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

Response to Consultation

PayPal

General

1. **Is the proposed scope of the recommendations appropriate for addressing frictions arising from data frameworks in cross-border payments?**

PayPal welcomes the opportunity to share our comments with the Financial Stability Board (FSB) on its proposed recommendations to promote alignment and interoperability across data frameworks related to cross-border payments.

As a global provider offering regulated payment services in more than 200 markets, we experience first-hand the frictions and challenges across different data frameworks in cross-border payments. Fostering a harmonized approach while balancing competing policy objectives is key to enhance cross-border payments and maintaining their safety and security to our customers, especially small businesses and consumers.

We appreciate the FSB focusing on the interaction between data frameworks and cross-border payments, especially given the G20 goal of increasing accessibility, transparency, and speed, and reducing costs, of sending money across borders. As described below, we'd encourage the FSB to consider the following:

- Data, and its free flow, is integral to enabling global payment flows. As such, we welcome the FSB's work to foster greater alignment and interoperability of data frameworks, as it is critical to improve efficiency in transferring payment data across borders. In addition, greater harmonization across jurisdictions would promote broader policy goals such as cross-border trade and economic growth.

- One area where the sharing of payments data across borders is critical is fraud prevention, given the global fraud threat. The fight against fraud is a global and collective issue that demands a coordinated, global response. 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.

- The recommendations adequately address both data privacy and the safety and efficiency of cross-border payments, while balancing the competing policy objectives. We welcome the Forum's creation as a positive step to enhance dialogue between data protection authorities and financial regulators, which is crucial to fostering mutual understanding and cross-border cooperation, with the goal of ensuring that users are able to make efficient and less costly legitimate cross-border payments.

Cross-border payments are at the heart of what PayPal is and does, and we are grateful for the opportunity to share our experience and expertise. We provide our responses to each of the questions, below.

2. **What, if any, additional issues related to data frameworks in cross-border payments, beyond those identified in the consultative report, should be addressed to help achieve the G20 Roadmap objectives for faster, cheaper, more accessible and more transparent cross-border payments?**

The report generally identifies the right issues related to the barriers created by misaligned data frameworks. We notably welcome the mention of fraud prevention in the report, where cross-border data sharing is critical in light of the global fraud threat.

Whilst we support recommendation 9 enjoining competent authorities to create legal pathways for cross-border data sharing, the issue of "hard" localization could be called out and more directly addressed in the report. It's worth underlining that data frameworks that are restrictive of data sharing come in many shades, from specific conditional limitations, to mandating local copies or local processing, to full prohibitions. Regimes forbidding data transfers across borders, or subjecting these to very challenging conditions, remain strong barriers to the free flow of data globally, and inhibit innovation and the development of safe and secure cross-border services.

In addition to legal pathways for data sharing, we moreover suggest considering the concept of "safe harbor" provisions, 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. This would complement ongoing efforts to align AML/CTF regimes and provide much needed legal certainty in the meantime.

3. **Is the proposed role of the Forum (i.e. coordinating implementation work for the final recommendations and addressing existing and newly emerging issues) appropriate?**

We fully support the creation of the Forum proposed in the recommendations. Improving dialogue, mutual understanding and cross-border cooperation amongst regulators, supervisors and international organizations is an essential step towards fostering greater global alignment in an area that is very technical and includes competing policy objectives. A certain degree of friction between data frameworks may be unavoidable given existing and ongoing national prerogatives such as public safety and national security. The Forum's role in promoting enhanced dialogue between national financial and other relevant regulators will be crucial to fostering greater mutual understanding and cross-border cooperation. We urge that the Forum's policymaker representation be broad and diverse to capture priorities beyond the privacy and financial regulatory perspectives to ensure that the

impact of unrelated regulatory activities on cross border payments is subject to appropriate attention and discussion.

The Forum can play a critical role in addressing disparate data transfer adequacy frameworks and methodologies. The current set of systems and approaches leaves much to be desired from an efficiency standpoint due to the uncertainty around which recipient nations might be recognized as “mutually adequate”. Some jurisdictions have a detailed adequacy list whilst others may not. The Forum is an appropriate venue to explore relevant solutions. For example, a more universal approach to adequacy “whitelists” would reduce the costs and time involved with this important data privacy determination. We would also urge the Forum to consider the existing body of data transfer tools that exist to explore how they can be enhanced and more efficient and aligned especially in the cross-border payments context.

We would moreover support the inclusion of the private sector in the Forum, as they can provide practical input, highlight persistent barriers, and support the identification of new and emerging trends in cross-border payments. A standing consultative group could be created, in order to advise the Forum. This group should also include consumer and privacy advocates.

Section 1: Addressing uncertainty about how to balance regulatory and supervisory obligations

4. Discussions with industry stakeholders highlighted some uncertainties about how to balance AML/CFT data requirements and data privacy and protection rules. Do you experience similar difficulties with other types of “data frameworks” that could be addressed by the Forum? If so, please specify.

It may worth considering much more widely the interplay between data regimes that are restrictive of data sharing (privacy/data protection, but also banker-client confidentiality, bank secrecy, state secrecy) and those that encourage data sharing (open banking/finance, regulatory or transaction monitoring for AML/CTF or operational security purposes, collaboration in fraud prevention). Close examination of each of these regimes would be warranted, as these are often multifaceted with different requirements (e.g. consent is required for open banking but not regulatory reporting) that may be misaligned across frameworks.

In particular, the Forum should address the need for cross-border data-sharing for the purposes of fighting fraud. The fight against fraud is a global and collective issue that demands a coordinated, global response. A critical component of this solution involves enhancing international mechanisms for the exchange of fraud-related data across various sectors, including banks, PSPs, telecommunication services, and social media and online platforms. Additionally, relevant authorities and law enforcement agencies should be involved. 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.

Industry participants would benefit from clear, global, rules to share live intelligence, which they can use to evolve and improve their risk and fraud prevention engines, including machine learning and AI detection systems, and to ultimately disrupt, mitigate and prevent fraudulent activity. Participation of competent authorities and law enforcement entities is necessary to be able to react swiftly to new threats and track down and disrupt these criminal enterprises.

The Forum could be a significant means to facilitate and to encourage this exchange of information, ensuring the involvement of regulators and law enforcers, as well as non-financial services participants that support fraud prevention, and the fight against money laundering and terrorism financing.

5. **What are your suggestions about how the Forum, if established, should address uncertainties about how to balance regulatory and supervisory obligations?**

   We have no additional suggestions.

6. **Are the recommendations sufficiently flexible to accommodate different approaches to implementation while achieving the stated objectives?**

   Yes, the recommendations appear to be sufficiently flexible to account for different approaches. The Forum should strive for harmonization and reduce fragment wherever feasible, while still accommodating jurisdictional variations needed to reflect different local infrastructures or cultural, linguistic, and business norms.

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

7. **The FSB and CPMI have looked to increase adoption of standardised legal entity identifiers and harmonised ISO 20022 requirements for enhancing cross-border payments. Are there any additional recommendation/policy incentives that should be considered to encourage increased adoption of standardised legal entity identifiers and the CPMI's harmonised ISO 20022 data requirements?**

   On the adoption of standardized legal entity identifiers in payments, we believe the recommendations should maintain and strengthen the principles of technology neutrality, competition, and interoperability, as well as acknowledge the complexity and richness of the payment ecosystem. For example, all identifiers (beyond IBANs, BCI, or LEI) should be permitted to better account for the multiplicity of payment business models. For instance, concerning account identifiers, whilst we acknowledge that IBANs are a commonly-used payment account identifier in the banking sector, it is worth bearing in mind that many PSPs do not use IBANs as account identifiers. For instance, the PayPal wallet uses the customer's e-mail address as the account identifier. It is therefore important to ensure that any recommendation accounts for multiple use-cases, and embraces technology neutrality, competition, and interoperability.

8. **Recommendation 4 calls for the consistent implementation of AML/CFT data requirements, on the basis of the FATF standards (FATF Recommendation 16 in particular) and related guidance. It also calls for the use of global data standards if**

and when national authorities are requiring additional information. Do you have any additional suggestions on AML/CFT data-related issues? If so, please specify.

It may be worthwhile for the Forum to develop secure, standardized channels for sharing AML/CFT-related data between authorities across borders. This would certainly streamline data-sharing requirements in this space and remove the need for competent authorities to require direct access to firms' data, except in exceptional circumstances.

With respect to FATF Recommendation 16 ("Travel Rule"), we appreciate the call for a consistent implementation of data formatting across jurisdictions to facilitate information sharing.

9. **Industry feedback highlights that uneven regulatory expectations for sanctions compliance create significant frictions in cross-border payments affecting the Roadmap objectives. What actions should be considered to address this issue?**

Legal certainty is key to removing frictions in compliance with sanctions policy. We would encourage the FSB, perhaps via the Forum, to promote greater international coordination on sanctions implementation and encouraging the use of standardized data formats and identifiers in sanctions lists, as suggested in Recommendation 5.

We appreciate the FSB's acknowledgement of friction in sanctions compliance. Sanctions compliance highlights the need to align data sharing policies to allow for compliance with all applicable laws to which PSPs are subject. Data standardization in sanctions compliance could help improve access to cross-border payments, a key Roadmap objective.

One area of conflict is when sanctions obligations in one jurisdiction conflicts with data privacy and acceptable use policies in another jurisdiction. For example, a PSP may have to collect personally identifiable information (PII) from an EU customer on a third-party beneficiary to complete a transaction. Sometimes, this requires checking a U.S. sanctions list to complete the transaction. Given the competing regulations, there can be questions as to whether we can ask for the necessary PII to complete the transaction. It is clear that there are many examples where the service provider could not allow a legitimate payment to be completed. This underscores the need to align data sharing policies, and clarify exceptions, to increase the ability to facilitate cross-border payments.

10. **Do the recommendations sufficiently balance policy objectives related to the protection of individuals' data privacy and the safety and efficiency of cross-border payments?**

The recommendations adequately address both data privacy and the safety and efficiency of cross-border payments, while balancing the competing policy objectives. The Forum's role cannot be understated in this regard, as enhanced dialogue between data protection authorities and financial regulators is crucial to fostering mutual understanding and cross-border cooperation, with the goal of ensuring that users are able to make efficient and less costly legitimate cross-border payments.

Section 3: Mitigating restrictions on the flow of data related to payments across borders

11. The FSB understands that fraud is an increasing challenge in cross-border payments. Do the recommendations sufficiently support the development of data transfer tools that specifically address fraud?

The fight against fraud is a global and collective issue that demands a coordinated, global response. As we underline in our response to question 4, we strongly recommend that the Forum address the need for cross-border data-sharing for the purposes to fight fraud, and we would encourage this to become a dedicated workstream within the Forum's activities. Unnecessary barriers to global and cross-sectoral data and intelligence sharing need to be removed – this is the biggest meaningful step that would permit collective action to really disrupt global fraud and scam models.

In addition to removing barriers to the sharing of data amongst the industry and with authorities, it might also be worth considering the role of "safe harbors" in this space, as referred to under question 2, as well as the role of innovative technologies for fraud prevention that work across borders while respecting data protection requirements.

12. Is there any specific sectoral- or jurisdiction-specific example that you would suggest the FSB to consider with respect to regulation of cross-border data flows?

We are supportive of harmonized cross border data flow frameworks that enable firms to drive efficiencies in their conduct of data transfers and reduce divergence across the jurisdictions in which we operate, while at the same time ensuring business compliance with framework principles. The FSB could consider the EU-US Data Privacy Framework (DPF) as one example of an approach that, in addition to handling complaints and enforcement against business non-compliance, addresses deeper issues tied to country "adequacy" decisions. The DPF introduces an enforcement mechanism available to individuals and designed to challenge national security activities as inappropriately compromising data privacy. A country's standing as adequate impacts a business's cross border activity because it helps reduce complexity and promote the necessary trust with stakeholders that firms rely on to scale their business. It represents a serious effort to balance national security and privacy interests which is instructive for the Forum as it proceeds.

We applaud policymakers that have taken strides to bring more coherence and fewer diverging approaches to cross border data flows. Their investments in promoting greater data free flow with trust are critical to economic growth in domestic and international contexts.

Section 4: Reducing barriers to innovation

13. How can the public sector best promote innovation in data-sharing technologies to facilitate the reduction of related frictions and contribute to meeting the targets on cross-border payments in 2027?

The primary obstacle to global data-sharing is not the lack of technologies and solutions, but rather the lack of global alignment in data frameworks, global coordination between competent authorities and domestic/political sensitivities. We welcome these

recommendations as an important means to bridge the gap between global data frameworks and addressing competing policy objectives.

That being said, we observe and welcome the BIS Innovation Hub tackling important projects in this space, aimed at addressing data sharing and data frameworks in ways that impact cross-border commerce and payments.

We would also note that innovation is primarily driven by business opportunities, including cost reduction. Establishing correct incentives for all participants will drive innovation faster than regulations alone. In this view, we would urge the FSB to consider:

• promoting regulatory and innovation sandboxes to assist firms in developing and test compliant data-sharing technologies

• adopting clear guidance on how new technologies can be implemented within existing regulatory frameworks

14. Do you have any further feedback not captured by the questions above?

We have no further comments at this time. PayPal appreciates the opportunity to provide comments on these recommendations, and we look forward to continuing working with the FSB on the priorities under the G20 Roadmap to enhance global cross-border payments.