12 December 2024

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

Overview of responses to the consultation

Introduction

On 16 July 2024, the FSB published a consultation report on recommendations to promote greater alignment and interoperability across data frameworks related to cross-border payments, with a comment period that closed on 9 September.

The consultation report set out 12 recommendations that aim to 1) address uncertainty about how to balance regulatory and supervisory obligations; (ii) promote alignment and interoperability of regulatory and data requirements as well as promoting their consistent and widespread implementation; (iii) mitigate restrictions on the flow of data across borders; and (iv) reduce barriers to innovation.

The FSB received 34 (including six confidential) responses to the consultation.[1] 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 respondents are geographically diverse, including entities located in Africa, Asia, Australia, the United Kingdom, the United States, and the European Union.

The majority of responses indicate broad support for the FSB recommendations, affirming that issues related to data frameworks are critically important to address in order to improve cross-border payments. There is a recognition of the importance of standardisation and regulatory alignment and that making data formats and regulations more consistent, easier to implement, and less onerous for cross-border payments market participants can help foster innovation and scalability. Many respondents agreed with the proposed recommendations and provided additional information and experiences drawn from their institutions to support the FSB's proposed approach.

As such, the comments did not lead to revisions to the proposed recommendations. However, information provided in the comments has been included in the supporting rationale for the recommendations. In addition, the comments have been important in shaping the development of a strategy by the FSB and its partner organisations to support implementation of the recommendations. In particular, the comments have helped the FSB and its partners to identify

[1] The public responses are available on the FSB website.

the most urgent and intractable issues related to data frameworks that warrant the focus of the FSB and its partners going forward.

1. Feedback on the proposed recommendations

The consultation report included questions intended to elicit feedback on the recommendations and on areas of concern (e.g. the potential for increased fraud in cross-border payments) that were identified in the course of developing the proposed recommendations. The feedback received is presented below following the four themes addressed by the data frameworks recommendations.

1.1. Addressing uncertainty about how to balance regulatory and supervisory obligations (Recommendations 1 and 2)

The first two recommendations propose to establish a forum to bring together various stakeholders relevant for data issues in cross-border payments, including payments, anti-money laundering and combating the financing of terrorism (AML/CFT), sanctions, and data privacy and protection authorities. In addition, it is proposed that the forum would work to identify divergences in data frameworks and to develop possible solutions to address them.

All respondents who commented on the forum expressed strong support for its establishment, which would help to bridge a gap in coordination and communication between financial sector and data privacy and protection authorities and experts. Most comments focused on how the forum could best carry out its work and the importance of leveraging the proposed private sector advisory body in the forum's work. In particular, several respondents urged that the advisory body should consist of geographically diverse members from a range of payment service providers, including smaller firms. Several respondents noted that establishing a forum was necessary to have a holistic approach for tackling the complexities of cross-border payments, which involve multiple jurisdictions, regulatory frameworks and technical standards, and underlined the importance of using the forum to address newly emerging divergencies ("scan the horizon"). A multi-stakeholder forum is also seen as helping to address data localisation and other data barriers such as regulatory fragmentation and inconsistent implementation, and to standardise pathways for data sharing. Broad support was given to the idea of dealing with standardisation of data elements in sanction lists as part of the forum's activities. Some respondents also mentioned providing support to innovative activity. Several respondents also considered the forum to be a useful venue to discuss fraud prevention.

1.2. Promoting the alignment and interoperability of regulatory and data requirements related to cross-border payments (Recommendations 3, 4, 5, 6, 7 and 8)

There was broad support for the recommendations that aim to promote greater alignment and interoperability of regulatory and data requirements related to cross-border payments. While the recommendations are considered a step in the right direction, there remains a significant amount of work to establish comprehensive standards that will guide consistent practices across

jurisdictions. Formalising these standards and driving adoption is seen as essential to enhancing both data interoperability and data privacy and protection.

- **ISO 20022 implementation**. One respondent noted that deploying ISO 20022 domestically, including the settlement of the last leg of a cross-border payment via a domestic RTGS system, shows that inconsistent language and guidance is often an area of challenge. This will be exacerbated for those where English is a second language who must navigate the current inconsistent usage guides. Creating an ISO 20022 harmonisation umbrella structure could resolve these issues. Another respondent highlighted the high cost of making changes to non-wire payment systems and suggested that the recommendation be revised to encourage national authorities to engage with their communities to educate them about the ISO 20022 format, seek input about the CPMI's ISO 20022 data harmonisation requirements, and consider how their jurisdictions can best support the goal of consistent implementation of payments-related data requirements in cross-border payments.

- **Implementation of FATF Recommendation 16**. Although the FATF has not yet finalised its revision of Recommendation 16, there was broad support for authorities to provide guidance on any additional data required to comply with local AML/CFT regulations. A few respondents suggested that this recommendation could encourage national authorities to use the Global LEI System for accessing essential data, enhancing AML/CFT measures and regulatory inconsistency across jurisdictions.

- **Issues arising from sanctions compliance in cross-border payments.** There was also broad support for the FSB to do work on sanctions in the context of cross-border payments. One respondent noted that since January 2017 the number of sanctioned persons has increased by 320% and highlighted the inconsistencies of naming conventions and lack of identifiers and its impact on false positives and effectiveness. Given that there are dozens of different sanctions authorities globally, each having their own data formats, standardising these and making the sanctions lists machine-readable is much needed to ensure the effectiveness of sanctions. Some respondents suggested mentioning or endorsing the LEI as a standard in sanctions publications to help to reduce false positives. Several respondents supported having further discussion in the forum on sanctions-related issues.

- **Enhancing use of standardised global identifiers, such as the LEI.** One respondent said that the use of ISO externalised codes (rather than proprietary codes) should be encouraged as a best practice when using the ISO 20022 format. By using ISO 20022 codes from published lists consistently with their descriptions, all those involved in the processing of a cross-border payment can unambiguously understand the information, increasing the end-to-end processing speed and transparency of the payment details. This prevents the need for manual intervention and interpretation for any of the elements where externalised codes may be used.

- **Cross-border data transfer standards and mechanisms.** There was good support of the FSB's engagement with the OECD and the work planned by the OECD through the Data Free Flow with Trust Experts Community. Regarding the development of policies aimed at enhancing cross-border payments, one respondent commented that the impact of these policies on local payment services and infrastructures should be

taken into consideration. The commenter noted that regulatory consistency and adequacy assessments or similar mechanisms are useful tools, but situations where these clauses do not exist should also be addressed in a way that do not affect the processing of local payments.

- **Artificial intelligence (AI).** One respondent suggested that AI systems processing cross-border payments should adhere to privacy regulations, making it essential that the data frameworks recommendations address the intersection of AI with privacy and data protection, ensuring that AI applications remain transparent and respectful of privacy. AI can significantly enhance fraud detection and AML/CFT compliance, so recommendations should consider how AI tools are integrated into payment systems while aligning with existing data standards and privacy requirements. While the FSB acknowledges that AI has significant intersection with data frameworks, the exploration of AI was judged to be beyond the scope of this report.

1.3. Mitigating restrictions on the flow of data related to payments across borders (Recommendations 9, 10 and 11)

- **Cross-border data sharing.** There was broad support of the need to establish legal gateways for data sharing, with several respondents suggesting to consider the concept of 'safe harbour' provision, which would provide shelter from liability to firms that undertake good-faith efforts to ensure the safety and soundness of cross-border payments, via for instance fraud prevention measures, AML/CFT controls, and risk management, and which would be consistent with FSB goals in these areas. Several respondents underscored the need to mitigate inefficiencies caused by data localisation policies, which should be avoided in the first instance where there is equivalence in data protection and privacy. Creating clear pathways for cross-border data transfer and sharing will empower market participants to comply with regulations while maintaining a seamless flow of information. By addressing these legal and procedural aspects, a foundation will be created that supports innovation and facilitates smoother, more secure cross-border transactions.

- **Fraud.** There was broad recognition of the need to enhance data flows for use in fraud prevention and detection controls. Obstacles to such data and intelligence sharing must be removed, as overcoming these barriers represents one of the most significant steps toward enabling collective efforts to effectively combat and disrupt global fraud and scam operations. Some respondents noted the challenges with identifying fraud in real time and preventing the dissipation of criminal funds. Increased speed and volume of transactions will require effective technology-based solutions (or face unmanageable compliance burdens) which could be prohibitively expensive for some organisations. One respondent suggested that the whole fraud chain be explored, beyond financial services providers which are usually the very last step of that chain. In some jurisdictions, 70% of scams originate online, mostly from online platforms such as social media.

  While in most countries it's extremely complex for financial services providers to share fraud data with other participants, exchanging information between the financial services industry and these platforms is impossible altogether. In particular,

respondents expressed strong support for the FSB to explore fraud prevention in cross-border payments. Some respondents noted that there is no other international organisation who could look at fraud, particularly in the context of cross-border payments. One respondent said that it would be beneficial if the FSB, alongside national crime agencies and other competent authorities, coordinated a forum in which this could be facilitated in a sandbox format to enable effective fraud prevention and data sharing among industry. Any work on fraud should include close cooperation between financial institutions, regulatory bodies, and law enforcement, including but not limited to AML regulators.

1.4. Reducing barriers to innovation (Recommendation 12)

There was good support for promoting public-private partnerships (PPPs) and the sharing of best practices. This is particularly relevant in the AML/CFT regimes as PPPs have demonstrated that they can provide dynamic information sharing on financial crime risks.

One respondent suggested that the recommendation related to supporting innovation could be expanded to encourage national authorities to develop a national or regional plan for LEI issuance with a focus on service providers and emphasise the role of national authorities in prompting broad LEI issuance, by organising hackathons or sandbox projects that explore the national or regional strategies for expanding the LEI population. Such initiatives would also strengthen the service provider ecosystem that leverages the LEI for key functions, such as verification of payee, sanctions screening, and payment processing. Another respondent recognised the role that some national authorities have played in organising sandboxes and public-private sector hackathon events, where institutions can safely work together using emerging technologies to innovate on topics such as financial crime prevention. They would like to use this platform to encourage the public sector to go further, to ensure we tackle all forms of financial crime at the root.