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

Response to Consultation

Institute of International Finance

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.

   ● We appreciate the FSB's initiative to remove frictions from cross-border payments.

   ● The holistic approach taken by the FSB is commendable and reflects the complexity of the issues at hand.

   ● It also aligns with the IIF's previous recommendations for addressing data barriers through a multi-stakeholder forum, addressing data localization and other data barriers such as regulatory fragmentation and inconsistent implementation, and standardized pathways for data sharing. Those recommendations are contained in our January 14, 2022 submission to the FSB on data frameworks and cross-border payments, and our suggested case studies on data frameworks' impact on cross-border payments, provided to the FSB on October 30, 2023, and our September 2023 staff paper on payments security and trust.

   ● While commendable, the FSB recommendations should have at their center an overarching objective of building greater levels of trust between jurisdictions. While jurisdictions may have various reasons behind data localization, almost all of them are fundamentally due to a lack of trust.

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 IIF had previously (in its January 14, 2022 submission to the FSB on this topic) identified several kinds of data barriers:

   o conditional limitations on data export (for example, on personal identifying information);

o local copy or processing requirements;

o "hard" localization, i.e. outright prohibitions on data export, or where export is only permitted under very challenging conditions (such as individual regulator approvals);

o regulatory fragmentation (e.g., in implementation of KYC and AML rules); or

o inconsistent implementation of international payment message standards and the data required to be included within payment messages.

● The proposed legal pathways for data sharing are strongly supported and reflect past suggestions on the IIF's part. In general, we support well-defined legal pathways to sharing data across data barriers where necessary or appropriate for reporting, compliance, and risk management, including on a cross-border basis, as a structured exception to data barriers of all kinds. In our January 14, 2022 submission, we advocated for the establishment of different types of legal pathways at B2B, B2G and G2G levels. This could go beyond the specific B2B legal pathway identified in Recommendation 9 and extend to B2G and G2G legal pathways.

● While the FSB recommendations directly address most of these issues, the issue of "hard" localization could be called out and more directly addressed. This goes beyond local copy or processing requirements and extends to outright prohibition of data export under e.g. state secrecy legislation or local supervisory requirements.

o The Forum could work with industry on more productive pathways towards data flows with trust, exploring some financial regulators' concerns that they could be potentially unable to discharge their regulatory duties absent such requirements.

● The mention of fraud in the recommendations is welcome. This would imply close cooperation between financial institutions, regulatory bodies, and law enforcement (including but not limited to AML regulators) in all countries in scope.

● Given the prevalence of "one leg out" issues as drivers of cross-border frictions, the FSB is encouraged to consider the non-G20 aspect of its recommendations further. There may be a need to set up a process similarly to what has been done with regard to crypto and stablecoins to ensure that there is momentum to implement the FSB's recommendations beyond the G20 members.

● In parallel to the assessment and desirable removal of barriers to the cross-border flow of payment data, the possible role of new technologies, such as PETs, in addressing data framework challenges while maintaining security and compliance could be explored given the need for all to better understand their implications and potential as alternative/complementary tools.

o Coordinating with the OECD Data Free Flow with Trust (DFFT) Expert Community, which is pursuing work on PETs, cross-border payments, and enhancing legal transparency around data rules, could help drive this work forward.

o When exploring how PETs can help overcome data framework frictions, however, it is important to ensure that regulatory frameworks themselves remain technology-neutral.

Although public-sector support for PETs development and adoption in collaboration with the private sector would be welcome, regulatory frameworks should not create requirements to adopt specific technologies.

● In addition to legal pathways for data sharing, consideration could be given to "safe harbor" provisions that provide shelter from liability to corporates that undertake good-faith efforts to pursue cross-border payments regulatory imperatives such as safety, soundness, anti-fraud, AML/CFT, and risk management.

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?

● Yes, the proposed role of the Forum is welcome.

● It is welcome that the proposed Forum is to include all or nearly all stakeholders. As to its composition and governance:

o It is proposed that the Forum will be "established by the FSB, in collaboration with the OECD, GPA and FATF" and will include "stakeholders from" various other public sector bodies. It would be helpful if those other bodies were more clearly identified.

o There should be recognition that the G20 does not represent all impacted countries, though it does provide a useful venue for advancing some objectives. The Forum should, ideally, make recommendations that have some political endorsement to provide buy-in and momentum for implementation.

o We have appreciated the opportunity to participate in the LRS and PIE taskforces, and think that adopting a similar mechanism for facilitating collaboration between the public and private sectors could be constructive.

● As to the mandate of the Forum, suggestions from our previous work on this topic (cited in our answer to question 1) that could be considered by the Forum as priorities include:

o 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.

o MOUs could be explored further by the Forum, including how they could be more usefully brought to bear on this topic. Our members have noted that often financial regulators will bring in extra requirements for why data should be partially or fully localized.

● Other suggestions from our previous work that the Forum could take forward include:

o Enhancing clarity, consistency, and the development of best practices around what kinds of data (e.g. sensitive information) are subject to protections and higher compliance burdens;

o Standardization of AML/CFT information sharing practices;

o Development of regulatory data access arrangements;

o Implementation of adequacy/equivalence assessments for cross-border transfer regimes and other mechanisms permitting cross-border data exchanges such as binding corporate rules and standard contractual clauses; and

o Consideration of IT platforms for secure cross-border regulatory information exchange.

• We observe that cross-border data sharing for fraud prevention is an important priority for the financial services industry at this time. While acknowledging the multitude of channels already in place for the exchange of information about particular frauds and financial crime typologies, the Forum may be able to serve as a non-duplicative venue to explore impacts and encourage the more efficient exchange of information, including across regulators, law enforcement, and non-financial service participants.

• As mentioned in our answer to question 2, the Forum should also coordinate closely with the OECD DFFT Expert Community to reduce potential duplication of work. We would appreciate any clarity that the FSB could provide on how that coordination could occur and on the respective roles of the FSB and OECD in collaboratively pursuing shared/aligned objectives.

• See generally our answer to question 2 as to other issues to be addressed by the Forum and its members.

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 is important to recognize that there are many different data frameworks or regimes that are restrictive of data sharing (e.g. personal data protection, banker-client confidentiality, bank secrecy, state secrecy, constitutional provisions or local supervisory requirements) and others that either permit or require data to be shared (e.g. open banking, regulatory reporting, transaction reporting, travel rule, etc.). Regulatory and transaction reporting requirements are multifarious and can arise under AML/CFT, securities, derivatives, prudential, payments or other regimes. Open banking regimes require customer consent but reporting regimes rarely do so. In many cases, these requirements to share or report data may also apply across borders.

• It may be helpful to study some particular measures that go beyond personal data protection and extend to "hard localization." Some of these were included in our suggested case studies on data frameworks' impact on cross-border payments, provided to the FSB on October 30, 2023. See our answer to question 12 for further details.

• Another reporting framework in potential conflict with restrictive data frameworks is the EU's Central Electronic System of Payment information (CESOP) framework which

obligates payment service providers (PSPs) to report cross-border transaction details to tax authorities in the EU. The framework contains many edge cases; each reported transaction not in scope is a violation of data protection or banking law.

- The problem of edge cases is one motivation for our suggestion in answer to question 2 about liability safe harbors.

- It should be acknowledged that some divergencies and inconsistencies in data frameworks stem from provisions in horizontal regulations, given existing and ongoing national prerogatives such as public safety and national security, or even in a given country's Constitution or fundamental laws. Consequently, the actions to overcome the frictions in cross-border payments created by these disparities must factor in this reality.

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

- In general, we support well-defined legal pathways to sharing data across data barriers where necessary or appropriate for reporting, compliance, and risk management, including on a cross-border basis, as a structured exception to data barriers of all kinds. See our responses to questions 2 and 4 for more detail.

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

- While the recommendations appear sufficiently flexible, it's also important to ensure they do not lead to further fragmentation.

- The IIF has previously identified a lack of consistent implementation of data standards, along with regulatory fragmentation, as forms of data barriers.

- The Forum should work towards harmonized implementation approaches where possible, while still allowing for jurisdictional differences that are necessary to reflect different local infrastructure or cultural, linguistic or business norms, to the extent that they do not materially impede global interoperability. This balance will be key to achieving the stated objectives consistently across different regulatory environments.

- Moreover, efforts taken to remove barriers to cross-border data flows should not, to the extent possible while removing these barriers, impose changes in the processing of local payments, as changes in payment infrastructures and services are usually costly and time- and resource- consuming.

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?**

• Our membership sees value in use of the FSB's preferred Legal Entity Identifier (LEI) in cross-border payments; however, there are concerns about mandating a single identifier at this time.

• We note that the CPMI harmonized requirements for ISO 20022 (at p. 25) recommend, but do not mandate, the use of BICs or LEIs as global identifiers, but also allow for other identification types. (If an identification other than BIC or LEI is used, then it is required to provide the Scheme Name and Issuer of the identification.) We consider this strikes the appropriate balance.

• The scope of standardized legal entity identifiers including the LEI goes well beyond ISO 20022 requirements and could be helpful in other areas, e.g. newly emerging domestic payments systems, fighting fraud, money laundering and tax evasion.

• However, the costs of LEI adoption in the complex retail cards ecosystem, could outweigh the benefits, especially considering that leading cross-border payment schemes already have robust mechanisms for identifying the parties (including potentially liable parties) in a transaction. Some considerations include:

o the 20-digit, alphanumeric structure of the identifier would create operational and infrastructural challenges;

o liability in the case of incorrect LEI reference information (e.g. through mergers, etc.) or incorrectly quoted LEIs may be unclear;

o the use of LEI is still very low in many jurisdictions and not all payment parties have an LEI or can even obtain one; and

o the usefulness of LEI adoption to payments processes including sanctions screening is limited by the fact that individuals cannot be issued LEIs.

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.**

● To improve AML/CFT effectiveness, the Forum could consider scope for Privacy Enhancing Technologies or techniques such as pseudonymization and compartmentalization of shared data to balance data protection with the need for effective AML/CFT mechanisms. Use of tokenization and ledger technologies present potential opportunities for innovation of such solutions.

● Additionally, the Forum and national authorities could support the use of existing secure channels and encourage their development where not already in place, including between authorities.

● It should be taken into account that FATF Recommendation 16 is under review and some of the options proposed in that review would be highly costly to implement.

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 sanctions compliance. We recommend promoting greater international coordination on sanctions implementation and encouraging the use of standardized data formats and identifiers in sanctions lists, as suggested in Recommendation 5. This approach would align with the IIF's previous calls for reducing fragmentation in regulatory requirements.

● As the IIF noted in its September 29, 2023 staff paper on payments security and trust, industry stakeholders have put forward several recommendations around sanctions screening processes in the past, including:

o more consistent application of sanctions screening requirements across jurisdictions;

o best practices on issues such as complying with list-based sanctions and comprehensive sanctions, importance of a principles-based focus, screening of aliases, whitelisting of false positives, and use of emerging technologies (e.g. machine learning) to reduce false positives;

o standardizing sanction list formats, the interpretation of contents, expected responses associated with listings, and list distribution approaches; and

o increasing uniformity in the list entries and greater use of structured identifiers and digital identities, including in beneficiary information.

● SWIFT has presented a program for the community to remove sanctions friction through collective action, which includes designing and documenting screening practices and supporting data quality principles for ISO 20022 messages through industry collaboration.

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?**

● While the recommendations address both data privacy and payment efficiency at a high level, the proposed Forum should further explore this balance along with the associated costs of achieving these objectives.

● Continued dialogue between data protection authorities and financial regulators is crucial. The IIF has previously advocated for such cooperation to ensure that data protection and efficient cross-border payments can coexist. We emphasize the importance of ongoing industry consultation in striking this balance.

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 recommendations address the right topics, and helpfully identify that data localization requirements can inhibit fraud mitigation, but are still too high-level to assess their impact on fraud operations.

● We support the recognition of the impact of fraud and the costs to payment service providers from this increasing challenge. The fight against digital fraud and scams is a challenge whose impact is most frequently faced directly by the financial sector (banks and PSPs). We support more shared responsibility with other sectors (e.g. telecommunications, social media platforms), and better coordination across sectors by security and enforcement agencies. To be clear, the IIF does not intend to recommend the FSB expand its mandate beyond issues of financial stability into fraud prevention.

● The IIF supports awareness of the importance of evaluating the cost of payments in this context, recognizing the role of the private sector in combating fraud and the importance of its ability to share data to do so successfully. The IIF hopes that the work of the Forum and these recommendations will drive more balanced consideration of these factors at the national level, if FSB highlights them.

● It is important to continue promoting innovative technologies for fraud prevention that work across borders while respecting data protection requirements.

● We have advocated for data sharing pathways with appropriate controls at different levels for cross-border payments purposes, as we note in our response to question 2.

● In this context, it would also be desirable, if very challenging given the need to involve other arms of government, to clarify safe harbors from liability (for example, from civil liability for defamation or injurious falsehood) where good faith efforts are made to report fraud that later turn out to be a false positive or based on incorrect information.

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?

● In terms of data barriers to be addressed, as highlighted in section 3 of the IIF's October 30, 2023 submission on suggested case studies, the impact of different types of data localization requirements in India, China, and South Korea on cross-border payment services is material. The Forum could consider these regimes in detail, perhaps through consideration of one or more stylized examples.

o The Reserve Bank of India's Storage of Payment System Data notice requires payment system providers to ensure that data relating to systems operated by them are stored only in India. This data should include the full end-to-end transaction details or information collected, carried or processed as part of the message or payment instruction. For the foreign leg of the transaction, if any, the data can also be stored in the foreign country, if required. In case the processing is done abroad, the data should be deleted from the systems abroad and repatriated not later than one business day or 24 hours from payment processing, whichever is earlier.

o As another example, early in 2019, a China Banking and Insurance Regulatory Commission decree was issued that prohibits the cross-border transfer of all customer

identification information and transaction information obtained in the course of performing AML/CFT obligations.

o Such requirements mandate global FIs to put technology, people and processes within the jurisdiction to perform AML/KYC duties or other functions and means they are unable to leverage global operating and support models, resulting in increased operational challenges and risks.

o South Korea's 2016 Protection of Location Information Act imposes spatial and location data transfer restrictions primarily to protect national security interests, additionally to the 2011 Personal Information Protection Act. The cross-border transfer of personal information of South Korean citizens is subject to certain notification obligations and requires additional, specific consent.

● Another example of a material data barrier considered in that submission is the EU-US "data bridge", the question being whether it presently provides sufficient certainty in the medium-term to encourage investment in data sharing arrangements that are desirable to reduce fraud and counter AML/CFT in cross-border payments.

● In terms of examples of addressing barriers that could be useful, adequacy assessment and decisions that officially acknowledge the equivalence of the data protection frameworks of two countries are useful tools. The adequacy decisions taken by the European Commission in accordance with General Data Protection Regulation (GDPR) are an example of this.

● Other tools that are available in the context of the GDPR that may be helpful examples include binding corporate rules or, for some purposes, standard contractual clauses with "docking" clauses.

● Regional or plurilateral data sharing arrangements such as the GDPR and the APEC Cross-Border Privacy Rules (CBPR) system, and the Global CBPR Forum, could be encouraged where assessed beneficial.

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?

● Innovation is primarily driven by business opportunities, including cost reduction.

● Establishing correct incentives for all participants will drive innovation faster than regulations alone.

● We would emphasize that the primary obstacle to global data-sharing is not the lack of technical means, but the lack of global alignment in data frameworks, as well as the lack of global coordination between competent authorities and domestic/political sensitivities. Political buy-in as to the importance of global data-sharing is essential.

● While insufficient on its own in this case, the public sector should continue to foster public-private partnerships, create regulatory sandboxes for testing innovative solutions, and provide clear guidance on how new technologies can be implemented within existing regulatory frameworks.

● The IIF is encouraged to see the BIS Innovation Hub tackling projects that address data sharing and data frameworks in ways that impact cross-border commerce and payments, and believes these aspects of potential projects will be increasingly important to undertake.

● As mentioned above, FIs need to be able to transfer data to service their customers, to manage risk and comply with a complex web of regulatory requirements. This is only going to continue to be possible if current trends towards greater restrictions in data transfer are addressed. The fundamental requirement It would be desirable to achieve a position where transfers are made pursuant to mutually recognized standards of protection which are recognized internationally.

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

● The FSB consultation report on data frameworks shows considerable alignment with industry concerns and suggestions (as well as other stakeholders' previous suggestions), including those raised by the IIF in previous submissions and papers on this topic, notably our January 14, 2022 submission to the FSB on data frameworks, our October 30, 2023 suggested cases studies as submitted to the FSB, and our September 29, 2023 staff paper on payments security and trust.

● Key areas of alignment include addressing data localization challenges, promoting standardization and harmonization of data requirements, supporting the use of standardized identifiers, establishing a forum to balance regulatory obligations, promoting innovation to address data frictions, expanding cross-border cooperation, and considering the impacts of data-related policies on cross-border payments. The report's recommendations largely reflect the industry's calls for reducing barriers to efficient cross-border data flows while maintaining security and regulatory compliance.

We are in favor of relevant authorities considering potential impacts on consumers and cross-border payments market participants when designing their data-related policies. Authorities should assess and keep at a minimum the (economic, operational, ...) impact that introducing requirements aimed at enhancing cross-border payments could have on local payment services and infrastructures.