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

Response to Consultation

Australian Payments Network

General

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

With respect to Recommendations 1 and 2, we agree that a forum be established by the FSB in collaboration with the OECD, FATF and GPA to collaborate on policymaking to resolve data framework frictions. Inclusion of other relevant stakeholders is also supported.

In terms of Recommendation 3, as we have stated publicly, we agree that ISO 20022 will reap greater benefit with harmonisation. Market Infrastructure Bodies such as HVPS+, IP+ as well standard setting bodies such as CBPR+, are appropriate bodies that could and should be tasked with driving consistent implementation of ISO 20022 in conjunction with other Standard Setting Bodies and other critical stakeholders. We recommend that CPMI should consider providing leadership and organisational structure to facilitate this important work.

Our experience in 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.

The Australian Community recognises that FATF's Recommendation 16 revision has yet to be finalised. Nonetheless, we agree that its implementation and application should be consistent and that national authorities have a distinct role to provide clear and accessible guidance which should also extend to any local regulations. As such, we support Recommendation 4.

We note GPA's census work on data privacy arrangement in different jurisdictions. We support the general aim of Recommendation 7 wherein concepts such as mutual recognition or adequacy arrangements can be established. Whilst such an approach may not immediately drive consistency, it may well help promote interoperability as a first step.

We note that there may well be sound reasons for data localisation. Nonetheless, national authorities should create legal pathways and other alternatives for the transfer and storage of payments-related data without compromising data storage security. This could help mitigate friction related to data localisation in cross-border payments. In the first instance, however, avoiding these types of restrictions should be the principle applied where there is equivalence in data protection and privacy. Therefore, we broadly support Recommendation 9 as well as the supporting Recommendations 10 and 11.

AusPayNet also encourages the continued evolution in technology offering solutions to data friction and improving both efficiency and enduser experience. The use of regulatory sandboxes is a pro-active example that should be harnessed further to encourage collaborative progress between the public and private sector.

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?**

Whilst fraud is noted, perhaps it is timely to change the terminology to economic crime. Mitigating economic crime should focus on areas beyond fraud, such as scams. Scams are fleecing people of billions of dollars which in turn undermines the confidence that citizens have in the digital economy.

An opportunity to improve payment outcomes should include the greater uptake of Confirmation of Payee (CoP) in cross-border payments. CoP requires data exchange, and this exchange has inevitable privacy, security and technical control implications that need to be addressed. We have seen CoP rolled out in domestic payment systems, where it has demonstrated its utility in reducing misdirected payments, fraud and scams. Its expanded uptake within cross-border payments would be a welcome tool in reducing misdirected payments, payment fraud and scams.

To lock in the benefits of the global digital economy we must address the harms of economic crime; this requires a global response. An appropriate cross-border data framework that not only enables CoP, but innovates around risk scoring, is essential in tacking fraud and scams and would strengthen the confidence that citizens have in the digital economy.

We encourage the FSB to ensure that there are tangible outcomes being developed in assembling any fora.

Whilst countries have various collaborative structures in place to attempt to address economic crime, it is likely that frictions in cross-border data frameworks impede progress in money recovery. We suggest that this could also be a part of the analysis. The deliverable should result in clarity in data being shared amongst national anti-scam centres that increases the likelihood of money recovery.

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 that the proposed Forum would be a welcome addition in attempting to resolve data framework frictions and facilitating exchange of ideas and analysis on cross-border payments and related data issues.

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.**

An example of uncertainty in an Australian context is Australian Privacy Principle (APP) 8: cross-border disclosure of personal information. As a result of this APP, a Privacy (International Money Transfers) Generalising Determination 2020 was sought and granted by the Office of the Australian Information Commissioner (OAIC) under the provision of the Privacy Act, so that data, such as personally identifiable information, can be exchanged between an Authorised Deposit-taking Institution on Australian Territory with a Financial Institution that is not on Australian Territory is in relation to an international money transfer (IMT). This is a cumbersome process, with a time limitation.

It is also of some note that most data that is sent across jurisdictions in a payment is unverified. This can lead to misdirected or, at its most malign, becoming an enabler of fraudulent and scam payments. An aspect that would reduce this friction would be the introduction of innovations such as pre-validation and Confirmation of Payee. These all involve some aspects of transnational exchange of privacy related information. To the extent that is possible, the ability to remove friction before a cross-border payment is initiated would be a 'golden path'. The removal of barriers that enable this golden path would generate a significant benefit to citizens and participants in the cross-border payments ecosystem. We would endorse it being a feature of any discussions within the Forum that attempt to resolve conflict between balancing AML/CTF data requirements with that of data privacy and protection.

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

The forum should establish a framework, perhaps through the lead of GPA, that either removes privacy-related frictions or establishes equivalency between jurisdictional privacy frameworks and thereby reduces friction. In our answer to question 4, we provided a uniquely Australian example, a Privacy Generalising Determination, to demonstrate that the space is complex. Each jurisdiction has its own set of data privacy laws and therefore a mapping exercise across jurisdictions may well be the first critical step required to establish a benchmark for jurisdictions that balances the objectives of AML/CTF, fraud prevention, economic crime and detection as well as data privacy.

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

We recognise CPMI's efforts in establishing harmonised ISO 20022 data requirements for cross-border payments as a good initial step in mitigating the risk of fracturing. We would suggest that the effort should be focused on marshalling the efforts of standard setting bodies such as CBPR+, as well as market infrastructure groups such as HVPS+ and IP+. Moreover, the effort should be extended to align not just the data requirements but the implementation of and usage guidance of the ISO 20022 standard. We note that collaboration in aligning the usage of ISO 20022 by CBPR+ and HVPS+ has commenced and we would suggest that CPMI has an interest in fostering this type of activity more formally.

Harmonising the efforts under the umbrella of CPMI should lead to consistent outcomes that will support smoother implementation of FATF Recommendation 16 and assist all participants in the payments ecosystem achieve the G20's ambition of faster, cheaper, and more transparent and accessible cross-border payments irrespective of the messaging infrastructure being used.

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?**

Legal Entity Identifiers tend to be voluntary in nature outside their original genesis for OTC reporting. As such they are not ubiquitous in many markets.

LEIs also come at a cost. If the intention is to widen their use, then perhaps the first goal is to make them more ubiquitous. An option for consideration may be that regulators enforce LEI creation at the point that a legal entity is itself created. Once ubiquity in LEI issuance is achieved, in combination with the self-evident utility of LEIs, greater uptake in other domains, such as payments, can be envisaged and harnessed.

With rapid developments in tokenisation and digitisation of identity, consideration should also be made to integrate these innovations should the business case warrant.

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.**

We support the objective of reducing fragmentation in data requirements for AML/CTF compliance in payments through the implementation of a global standard set out in FATF R16 and its upcoming revision. Application of additional data requirements should have appropriate levels of clarity and consistency and articulate the specific risk that is being addressed. Moreover, each additional data requirement increases the level of compliance

resources which in turn increases cost and potentially adds friction that reduces the speed of payments.

The use of National Risk Assessments should be encouraged when public policy dictates bespoke requirements are required, and they should align with existing global data formats.

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?**

   There is a significant amount of evidence that uneven expectations for sanctions compliance creates significant friction in cross-border payments. It would be worth examining the issue in more detail for additional insight.

   There are other contributing factors, such as an excessively low institutional risk appetite. This will likely be driven by the fines associated with breaches.

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?**

    AusPayNet agrees that the recommendations are calibrated appropriately and balance policy objectives with data privacy and efficiency.

    Recommendation 5 should be implemented by Sanctions authorities as a priority. It is a small step that could yield significant benefits for the least amount of effort yet potentially yield outsize results in terms of improvement in screening outcomes.

    It is in the best interest of sanctions authorities to standardise the way sanctions lists are formatted, shared and updated. The risk associated with modifying sanctions lists so that they can be ingested into sanctions screening tools has been noted on numerous occasions. Not only is it costly, but it also adds unnecessary time from receipt of the sanctions list to when it can be ingested into sanction screening tools, as well as the risk of error.

    The use of standardised identifiers should be encouraged where they exist. However, the principle should be that for each additional data point added, it must demonstrably reduce friction.

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?**

    In our response to Question 2 we indicated that fraud should be expanded to economic crime, including scams. Scams today move funds at a significant pace and are impacting citizens' trust in the digital economy. With cross-border payments rapidly increasing in speed, it suggests a more concerted effort is required that supports current national and

transnational efforts to address scams. It will not bode well for the G20 to see the improvement of cross-border payments in terms of speed, cost, access and transparency being harnessed by scammers that then further undermines trust in the digital economy. As such, our members agree that Recommendation 10 will be of assistance.

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?**

    No Comment

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?**

    AusPayNet encourages the continued evolution in technology offering solutions to data friction and improving both efficiency and end-user experience. The use of regulatory sandboxes or their equivalent is a pro-active tool that should be harnessed further to encourage collaborative progress between the public and private sector.

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

    There is a suggestion from our members that there may need to be a move away from focusing on payment schemes to applying relevant data frameworks. If the payment scheme permits a specific activity then the data framework for that specific activity should apply.

    By way of example, the historical purpose of card schemes was purchases. Many card schemes now permit, and even encourage, remittance activity. The data framework should apply to those remittance/payment activities, but not to those activities which are out of scope. This is analogous to the concept of ‘same activity, same risk, same rules’.