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

Response to Consultation

Swift

General

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

   Yes, the scope is appropriate and comprehensive. This is a solid first step towards the creation of an inclusive and open multi-stakeholder dialogue between the public and private sector actors towards the challenges posed by the complexity of non-alignment of data handling practices across jurisdictions with respect to cross-border flows.

   The recommendations in combination with the setup of a forum have the potential to address the industry gap that is widening in times of rapid technological advancement to facilitate collaboration and tackle financial fraud in cross-border payments.

   As Swift has been at the forefront of tackling friction in cross-border payments flows by driving continuous efforts around standardization of data and co-creation of community data services that can reduce friction in the cross-border payments chain, it welcomes FSB's attention to the subject. The proposed scope and recommendations are considered holistic and rightly aim for a standardized approach to data sharing and implementation pathways to ease existing data barriers.

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?**

   There are several underlying causes for friction and costs in the cross-border chain related to data frameworks. Among others, there could be elevated cost of infrastructure, which can be induced due to jurisdictions that imply hard localization or in some cases conditional copy and export requirements. Similarly, procedural variations, especially in KYC and AML practices towards reporting are related areas of friction. Local open banking regulations are sometimes decoupled from the 'hard localization' policies that are implemented in some

jurisdictions making it difficult for private sector players to offer services confidently or to implement frictionless flows.

Finally, the scope of this work should consider beyond the G20 as some of the real frictions, ambiguity or lack of standardization, exist across both G20 and non-G20 jurisdictions, and meaningful results will only be realised if the work targets the broader global community as well.

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?**

The creation of the Forum as an advisory body and co-ordinator is very welcome and much needed. However, as jurisdictions strive for data sovereignty, the Forum's challenge is foreseen to be the extent to which the recommendations are implemented with success and the continued inclusivity across its composition.

We welcome the approach on having private sector advisory. As data has custodians and handlers of different natures from financial institutions to technology providers and overlay service providers to market infrastructures, and Swift with its very unique role, we hope that this can foster a more co-ordinated approach to prepare for better end-to-end governance and interoperability for future financial flows.

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.**

Swift works with and for financial communities across the globe, connecting more than 11,500 financial institutions in more than 200 countries and territories. As such, we are a true global player, and the extensive data of our users when aggregated is a key asset for the effective detection of risk. Several of the innovations and value-added services we deliver for this purpose are for the public good of the whole financial community, increasing the safety and soundness of the global financial ecosystem.

Our vision is to enable the global financial ecosystem with standardized anomaly detection capabilities, supported by collaborative analysis based on the central view we have on our network data, for the identification of financial crime and fraud, that can be invoked anywhere in the processing chain (e.g. with pre-validation during transaction initiation, or during processing).

As a global player however, community success is hindered by the ambiguity and variance of policies and regulation across jurisdictions , and certain participants have shared these are the most significant barriers to adopting global services.

Ambiguity or lack of clear legal pathways limits the value of the cross-border services. As the industry recognises that financial crime, including fraud, cannot be solved by financial

institutions individually, and that global collaboration is required to reinforce the industry's defences, a Forum actively exploring the possibility of collaboration for data related to payments for the purpose of economic crime detection is compelling.

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

   Clear legal pathways to sharing data across borders conditionally or under exceptional scenarios would be very helpful with a clear understanding of the nature of data and the scenarios. Also, a clear way to recommend or restrict the use of AI or privacy enhancing technologies for the same. Finally, the recommendations should make clear the role of the actor in the payments chain the obligations refer to, with the role itself being interpreted in a standardized manner across the jurisdictions.

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

   Yes, we believe at this point the recommendations appear to be flexible.

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?**

   Promoting alignment and interoperability is key to achieving the stated G20 roadmap objectives. Recommendations should focus on adoption of richer and structured data - as supported by ISO 20022, including encouraging the option of structured identifiers such as the LEI, but not solely focusing on LEI.

   Swift has been extensively working to ensure universally understood and accepted identifiers can be used to address, track and predict the behaviour of transactions such as BICs, LEIs and UETRs.

   Recommendations should strike the right balance between encouraging and mandating adoption, as mandating could have unintended consequences as evidenced in a recent FATF R16 consultation where many industry stakeholders commented that mandating LEI for Legal Persons would create challenges for many SMEs .

   A Forum bridging policymaker challenges with those of industry associations and practitioners' views could really add value to the proposed rulemaking.

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.

Overall, we welcome the use of global standards and believe there are many benefits to such an approach. However, we are also aware of the practical challenges which may arise when mandating certain data elements. For example (and as highlighted in Q7) mandating LEI for Legal Persons could create challenges for many SMEs.

To find a practical way forward, we believe close cooperation between public authorities/regulators and the public sector is necessary. A forum with the insights of relevant stakeholders could provide great direction on the practicalities, benefits and consequences of proposed changes to regulations and data requirements.

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?**

Swift has been collaborating with the Wolfsberg Group since 2012 to help Sanctions List authorities standardize the structure of their lists. A data model was created for the United Nations, which was adopted by the US Treasury OFAC. So far, uptake by other authorities/regulators has been limited. However, we would welcome further exploration around this and other similar existing initiatives to address and draw clarity on existing attempts by the industry and how these can help progress on the Roadmap objectives, especially as data requirements are evolving.

The question of interoperability between instant payment schemes is another area where collaboration on how to address AML/CFT requirements would greatly benefit from a Forum approach.

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?**

Swift believes that the recommended measures will significantly enhance the technical and operational efficiency of solutions for cross-border data sharing. The proposals advocating for common standards in data format and identifiers will indeed streamline operations and improve interoperability among stakeholders. For instance, the recommendation for national authorities to encourage the adoption of the Bank for International Settlements' Committee on Payments and Market Infrastructure (CPMI)'s harmonized ISO 20022 data requirements is a clear example of how adopting common standards can reduce fragmentation and improve the speed, cost, and transparency of cross-border payments.

However, we believe that the establishment of a robust legal framework, along with harmonized guidelines for localization and processing practices, presents an even greater opportunity for impact. The text highlights that discrepancies in legal requirements and supervisory expectations across jurisdictions can lead to significant compliance challenges. By harmonizing usage and accepted behaviour concerning localization, as mentioned in Recommendation 9, we can mitigate inefficiencies caused by data localization policies that can impede effective payment processing and increase operational risks.

Such legal harmonization not only bolsters overall efficiency but also fosters a more dynamic and responsive environment within the industry. As noted, creating clear pathways for cross-border data transfer and sharing, as stated in Recommendation 10, will empower market participants to comply with regulations while maintaining a seamless flow of information. By addressing these legal and procedural aspects, we can create a foundation that supports innovation and facilitates smoother, more secure cross-border transactions.

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?

There is inherent value in balancing the effectiveness of transparent data sharing with the protection of individual privacy, particularly amidst diverse legal and regulatory frameworks. The recommendations outlined do promote transparency and encourage dialogue around these essential efforts, as seen in Recommendation 7, which calls for the OECD and relevant stakeholders to explore options for enabling faster, less costly, and more accessible cross-border payment-related data flows while ensuring high levels of privacy protection.

However, while these suggestions are positive and contribute to the notion of transparency, they fall short of formalizing common standards to the extent necessary for achieving the interoperability proposed in other recommendations. For instance, Recommendation 3, which advocates for the adoption of the Bank for International Settlements' Committee on Payments and Market Infrastructure (CPMI)'s harmonized ISO 20022 data requirements (which is crucial for standardizing data formats used in cross-border payments) is more precise.

While we view these recommendations as a step in the right direction, there remains a significant amount of work to be done to establish comprehensive standards that will guide consistent practices across jurisdictions. Formalizing these standards and driving adoption is essential to enhancing both data interoperability and privacy protection. This necessity is underscored by Recommendation 4, which emphasizes the need for national authorities to implement FATF Recommendation 16 to avoid inconsistencies in data requirements related to AML/CFT compliance. By addressing these gaps, we can enable more effective cross-border data sharing without compromising individual rights.

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?

Please refer to some examples quoted against context in answers above.

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 public sector can significantly enhance data sharing and regulatory facilitation of fraud prevention by establishing clear goals and long-term incentives for private sector investment. In this context, while specific technological choices are important, they are secondary to the need for consistency in market practices that enable sustainable investment.

For instance, the recommendations related to harmonizing ISO 20022 data requirements (Recommendation 3) underscore the importance of standardization, which fosters a predictable and stable environment for market participants. This consistency is vital for encouraging long-term investment and innovation in fraud prevention technologies.

Moreover, the recommendation for national authorities to implement FATF Recommendation 16 (Recommendation 4) speaks to the necessity of a common framework for compliance that would further reduce fragmentation in data requirements. By prioritizing such consistency in regulatory and operational practices, the public sector can create a more favourable landscape for private sector engagement in fraud prevention initiatives.

Recent breakthroughs in federated learning and privacy-preserving technologies have the potential to unlock opportunities for financial institutions to share insights, address frictions and collaborate to solve industry-wide challenges. Leveraging privacy-enhancing technologies, it could be possible for institutions to share insights in a way that remains wholly anonymous. Used in conjunction with federated learning there is potential for market participants to gain collective insights from their aggregated datasets, without sharing their actual data.

A specific focus by the public sector to align on standards, regulation and operational guidelines for the use of privacy-preserving technologies and AI would be welcomed to help drive adoption of these technologies in a cross-border payment context.

Ultimately, it is this alignment around consistent practices and clear objectives that will drive effective collaboration between public and private sectors, leading to more robust data sharing capabilities and improved safeguards against fraud.

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

-