing to the high cost, slow speed and lack of transparency in cross-border payments.[14] Payment systems around the globe have historically used a wide range of messaging standards for domestic payments. Against this backdrop, the growing worldwide adoption of ISO 20022 in payment systems[15] is an opportunity to achieve greater interoperability of messaging standards, with richer and more structured data allowing for significant benefits for enhanced cross-border payments across segments and end users.

While a global adoption of ISO 20022 is a very significant opportunity to improve cross-border payments, limited, incomplete, or inconsistent implementation of the standard in different jurisdictions and regions risks undermining its benefits. For example, many of the inefficiencies with cross-border payments faced by both the financial industry and its customers are caused by misaligned message flows and inconsistent data usage along the end-to-end payment chain. Thus, while ISO 20022 provides a common base for a more interoperable exchange of cross-border payment messages, how the standard is used in practice could vary considerably, and frictions in the processing of cross-border payments could continue to persist even as ISO 20022 is adopted.

To address inconsistent implementation of ISO 20022 hampering the efficient processing of cross-border payments, the Roadmap directed the CPMI to develop, jointly with industry, a set of harmonised ISO 20022 requirements for use in cross-border payments. These data requirements were published in October 2023[16] and foster consistent end-to-end use of ISO 20022 in cross-border payments. These harmonised data requirements are intended to supplement existing usage guidelines and market practices to further harmonise the use of ISO 20022 and help the G20 achieve its speed, cost, and transparency targets. They are critical in supporting the implementation of other recommendations in this report, particularly the implementation of a revised FATF Recommendation 16 standard (Recommendation 4).

---

13 Priority Action 8, "Finalising the ISO 20022 harmonisation requirements and promoting their real-world implementation," in FSB (2023a).

14 FSB (2020), *Enhancing Cross-border Payments – Stage 1 report to the G20: technical background report*, April. FSB outreach to the private sector in 2023 noted that frictions can differ based on the payment rail used (e.g. SWIFT, remittance providers, credit card networks) and the identifier used to settle a transaction (e.g. American Banking Association (ABA) routing number vs. International Bank Account Number (IBAN)), among other factors.

15 A CPMI survey conducted in late 2021 for ISO 20022 harmonisation indicated that 78% of the survey respondents (out of a total of 56 payment system operators in 38 jurisdictions) have either implemented or have concrete plans to implement ISO 20022 by 2025.

16 CPMI (2023), *Harmonised ISO 20022 data requirements for enhancing cross-border payments*, October.

Realising the benefits of harmonised ISO 20022 usage in cross-border payments depends on the widespread and consistent use of the CPMI data requirements (e.g. as network effects arise). To support this goal, the joint task force of CPMI and the global industry Payments Market Practice Group (PMPG) on ISO 20022 harmonisation has been working with the High-Value Payment System Plus (HVPS+) group (the self-standing ISO 20022 market practice group for private and central bank-owned high-value payment systems) and with the Cross-border payments and reporting plus (CBPR+) group (the ISO 20022 market practice group for cross-border, correspondent banking payments) to align HVPS+ and CBPR+ usage guidelines with the CPMI data requirements. Coordinating with these and other global market practice groups was strongly supported by the respondents to the public consultation as a way to enhance consistency in implementation and across the end-to-end cross-border payment chain.

Some respondents to the public consultation supported mandating the ISO 20022 adoption across Payment Market Infrastructures (PMIs) to avoid issues like data loss due to alternation or truncation when payments flow through different PMIs with varying data capacities. PMIs, acting as gatekeepers in the payment ecosystem, must be held responsible for setting clear rules for cross-border payments to ensure the integrity and efficiency of these systems. Other respondents, however, noted that harmonisation has costs for payment systems and jurisdictions should be simply encouraged to find their best ways to support the goal of consistent implementation of payments related data requirements in cross-border payments.

Overall, the recommendation that national authorities should encourage the adoption of these harmonised data requirements by market participants (including payment system operators, payment service providers and end users) by the end of 2027 seems to strike a right balance.

Another suggestion related to the need to clarify the interpretation and usage of some data fields. In this regard, it was suggested to liaise with FATF, the Wolfsberg Group and other financial crimes experts to ensure consistency and common understanding between the AML/CFT and message standards communities, a suggestion that may be taken up by the work of the Forum.

**Recommendation 4:** To avoid the inconsistent application of cross-border payment-related data requirements for AML/CFT compliance, national authorities should implement FATF Recommendation 16 and provide clear and accessible guidance on any additional data required to comply with local AML/CFT regulations. They should also use applicable global data standards, where available.[17]

The aim of this Recommendation is twofold: (i) to reduce fragmentation in data requirements for AML/CFT compliance in payments through the implementation of a global standard, which is set out in FATF Recommendation 16 and leverages ISO 20022 to promote consistency; and (ii) to encourage the provision of clear and accessible guidance about the application of any additional data requirements, beyond the minimum set out in FATF Recommendation 16 needed to address specific risks.

A FATF stocktake from 2021 to identify key areas of divergence in the implementation of AML/CFT requirements found that inefficiencies caused by inconsistent implementation of such rules caused frictions for cross-border payments. Rising costs appeared to be the main consequence, followed by reduced speed, reduced access, and inconsistent levels of

[17] Priority Action 6a, "Enhancing FATF rules on wire transfers," in FSB (2023a).

transparency. The stocktake also noted that some differences in requirements might be necessary to address different risks and contexts across jurisdictions.[18] The FSB stocktake and subsequent industry engagement similarly highlighted that differences in the implementation of FATF standards across jurisdictions result in disparities in the data required for inclusion in payment messages by different domestic AML/CFT frameworks. This may create ambiguity and greater complexity for firms and can result in payment delays, additional costs resulting from the need for manual intervention in payments, false positives in screening processes and increased regulatory and legal risk.

The FATF is currently reviewing its Recommendation 16 to take into account recent and upcoming developments in the payments systems architecture and to address some issues highlighted in this report. These include the adoption of ISO 20022 messaging standards and the need to encourage the use of standardised entity identifiers, such as the Legal Entity Identifier (LEI), in payments data, with a view to improving the consistency and usability of message data in cross-border payments and facilitating more efficient and accurate implementation of AML/CFT controls. Promoting a more consistent application and alignment of AML/CFT standards would enable financial institutions to reduce the level of resources needed to intervene manually in payment messages. In delivering its planned guidance for Recommendation 16, once the latter is revised, FATF will consider data-related issues, in coordination with other interested authorities (see also Recommendation 2 above).

While the FATF Recommendations aim to create consistency and define minimum standards, domestic regulators may choose to introduce bespoke data requirements to address specific risks, which vary across jurisdictions. When additional, bespoke requirements are needed, authorities should transparently set out the public policy rationale for them. Moreover, they should seek to make these requirements easy to access and understand so that all financial institutions can easily comply. To reduce fragmentation, consideration should be given to aligning, as much as possible, the data formats needed to meet minimum data requirements, and using applicable global data standards for any additional optional data.

Respondents to the public consultation noted the ongoing review of Recommendation 16 and often referred to the comments they made in that context. A general theme was the need to address the uncertainties on which data should travel along the payment chain, including whether and how information that is required for one national authority should or should not travel through the payment chain. Broad support was stated for the objective of ensuring consistency in implementation across jurisdictions.

**Recommendation 5:** Sanctions authorities should take steps to standardise the way sanctions lists are formatted, shared and updated. The use of sufficient and standardised identifiers should be encouraged to better facilitate identification, reduce false positives, and promote links between data sources.

In the FSB stocktake and subsequent FSB stakeholder engagement, as well as in the public comments received in response to the consultation report, the challenges of complying with sanctions obligations is the most frequently cited issue affecting the cost and speed of cross-border payments. Among other issues, public sector and industry stakeholders have highlighted

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

technical challenges in complying with sanctions regimes as a key friction for cross-border payments. Given that there are dozens of different sanctions authorities globally, each having their own data formats, standardising these and making the sanction lists machine-readable is much needed to ensure the effectiveness of sanctions. Listed designated parties may vary from one jurisdiction's sanction list to another and the format in which this information is shared is not standardised across jurisdictions. These discrepancies result in increased compliance costs as cross-border payments market participants must apply non-standard technological solutions to capture this information. Inconsistent and text-based presentation of sanctions lists can also result in a significant occurrence of false positives during sanctions screening. This reduces processes speed as legitimate payments must be manually investigated. It also diverts resources away from the timely investigation of payments that are of genuine concern. Standardised presentation of information in sanctions lists would allow cross-border payments market participants to invest more in standardised screening solutions. In addition, the use of standard unambiguous identifiers could materially reduce false positive rates and streamline screening processes. The Forum could explore options to address the inconsistencies in data elements relevant for sanctions screening. Given the critical link between this work and FATF Recommendation 16 and FATF recommendations related to sanctions implementation, this work could be carried out in close coordination with the FATF and national sanctions authorities.

During additional FSB engagement with industry, stakeholders raised the matter of separate challenges arising from the conflicting and inconsistent regulatory requirements related to sanctions implementation. Public comments on the proposed recommendations also included significant discussion of the inconsistencies of the legal and regulatory requirements and related supervisory expectations across jurisdictions, which create significant challenges in complying with sanctions obligations when processing cross-border payments. This specific issue falls outside of the scope of this report but options to address it may be investigated by the competent authorities.

**Recommendation 6:** National authorities should support the enhanced use of standardised global identifiers, such as the Legal Entity Identifier (LEI), including by taking steps to emphasise that the use of standardised global identifiers in cross-border payments is best practice.

The FSB's engagement with cross-border payments market participants has found that poor data quality, fragmentation in data sources and limited standardisation of data exchange cause complexity when processing cross-border payments, which increases their cost, limits speed and impacts transparency. Recourse to global standardised identifiers, where available, could contribute to addressing such problems and has clear links with the objectives outlined in the previous Recommendations 3, 4 and 5. The FSB has previously reviewed the scope and technical and operational requirements of existing and proposed global digital identifiers for both legal entities and natural persons as part of the Roadmap.[19]

There are standardised legal entity identifiers available that could partly serve this purpose, such as the Business Identifier Code (BIC). The LEI may offer advantages as it is not linked to a specific messaging network and is available to all corporate and legal entities. The LEI can be used to verify the identity of all legal entities involved in a payment chain. The G20 included a

[19] FSB (2020)

priority action[20] in the Roadmap to "explore the enhanced use of the LEI in cross-border payments."[21] This was due to its broad characteristics and G20 endorsement of the FSB's creation of the LEI.[22]

The FSB's work on options to improve adoption of the LEI, in particular for use in cross-border payments noted that both authorities and market participants recognise the potential benefits of the LEI in strengthening data standardisation as well as assisting and supporting straight through processing (STP), customer due diligence (CDD) processes and sanctions screening, all of which contribute to the Roadmap's targets and objectives and reinforce the recommendations above.[23]

The October 2024 FSB *Implementation of the Legal Entity Identifier: Progress report*[24] recommends FSB Member jurisdictions, in collaboration with the Regulatory Oversight Committee[25] and the Global Legal Entity Identifier Foundation[26] to explore, where appropriate, the scope to mandate use of the LEI for certain payment message types for routing message formats migrating to ISO 20022 messages; continue exploring, with national regulators and others, the role the LEI might play in assisting entities with due diligence for KYC, as well as other use cases such as sanctions screening; consider a staged approach to the introduction of the LEI requirement in payment messages, by assessing which categories of entities or which thresholds of payment value could be considered for the gradual introduction of LEI requirements for payments. The same Report recommends that relevant standard-setting bodies and international organisations should consider issuing guidance on the role that the LEI and possibly the vLEI might play in assisting entities with due diligence for KYC and sanctions screening, and fraud prevention.

In October 2023, the CPMI recommended, as part of ISO 20022 implementation, to identify financial institutions involved in cross-border payments via globally recognised and publicly available identifiers and recognised the benefits of using standardised identifiers like the BIC or the LEI in cross-border payments for this purpose.[27] The FATF is also considering, in its review of Recommendation 16, encouraging the inclusion of standardised global identifiers, such as the LEI, as part of the information accompanying all qualifying payments or value transfers. The FSB

---

20 The stocktake work on identifiers for individuals, while noting the importance of the issue concluded that this workstream was not likely to provide a material contribution to achieving the targets by 2027 due to several challenges. A positive impact of an enhanced use of global legal entity identifiers could, however, provide a renewed stimulus to the work on identifiers for natural persons.

21 FSB (2023a), page 10.

22 At the June 2012 Los Cabos Summit, the G20 Leaders endorsed FSB report (2012), *A Global Legal Entity Identifier for Financial Markets* June. They encouraged "global adoption of the LEI to support authorities and market participants in identifying and managing financial risks". The LEI was established by the FSB in 2012 to support authorities and market participants in identifying and managing financial risks. It has well-established governance features, including oversight by the Regulatory Oversight Committee (ROC), a group of more than 65 financial market regulators and other public authorities, as well as 19 observers from more than 50 countries, and a specific data quality management programme.

23 FSB (2022), *Options to Improve Adoption of the LEI, in Particular for Use in Cross-border Payments*, July.

24 FSB (2024), *Implementation of the Legal Entity Identifier: Progress report*, October.

25 The Regulatory Oversight Committee (ROC) is a group of more than 65 financial markets regulators and other public authorities and 19 observers from more than 50 countries. It promotes the broad public interest by improving the quality of data used in financial data reporting, improving the ability to monitor financial risk, and lowering regulatory reporting costs through the harmonisation of these standards across jurisdictions.

26 Established by the Financial Stability Board in June 2014, the Global Legal Entity Identifier Foundation (GLEIF) is tasked to support the implementation and use of the Legal Entity Identifier (LEI). The foundation is backed and overseen by the Regulatory Oversight Committee (ROC).

27 CPMI (2023), *Harmonised ISO 20022 data requirements for enhancing cross-border payments-final report*, October.

is aware that sanctions authorities responsible for listing sanctioned entities utilise the LEI, when possible, to identify sanctioned entities. Although the vast majority of potential sanctions targets may not be eligible for an LEI, as they are not legal entities, and many others would not register for one, the LEI could contribute to reducing the number of false positives. These false positives may currently be a cause of reduced speed and increased costs. In addition, private sector participants included the use of the LEI among the best practices in payments. For example, in its September 2021 white paper, SWIFT's Payments Market Practice Group (PMPG)[28] provided information on existing market practices regarding the LEI as an identifier in payments. It also illustrated the use case for the LEI in payments: benefits for participants include more transparent, efficient and secure payments.

In considering providing enhanced support for the use of the LEI in payments, authorities could also consider that the potential benefits accruing from a global standard identifier, with a strong governance framework and robust data quality management programme as in the LEI case, have been recognised in several other domains (e.g. statistics and trade[29]) suggesting that a jurisdiction-wide approach of support for the use of the LEI might also be considered.

Respondents to the public consultation supported the rationale underlying this recommendation, namely that the use of a standardised global identifier for legal entities could benefit cross-border payments in a variety of dimensions (e.g. sanctions, AML, fraud prevention). Some respondents added that LEI Level 2 data that answers the question of 'who owns whom' could provide useful information on beneficial ownership when linked to high-quality beneficial ownership data via (ongoing) mapping exercises.

**Recommendation 7:** Building on its ongoing evidence-based and multi-stakeholder work on cross-border data flows, the OECD, together with data privacy and protection authorities and relevant cross-border payments stakeholders, should explore different options to enable faster, less costly, more transparent and more accessible cross-border payment-related data flows while ensuring high levels of privacy protection.

In addition to promoting standardisation and greater consistency across different regulatory and data requirements, including in their implementation, the recommendations in this report aim to promote interoperability in particular with reference to data privacy and protection and data transfer rules. During the FSB's engagement with industry on this topic, industry stakeholders have asked for common principles to be adopted between different privacy frameworks to enable mutual recognition across jurisdictions. Some industry participants encouraged adequacy arrangements or other mechanisms for data transfers to address different approaches to data privacy between major markets. The GPA ran a census in 2023, gathering information from 78 GPA members to provide a timely picture of the policies and delivery approaches that currently

[28] SWIFT PMPG (2023). *Global Adoption of the Legal Entity Identifier (LEI) in ISO 20022 Payment Messages Version 2*, December. The SWIFT PMPG is a global discussion forum of private sector payments experts which takes stock of payments market practices across regions, discusses market practice issues, and recommends market and best practices related to payments messages.

[29] Committee on Monetary, Financial and Balance of Payments Statistics (2023), CMFB opinion on the Legal Entity Identifier (LEI) as unique identifier of financial and non-financial companies for statistical purposes, May. International Chamber of Commerce (2023), *Trust in Trade*, March.

guide and regulate data protection and privacy around the world.[30] Box 1 provides a brief overview of the main findings of the survey.

**Box 1: GPA Information on cross-border data transfer mechanisms**

The 2023 GPA Census found that, of the authorities surveyed, most jurisdictions (90%) have laws that include provisions on restricting transfers of personal information across borders. This figure increased slightly compared with 2020 (83%). On the other hand, only a minority of authorities (17%) reported that they require facilities in the jurisdiction for data processing. This figure was lower than that reported in 2020 (27%).

The authorities were also asked in the survey about existing mechanisms within their legislation for cross-border transfers of personal data. Most authorities reported that their legislation that provides mechanisms such as model clauses (56%) and binding corporate rules (62%). To a lesser extent, the authorities reported that legislation provides for commercial agreements (42%) and certification schemes (40%).

Extensive work on different cross-border data transfer tools and their commonalities has been carried out by both the GPA Global Frameworks and Standards Working Group (GFSWG) and the OECD. The GFSWG has delivered various comparative and analytical outputs,[31] focusing on clarifying transfer mechanisms in various global frameworks and highlighting commonalities between them. In 2023, it completed a detailed comparison of standard contractual clauses in different data protection and privacy frameworks, with the aim of helping GPA members and organisations to understand different transfer mechanisms and identify gaps and opportunities for further work.

The OECD has also explored this topic in depth, noting how in the case of cross-border data flows, governments, data protection and privacy authorities, and other stakeholders increasingly use a range of approaches to transfer data across borders while ensuring that, upon crossing a border, data are granted the desired oversight and/or protection.[32] The OECD also noted that while frameworks aimed at generating trust and facilitating data flows build on commonalities and elements of convergence, yet businesses identify challenges to fully operationalise them at the global level. The OECD thus carried out work to inform a more comprehensive understanding of challenges and ways forward for the policy agenda of 'data free flow with trust'.[33]

While this work on the convergence of data transfer frameworks has not specifically focused on the cross-border payments-related data flows, more recently the launch of a dedicated working group of the Data Free Flow with Trust (DFFT) Experts Community has been looking into this specific issue. The DFFT policy agenda – promoted by the Japanese G20 (2019) and G7 (2023) presidencies – aims to promote the free flow of data while ensuring that privacy, security, and intellectual property rights will be respected and protected. The DFFT Experts Community was launched at the OECD in April 2024 to operationalise the concept of DFFT and bring governments and stakeholders together to advance solutions-oriented, evidence-based, and multi-stakeholder cooperation on relevant DFFT issues, and inform the development of concrete

30 GPA (2023), *Navigating the Global Data Privacy Landscape: the 2023 GPA Census*.

31 GPA (2022) *Global Frameworks and Standards Working Group: Report*, July. Annexes A and B of the Report provide a detailed account of cross-border data transfer mechanisms.

32 OECD (2022), *Fostering cross-border data flows with trust: OECD Digital Economy Papers,* December.

33 OECD (2023), Moving forward on data free flow with trust, April.

responses to a variety of practical problems related to data transfers and sharing in a cross-border context. A DFFT working group is exploring cross-border payments-related data flows with more than 50 cross-border payments stakeholders, including national authorities involved in payments and in privacy and data protection, relevant international standard-setters, such as the FATF, and payments industry experts. The working group will assess tools and legal bases for cross-border transfers of personal data that may be particularly appropriate in the context of cross-border payments and could eventually feed into the policy work of the OECD through its regular governance channels.

Respondents to the public consultation urged that the Forum coordinates closely with the OECD DFFT Experts Community to reduce potential duplication of work and asked how national DPAs are expected to engage in this work, a point that will be further assessed together with the organisations launching the Forum (i.e. FSB, FATF, GPA and OECD). This is also very relevant for the follow-up work to be carried out at national level (as per the following recommendation).

**Recommendation 8:** Building on the work outlined in Recommendation 7, relevant authorities should adopt and enforce consistent standards in domestic privacy and data protection regimes applicable to payment processing and identify appropriate cross-border data transfer mechanisms.

The work carried out under Recommendation 7 could serve as the basis for identifying appropriate mechanisms for payments-related data transfers. For example, financial services firms sometimes rely on “equivalence” or “adequacy decisions” from jurisdictions that find that another jurisdiction has equivalent or adequate data protection and privacy requirements to transfer data across border in the normal course of business.[34]

To facilitate mutual recognition and ensure interoperability (e.g. via effective equivalence or adequacy assessments), jurisdictions should adopt and enforce consistent standards in domestic privacy and data protection regimes applicable to payment processing. In doing so, authorities should administer transparent rulemaking processes and clearly articulate these policies in public communications, including implementation guidance, as appropriate. Authorities should seek public input and engage with foreign counterparts to support understanding of data protection and privacy policies and regulatory cooperation, with a view to moving towards adequacy assessments or similar mechanisms over time.

This will facilitate cross-jurisdictional benchmarking and provide respective assurance that the data are adequately protected in the destination country. Enabling consistent data protection and privacy standards can foster mutual recognition arrangements and interoperability as well as limit the need to restrict personal data transfers to and from overseas jurisdictions.

To support the objectives of this recommendation, jurisdictions should allow the implementation of specific data transfer tools, such as standard contractual clauses, binding corporate rules,

[34] Equivalency assessments are also used where there is a cross-border payments system operator recognised by multiple jurisdictions with supervisory responsibilities. Supervisory authorities can undertake equivalency assessments of supervisory counterparts to determine if informed reliance can be placed on the designated primary supervisory authority. The assessment will consider the primary supervisory approach and whether it is broadly equivalent and achieves similar outcomes. This example of an equivalency assessment is not related to data privacy and protection rules.

certifications[35] or other similar tools, based on the assessment that they provide sufficient data protection safeguards for personal data transfers in the payments context and meet the requirements of the payment industry. These tools allow parties to identify responsibilities and ensure accountability of different parties throughout the data transfer journey. In addition, these tools may help to provide the assurances that the jurisdiction of origin considers important, even in the absence of protections in the legal framework in the destination jurisdiction.

# 3. Mitigating restrictions on the flow of data related to payments across borders

The FSB stocktake noted that the G20 Payments Roadmap objectives can be undermined by policies that require data to be stored or processed in-country. These policies include restrictions on the transfer of data across borders (data localisation) or requirements to maintain a copy of the data in the local jurisdiction (data mirroring). These restrictions range from requirements for data generated inside a jurisdiction to be stored and processed by firms within that jurisdiction to data export conditions that need to be met before data can be moved abroad.[36] Data localisation policies force firms to locate all or part of their data and/or operations within the borders of the jurisdiction that imposes these policies.

Data localisation policies may be driven by differing public policy objectives. These may include an interest in building local operational resilience in data systems, protecting against cyber security threats and, as seen by some authorities, having the further benefit of strengthening customers' confidence in data storage security in the national payment system. Authorities may also put in place data localisation policies to ensure access to data for law enforcement and supervisory authorities if they are not confident that they will have access to these data absent such policies. Many of the objectives of data localisation policies extend beyond those of financial regulation and are often not set by financial regulators.[37] However, data localisation policies have consequences that may cause delays or even stop cross-border payments.

For cross-border payments market participants with operations in multiple jurisdictions, these restrictions can limit the internal sharing or aggregation of data. The inability to aggregate – or delays in aggregating – locally-held data also make it more difficult to assess and manage risk on an enterprise-wide basis, including effectively identifying cross-border fraud and complying with AML/CFT requirements, sanctions, and other regulatory obligations. In addition, data localisation policies can increase risks of incomplete data, leading to transaction fails that disrupt STP. Infrastructure and personnel may need to be duplicated in individual jurisdictions, creating fragmentation and adding complexity, multiplying opportunities for error and creating new vulnerabilities to cyber incidents. Monitoring for malicious activity can no longer occur centrally, taking advantage of all the relevant data, and the ability to transfer data to reserve capacity in

35 Such tools are envisaged by the Global Cross-Border Privacy Rules Forum, established in 2022, building on the Asia-Pacific Economic Cooperation (APEC) cross-border privacy rules (CBPR) framework. For more information, please see Asia-Pacific Economic Cooperation (2023), *What is the Cross-Border Privacy Rules System*, June.

36 GPA (2023).

37 FSB (2019), *FSB Report on Market Fragmentation*, June.

another geolocation (e.g. in the event of a cyber attack) is lost. This may also degrade the security of the data and the global resilience of the data systems.

There may also be a loss of economies of scale as more data centres must be established and maintained. As a result, firms involved in cross-border payments face increased costs to appropriately manage risk and to store, secure, and integrate data into global operations. This may affect the price of cross-border payments for consumers. The resulting increase in costs and operational complexity may also compel some cross-border market participants to leave certain markets, or act as a barrier to entry for smaller players, reducing competition in cross-border payments and potentially affecting availability and access to financial services.

The objective of the recommendations below is to mitigate these unintended consequences of restrictive policies on data storage and transfer[38] while avoiding compromising on the underlying objectives of some data localisation policies, such as improving operational resilience and the effectiveness of supervision and law enforcement.

**Recommendation 9:** National authorities should provide a clear and reasonable legal pathway for cross-border payments market participants to transmit across borders data related to payment processing, risk management, or fraud and financial crime prevention. Where applicable, national authorities should provide alternatives to requirements to use local computing facilities.

National authorities should avoid imposing restrictions on the transfer of data outside of their jurisdiction in situations in which the destination jurisdiction conforms to broadly equivalent data protection and privacy standards. Meeting equivalent protection and privacy standards is important because lack of confidence in that equivalence can be a motivation for a jurisdiction to implement data localisation policies. In jurisdictions where data localisation policies exist, national authorities should provide firms with alternatives to those policies to facilitate effective payment processing, risk management, fraud and financial crime prevention.

Creating legal pathways and other alternatives for the transfer and storage of payments-related data without compromising data storage security could help mitigate frictions related to data localisation in cross-border payments. In addition to facilitating data aggregation within global firms for risk management and regulatory compliance, as described above, pathways and alternatives for data transfer and storage may also support improved operational efficiency in cross-border payments. Industry stakeholders have cautioned that the creation of pathways, while helpful in addressing the issues described, could also lead to fragmentation.

The increasing prevalence of fraud in cross-border payments was frequently cited in the public responses to the consultation report as a significant concern. There was broad recognition of the need to enhance data flows for use in fraud prevention and detection controls, not just among cross-border payments market participants but including social media and telecommunications firms, which are also stakeholders in anti-fraud efforts.

[38] For a description of categories of data restrictive policies, see M. Ferracane and E. van der Marel (2024), *Governing personal data and trade in digital services*, January.

The Forum could develop principles and best practices to help jurisdictions avoid this type of fragmentation, while maintaining the underlying objectives that may motivate data localisation policies.

**Recommendation 10:** National authorities should establish clear and transparent mechanisms to allow cross-border payments market participants to share data with foreign regulatory and supervisory authorities, as appropriate. Cross-border payments market participants should ensure relevant regulatory and supervisory authorities have full and timely access to data in accordance with their respective mandates.

When establishing data restrictive policies, jurisdictions frequently cite the valid need to maintain access to private sector data for regulatory and law enforcement activities. Financial regulators need access to payments data to fulfil their responsibilities in relation to the regulation and supervision of the financial sector. They may also need to access personal data in matters related to financial crimes and/or suspicion of fraud. In addition, several authorities from different jurisdictions might need to play a role in regulatory and supervisory issues involving cross-border payments. Instead of requiring data to be held locally, authorities should establish requirements for cross-border payments market participants to allow access to payments data for regulatory and supervisory activities. These should include legal arrangements that facilitate access across borders, either directly or via local authorities, e.g. under the terms of a memorandum of understanding. National authorities should provide an opportunity for cross-border payments market participants to grant prompt access to payments data requested by financial regulators before being required to use local computing facilities. When considering their domestic policies, authorities may look to build on existing and emerging governance models, including taking into account approaches to government access for law enforcement and national security purposes such as those embodied in the OECD Declaration on Government Access to Personal Data Held by Private Sector Entities.[39]

**Recommendation 11:** When designing their data-related policies, relevant authorities should consider potential impacts on consumers and cross-border payments market participants. In particular, jurisdictions should consider how data restrictive policies, including data localisation and data mirroring requirements, could affect the cost, speed, transparency and accessibility of cross-border payments.

When considering data restrictive policies, relevant authorities should analyse the impact of those policies on cross-border payments before imposing them. As described above, such policies have a variety of impacts on the operation, efficiency and costs of cross-border payments, which could lead to broader economic effects. For example, if such policies necessitate firms building and integrating additional data centres into a global operational infrastructure, this may act as a barrier to market entry. Additional requirements associated with operating in a jurisdiction with data restrictive policies may affect the costs and availability of cross-border payments.[40]

---

39 OECD (2022), Declaration on Government Access to Personal Data Held by Private Sector Entities, December.

40 See Centre for Information Policy Leadership (CIPL) (2023), *The "Real Life Harms" of Data Localization Policies*, March; D Medine (2024), Data Localization: A "Tax" on the Poor, *Centre for Global Development Working Papers 674*, January. For an analysis of the impact of data localisation on gross domestic product (GDP) broadly, see European Centre ECIPE (2014), The Costs of Data Localisation: Friendly Fire on Economic Recovery.

The potential impact of enacted or proposed data restrictive policies could be measured in a variety of ways. The World Bank, OECD and other scholars and international organisations have conducted empirical and policy analyses on data restrictive rules that relevant authorities can leverage in conducting similar analyses. In the longer term, the Forum could undertake the development of a framework to assist relevant authorities in assessing impacts in this area, but the factors below are illustrative of relevant considerations:

- Impact on operational resilience, including cyber resilience.[41] These impacts stem from creating data siloes that prevent institutions from building redundant systems and in aggregating data that may help detect threats.

- Impact on effectiveness in detecting and preventing fraud and financial crime.[42] Similar to the operational and cyber-related impacts above, the fragmentation of data hinders efforts to detect and monitor cross-border financial crime trends, risks, and threats.

- Impact on the overall availability of cross-border payments services.[43] The added costs associated with some data protection and privacy requirements may serve as a deterrent to foreign firms entering the market, particularly smaller firms, or limit their ability to provide potential services. This may disproportionately affect providers to low-income consumers.

- Data restrictive policies can create identifiable macroeconomic effects. They can increase import prices for downstream industries that rely on data, thereby reducing exports and overall trade. The World Bank notes that the benefits of reducing data restrictions would be, on average, about 5% on trade in services[44] and that the gains in productivity would be on average of about 4.5% on average in the event that restrictive data policies were removed.[45] These impacts have identifiable effects in terms of GDP.[46]

Impact analysis could also take into consideration alternative ways of providing the same outcome in a less restrictive manner. Respondents to the public consultation also suggested that authorities that are considering imposing or extending data barriers should identify the regulatory objective sought to be achieved, and consider whether other, less restrictive means – including but not limited to privacy-enhancing technologies (PETs), regulatory reporting or data access mechanisms – could achieve the same objectives. Jurisdictions should also consider potential intangible impacts of data policy, such as slower payment transactions and reduced trade and

---

41 CIPL (2023); Medine (2024). OECD (2023a), *The Nature, Evolution and Potential Implications of Data Localisation Measures*.

42 CIPL (2023).

43 See the case studies contained in Medine (2024).

44 See World Bank (2020), *World Development Report 2020*. See also N Cory and L Dascoli (2021), How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them, Information Technology & Innovation Foundation (ITIF), which states: "Using a scale based on OECD market-regulation data, ITIF finds that a 1-point increase in a nation's data restrictiveness cuts its gross trade output 7 %, slows its productivity 2.9 %, and hikes downstream prices 1.5 % over five years."

45 See World Bank (2020); See also OECD (2023) finding, based on an OECD-WTO business questionnaire, that depending on the type of measure in place, data localisation could raise data management costs by between 15 and 55%.. See also M Ferracane and Evan der Marel (2018), , Do Data Policy Restrictions Inhibit Trade in Services?, ECIPE .

46 See E van der Marel, H Lee- Makiyama and M Bauer (2014) , *The Costs of Data Localisation: A Friendly Fire on Economic Recovery*, ECIPE.

commerce benefits, in deciding whether to support or inhibit the achievement of the policy objectives outlined above.

Factoring in such considerations will help authorities make informed decisions regarding the causal connections and trade-offs between and among data protection and privacy objectives and other policy goals.

# 4. Reducing barriers to innovation

There are many promising innovations that could help address frictions in the payments system arising from data frameworks. These include technologies that allow for data sharing in protected environments, full payment traceability, improved customer verification and pre-payment validation, among others. As with other innovation efforts, the development and scaling of these technologies in the cross-border payments market depends on significant effort by the private sector, including firms' willingness to invest significant financial and human resources and to take on the legal and regulatory risk that may come with unproven technologies. There is also additional cost involved in navigating competing legal and regulatory requirements – affects investment decisions related to launching innovative new products. There is an opportunity cost for firms when choosing to invest in these technologies, which involves making a choice to forego other product development opportunities or investments.

In the face of these costs and risks, cross-border payments market participants may not pursue even the most promising new technologies absent a supportive legal, regulatory and policy environment. In order to overcome these barriers, it will be important to create space for innovation by ensuring the environment supports the adoption of new technologies while maintaining security and consumer protection. This may include a range of actions, from positive "signalling" from regulators to regulatory exemptions and safe harbours for innovation in payments.

**Recommendation 12:** National authorities and international standard setters should promote innovation that may offer solutions to data frictions in cross-border payments by taking steps to foster public-private sector partnerships, facilitate dialogue with innovators, create regulatory frameworks that support innovation, and share best practices with international counterparts.

Innovation in payments while maintaining security and consumer protection is already a key priority for many jurisdictions, but the structures that have been put in place to support innovation vary widely from jurisdiction to jurisdiction. For example, many jurisdictions have introduced regulatory "sandboxes" or offices of innovation. In addition, the BIS Innovation Hub has initiated a number of projects that aim to address the particular frictions described in this report. The design of sandboxes varies, but they typically allow firms to experiment with cutting-edge technology in a controlled setting – usually involving some kind of limit on activity – under the supervision of a regulatory authority. Innovation offices within regulatory agencies provide a mechanism for new or existing firms to engage with regulators as they introduce new technology or engage in novel business models. Similarly, national authorities have hosted "tech-sprints" to actively spur industry to develop technology solutions to policy issues. While these are important initiatives, industry feedback highlights that they often lack cross-border regulatory coordination to facilitate the development of products that operate in multiple jurisdictions. In addition, there

is a lack of mechanisms to support cross-border payments market participants in the transition from sandboxes or tech sprints to operating "live in the market".

In addition to these firm-level approaches to encouraging innovation, many countries have also introduced fintech laws, issued new regulations, and provided regulatory guidance aimed at creating a level playing field and supporting clear regulatory pathways for innovative payment service providers. The appropriate approach, or combination of approaches, will depend on national circumstances, including the domestic regulatory framework, the level of development and complexity of the financial sector, and the frictions consumers and firms are experiencing resulting from the use of existing payments systems. Examples of such pathways have included provisions to create new licences for non-bank payment service providers (e.g. third-party service providers that initiate payments) and regulation that promotes open banking or open finance business models. The FSB stocktake identified open banking and open finance, which aim to change the way payments-related data are accessed and shared, as particularly promising in addressing frictions in payments. For instance, many open banking initiatives are working on confirmation of payee solutions that can increase transparency and reduce erroneous or fraudulent payments. This is an area that will be further explored by the CPMI.

An additional element that is critical in supporting innovation is improving the understanding of new technologies among relevant public and private sector stakeholders. Supervisory authorities, for example, may not be comfortable assessing new technologies they are not yet expert in. The Forum could play a role in providing a channel for information sharing about technologies and in sharing best practices for regulators to support innovation.

### Box 2: Privacy Enhancing Technologies

Some of the most promising technological innovations to address data-related frictions in cross-border payments are privacy enhancing technologies (PETs). PETs are a collection of digital technologies and approaches that permit collection, processing, analysis and sharing of information while protecting the confidentiality of personal data.[47] While there are many forms of PETs, the OECD groups them into four categories, all of which may have applications for cross-border payments:

- **Data obfuscation tools**, which include tools that allow for anonymisation or zero-knowledge proofs.
- **Encrypted data processing tools**, which allow computations to run over data that are never visible or disclosed; in contrast to data obfuscation, the underlying data remains unmodified but hidden by encryption.
- **Federated and distributed analytics** allows executing analytical tasks data that are not visible or accessible to those executing the tasks, which allows sensitive data to remain under the custody of a data source while it is analysed by third parties.
- **Data accountability tools** offer new controls over how data can be gathered, used or provide transparency and immutability into transactions.[48]

One example of how PETs may be used to address data-related frictions in cross-border payments is a project developed in the context of a challenge sponsored by the UK and US governments. The

47 OECD (2023b) *Emerging Privacy Enhancing Technologies: Current Regulatory and Policy Approaches*, March.

48 OECD (2023b).

winning project focused on enhancing cross-border data access in order to combat financial crime, including fraud.

While PETs are promising technologies, there are a number of barriers to their adoption in the context of cross-border payments. There is a general lack of understanding of PETs among cross-border payments market participants, both in terms of a lack of understanding of the technologies that support PETs and also an understanding of the costs and benefits of PETs. In addition, regulation of PETs is still evolving, which leads many cross-border payments market participants to hesitate to embrace PETs in the provision of financial services. Firms involved providing cross-border payments services are often concerned that utilising a new technology, absent a legal or regulatory safe harbour, could expose them to increased legal and regulatory risk or even create heightened expectations on the part of supervisors. In general, the lack of adoption of PETs is likely to create difficulties for the further growth and development of the technology itself.