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

Response to Consultation

UK Finance

General

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

   We welcome and support FSB's role as well as the recommendation. In taking this forward it is imperative that substantial implementation efforts be managed in partnership with market practitioners. A balance should be struck with individual rights and freedoms such that they are not eroded in the quest for a more frictionless transfer of data.

   Addressing frictions arising from data frameworks in cross-border payments must take a holistic approach. This approach needs to address end-to-end data quality starting from the initiator of the payment through the payment chain and ending at the ultimate recipient.

   Textual legal / rule differences and technical / network validation differences require addressing concurrently so frictions addressed at the legal / rule level are proven to be effective when individual pieces of data are proven to be able to travel with less friction.

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?**

   We encourage the forum to consider providing or facilitating central management of data to address challenges globally and reduce duplicate work and interpretation. For example, the EU data strategy includes a series of legislative initiatives to foster data exchange which aligns to one of the objectives: addressing data flow restrictions. In particular, Chapter VIII may have elements that could be leveraged to facilitate interoperability efforts in the international payments context.

   In considering data frameworks for cross-border payments, clear linkage of recommendations to the measurement of the G20 roadmap objectives would be beneficial

for the market to prioritise. In taking forward work on data frameworks in cross-border payments, UK Finance members recommend the following should be addressed:

- Standards: there are potential inconsistencies in how information such as name and address are formatted. One example is “state” in US, “province” in China, and “county” in UK. Another example is the challenges of translating local Arabic names to Latin alphabet, often there are different possible spellings and therefore coordination and consistency is required globally across different type of message in format for AML. Additionally, the data formatting between various sanction lists could be different resulting in potential errors, higher level of manual interventions and delays. As a result, a level of standardisation with machine readable list would be hugely beneficial – it also makes it easier and faster to keep up with updates and changes.

- Data interoperability: Enhancing data interoperability and data mapping quality could play a part in mitigating frictions while recognising the different needs of each jurisdiction. For example, while LEI and BIC serve different purposes, and equally, some jurisdictions may have a preference on one ID over another (for example, the US being more SWIFT centric, relies more heavily on BIC). Instead of data standardisation, enhancing data interoperability across the different systems throughout the end-to-end payment chain would be a more realistic approach to enhance the accuracy, consistency, automation and speed of payment flow. LEI provides a more complete and transparent view of the entities involved in the transaction. This could be helpful for risk management, fraud detection and sanction screening purposes. Nevertheless, different jurisdictions will have different preference on unique identifiers. This may involve partnership with organizations such as SWIFT and GLEIF.

- Transparency: Not knowing the cause of friction is the source of ambiguity. Transparency of differences across different markets often solve for more than trying to negotiate changes across different domestic markets. In this sense, publication of differences should have greater focus as it provides certainty to the markets on friction points.

At a more granular level, confidentiality of data (banker’s duty of confidentiality) is a key issue (in addition to data protection issues). We’d suggest that disclosure of personal data by a participant to a regulatory authority to meet regulatory / legal obligations should not be treated as a breach of duty of confidence (and should therefore avoid any civil liability claims). This principle could be embedded within the framework, though individual countries would then need to review their domestic laws in order to ensure this is clear in their jurisdiction. The civil liability protections in the UK’s Economic Crime and Corporate Transparency Act 2023 may be a helpful point for reference.

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 agree with the proposed role of the Forum as set out in the FSB’s consultation and presume that the enforcement would be through domestic regulation. In coordinating of the work for final implementation, we suggest that the Forum give consideration to:

- Industry practices: end to end data quality across the payment chain relies on how the end client provides the data against what message format is implemented in each market

or network. Therefore, renewed emphasis should be given to message format usage practices and end client incentives.

• Public sector, with private sector consultation: We support that the proposed Forum working effectively with private sector and existing fora (for example the Payments Market Practice Group). Indeed, we suggest that the FSB extend their proposal to identify private sector stakeholders to serve in an advisory capacity by considering co-option on the Forum of relevant private sector experts. Closer and ongoing public and private sector collaboration, with the relevant private sector involvement, will provide the Forum with better oversight over coordination of the implementation and, importantly, have oversight on the end-to-end implementation of the guidance.

- Implementation: As data flows begin and end with the clients, the proposed Forum should also give consideration to the end client and also perhaps on how to incentivise clients to include the correct and complete information.

- Horizon scanning: we suggest that the Forum should encourage public sectors to flag upcoming data related rules that could have impacts on cross-border payments and also consider a process to ensure that new potentially emerging divergences and inconsistencies are addressed as they arise.

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.

The Forum could give consideration to additional areas where the industry faces uncertainties when balancing data compliance requirements with data privacy and protection rules.

The recent discussion with FATF on R16 brought to light similar issue in card transactions, and it was potentially deemed sufficient that the reference data standing behind identifiers (e.g. merchant IDs, card numbers) can be made available to law enforcement upon request. Consistency of AML/CFT data requirements and data privacy and protection rules across payment types will be important especially as payment use cases using card rails are expanding.

We note that the ongoing FATF R16 review will separately consider principles on what data originating from the payer should travel through the payment chain as part of the payment message; what (if any) data could be supplemented throughout the payment chain; what data should remain as information obtained through additional investigation at each of the cross-border payments market participants; what data are not allowed to travel through the payment chain. These principles should be clearly set out as part of the R16 review.

Further, consideration needs to be given to how, who and where the data is being processed i.e. use of Artificial Intelligence which brings its own risks.

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

We welcome the opportunity to help shape how the Forum, if established, could help to balance uncertainties about balancing regulatory and supervisory obligations.

Engagement with the industry through established community groups would provide insight from the participants as to how to address uncertainties in balancing regulator and supervisory obligations, while consultations would provide opportunities to shape discussions.

We suggest that the Forum should be able to issue specific guidance and be called upon to opine on specific use cases. With further innovation in payments the market will encounter new user cases that require analysis, review and stakeholder engagement.

The Forum should validate any recommendation against specific use cases where the context of the payment and usage of particular data is put to a test that is specific and measurable. While coordinated public private partnership should be taken forward to assess emerging recommendations.

We suggest that the Wolfsberg Group, an association of 12 global banks which aims to develop frameworks and guidance for the management of financial crime risks, provides a good example of provision of coordinate guidance.

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

The Forum should develop objective metrics when putting forward recommendations that effectively address the G20 objectives. In this way, the various recommendations can be compared against its perceived benefits as a basis of policy decisions.

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?**

The industry is supportive of the increased adoption of standardised LEI and harmonised ISO 20022 requirements for enhancing cross-border payments, but these require coordinated and consistent implementation support and guidance to enhance cross-border payments. Further consideration could be given to:

- Further granularity for extending the use of LEIs, for example, to support branches of legal entities located in the same jurisdiction.

- Data interoperability such as how LEI can be mapped to BICs and vice versa (and possibly map to local unique identifiers). Different jurisdictions will have different preferences for unique identifiers so that enhancing data interoperability could reduce friction while recognising the different needs for each jurisdiction.

- Linkage between card-based identifiers and LEIs should be established – there is reference data that links BICs to LEI and the same should be established for BINs and Merchant ID to LEI.

- Analytics, for example, it has been reported that the Bank of England is developing an analytics tool with the BIS Innovation Hub London centre on a project that will explore how technology can enhance the analytical use of ISO 20022 data to shed light on economic conditions, system liquidity and compliance.

While we are supportive of the alignment and interoperability of regulatory and data requirements it is important that the FSB recognise that harmonisation will take time, will provide an operational challenge, and some of the CPMI requirements are not within the gift of the banks, for example, it is the underlying clients that will have to provide remittance data. Similarly with LEI, very few firms have an these and there is long way to go to get ubiquity: in the UK less than 200,000 from around 4 million businesses have LEIs. These businesses will have to step through a process of getting an LEI, renewing it and provide additional data with their payments even if they make a few cross-border payments a year.

To meet the scope of the implementation challenges the FSB or the proposed Forum could identify which ISO harmonisation recommendations would move the dial for combating financial crime and encourage standard setters to prioritise them.

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.**

UK Finance members have suggestions to aid consistent implementation of AML / CFT data requirements, in particular, for enhanced clarity, transparency and information, for example, clarity on whether information that is required for one national authority should or should not travel through the payment chain.

Additionally, current known issues include the use of purpose of payment often using national codes that have no relevance outside the given domestic market. Other cases include the requirement to investigate beneficial owners of parties visible in the payment chain for sanctions compliance purposes in a particular market.

Transparency over different data requirements and extent of due diligence required can solve for a significant part of the ambiguity in the current market.

However, our members note that issues are not just about the interoperability of the data but also the regulatory context that forces some data to be inserted. Firms use filters similar to that used for Sanctions to look for missing data within payments but also where

meaningful information is replaced, “unknown customer” in place of someone’s name for example.

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?**

Addressing the issues of uneven regulatory expectations for sanctions compliance would be welcomed.

The provision of specific guidance on what a risk-based approach entails in each market and measurement of the differences against FATF mutual evaluation progress would be a positive development. This would showcase how a high-risk party is identified, how a high-risk transaction type is identified and what due diligence is considered necessary to rule out a particular party being a sanctioned entity.

With regard specifically to SEPA Instant Payments there are differences in screening approaches across SEPA payments: intraday transactions screening is not allowed whereas PSU screening is required. The rationale is that they now also require customers to be screened daily by all participating FIs and that any updates to the EU list are made immediately to screening systems. A number of firms screen customers daily already, for example, following their internal guidance to have up to 36 hours from source list update to live within their filtering systems. The European Commissions have also stated that any duplicated Sanctions entities on lists other than the EU must also not be filtered. This puts some firms in an impossible situation as they have payment scheme guidance to adhere to but also their regulatory Sanctions responsibilities. Consequently, some firms don’t have an agreed go forward position and require further clarity.

We also noted that the timeframes to implement for EU entities under the IPR are short for many PSPs and the lack of clarity surrounding screening have increased the burden on PSPs. The SEPA Instant payments scheme response time is 10 seconds as to whether the PSP will accept the payment or not. For any Sanctions hits, it would be impossible to conduct manual investigation in this time frame to determine if hits are false positive or not - the likely decision will be to automatically reject the payment. It is plausible that this problem will become apparent with other schemes as we see a move to payment schemes tightening their turnaround times. The scheme guidelines and Sanctions requirements need to both be considered going forward avoid such conflicts.

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?**

UK Finance members note that the individual rights and freedoms should not be eroded in the push for a more frictionless transfer of data. To balance policy objectives with individual’s data privacy, consideration could be given to the provision on a consistent consumer disclosure. One approach could be the encryption of individual fields so parties that have a need to know that particular data can have select access, but the impact of this approach should be fully assessed with the focus on delivering the right end outcome.

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?

Further consideration needs to be given to addressing challenge of fraud in cross-border payments.

One element to be considered is the standardisation and interlinking of domestic / regional verification of payee schemes, such as Confirmation of Payee in the UK. Firms' ability to verify account name and other details could be a useful tool in mitigating levels of fraud in cross border payments.

For accounts owned by legal entities, the pre-validation process will be easier to confirm if an account is owned by specific BIC or LEI (vs. than by name), especially if the master data is using a different character set.

Additionally, consideration should be given to the increasing use of AI as a tool to combat fraud but to do so in a consistent manner.

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?

There are a number of specific examples the FSB could consider with respect to regulation of cross-border data flows:

- Data localisation rules that directly impact cross-border payments including India RBI's Storage of Payment System Data notice1 and China's National Financial Regulatory Administration (former China Banking and Insurance Regulatory Commission) decree2 CBIRC (2019), Banking Financial Institutions Anti-money Laundering and Counter Terrorist Financing Management Measures (Decree No. 1).

- Prohibiting the cross-border transfer of all customer identification information obtained in the course of performing AML/CFT obligations.

- Broader data localisation requirements such as the ones in SEBI Cloud Framework. Those broad localisation requirements will negatively increase cost doing business, undermine risks management ranging from AML to cyber, and reduce resilience, which in turn lead to costly, insecure, and inefficient cross-border payments.

- Give specific consideration to local laws requiring data localisation, for example, the laws within Germany mandate that data originating within Germany stays within its borders.

- There are differing requirements on preventing consumer harm which require harmonisation.

In addition, FSB should establish a mechanism through the proposed Forum could address emerging and ongoing data localisation requirements.

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 play a crucial role in creating the right conditions that promote innovation, to include initiatives such as through the:

- creation of safe harbour laws to allow cross-border exchange of data related to fraud;

- promotion for the development and use of best practice and other technical tools to facilitate matching of names and addresses, to reduce friction and increase speed while promoting transparency;

- promotion of pre-validation as best practice;

- provision of a clear and reasonable legal pathway, by national authorities, for cross-border payments market participants to transmit across borders data related to payment processing, risk management, or fraud and financial crime prevention;

- provision, where applicable, of alternatives to requirements to use local computing facilities;

- encourage the use of privacy enhancing techniques.

One example for the potential involvement of the public sector is at a central government level in the UK where there an opportunity to align to other markets where tax, ID, National Insurance numbers are more prevalently used within payment messages.

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

Additional points for consideration include:

- The GDPR (see Art 40) provides for “Codes of Conduct” which assist parties in meeting data protection requirements and require approval from local regulators. This is a tool which could be utilised by the Forum.

- Regulation of non-bank PSP owned payment technology and infrastructure should be considered to ensure customers are protected from potential harm and also to ensure that their rights are protected under data protection legislation respected.

In addition, we would suggest reaching out to the Global Cross Border Privacy Rules Forum3 (UK is a member) which supports a framework for effective protection and flow of data internationally for any key learning points.