FSB FINANCIAL STABILITY BOARD

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

Response to Consultation

The Future of Financial Intelligence Sharing (FFIS) research initiative

General

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

In general, the FFIS research programme supports the proposed FSB recommendations and approach set out in the FSB proposals, particularly with regard to Recommendation 9.

However, it is worth noting that - at a more conceptual level - the FFIS research programme suggests the G20 Payments Reform Roadmap policy officials reconsider referring to fraud and financial crime measures as ‘frictions’. Much of the G20 Roadmap documentation emphasises the need to reduce or remove identified ‘frictions’ and, so, placing fraud and financial crime controls under this heading inevitably frames them as potential problems which in some way inhibit a higher priority goal.

The implication is that ‘addressing’ these frictions means to remove or reduce them.

We suggest, as the FSB consultation document does, that effective fraud and financial crime detection and preventative systems are central to the integrity of a safe, secure and well-functioning payment system. As such, the broader G20 Roadmap terminology (in further policy and strategy documents) should avoid referring to such safety mechanisms as ‘frictions’.

We recommend that effective controls to mitigate against fraud and financial crime risk should be referred to as ‘design features’ of cross-border payments, not a ‘frictions’. We make this case because:

1) The framing of these issues as ‘frictions’ assumes that such measures will always negatively impact on efficiency. However, examples of innovation (see below) in terms of integrating payment processes with fraud and financial crime checks show that such detection and preventative systems need not come at the expense of efficiency. There are win-win scenarios for speed and safety (with regard to fraud and financial crime risks) and,

therefore, the terminology used by policy-makers should account for the need to support such scenarios.

2) It would be odd to refer physical security infrastructure as a 'friction' to enter a building. Instead, appropriate security features (relevant to the risks) are understood to be essential to keep users safe and secure. Effective fraud and financial crime frameworks should, likewise, be a design priority for safe and secure payment systems and referred to as such.

However, we believe the FSB proposals do indeed take this conceptual approach and the use of the word 'friction' for fraud and financial crime risk mitigation may be a legacy effect arising from the original framing of the G20 objectives.

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?**

A) Understanding the threats and impact of the policy push towards faster payments cross border

Good policy-making is informed by robust assessments of the cost and potential negative impacts arising from any policy decision. We recommend that the FSB should also consider asking relevant competent authorities (including key national law enforcement authorities) to produce a collaborative evaluation of the potential harm caused by faster and instant payment systems cross-border initiatives to existing key sanctions evasion, fraud and financial crime prevention capabilities.

B) Develop the mitigation framework for the threats.

After understanding and evaluating the threat potential of faster or instant cross-border payments, G20 policy makers should adequately mitigate the risks.

G20 Cross Border Roadmap 'Data Frameworks' proposals engage with international standards - such as they exist - for data protection laws and AML/CFT requirements set by the Financial Action Taskforce, and then sets out an intent harmonise or minimise issues which may disrupt efficient payments. However, there is no international standards setting body for fraud prevention. As such, there is no 'data framework' to accommodate, align to or - even - to minimise or harmonise with respect of fraud prevention.

As such, we recommend that the FSB Forum should take a leadership role in encouraging the establishment of such international standards for fraud prevention – in the interests of a safe and secure cross-border payments framework that deliver on faster, cheaper, more accessible and more transparent cross-border payments. The framework for mitigating faster payments must be built alongside the framework for safer cross-border payments.

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 FFIS research programme supports the creation of the Forum as a much-needed coordination mechanism, across payments, data protection and fraud, financial crime and sanctions issues.

In reference to the point made in the previous question, however, we urge that the Forum develop a particular expertise in fraud detection and prevention – given the absence of another international standard setter active in understanding what effective fraud controls look like for faster cross-border payment systems.

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.**

   N/A

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

   We support the role of the Forum to document and leverage existing national innovation, private sector innovation and BIS Innovation Hub projects to explore how technology and, potentially, policy change can resolve coordination issues between different regulatory and supervisory obligations.

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

   The FFIS research programme supports the flexibility of the recommendations, but the Forum will need to support and encourage further practical work to interpret the recommendations in practice.

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?**

   From the perspective of the fraud and financial crime integrity benefits of ISO 20022, our research indicates that the implementation of ISO 20022 can support a range of fraud and financial crime detection capabilities to function cross-border (and across payment system boundaries), including tracing of funds and the development of models for detection of economic crime risk trained on federated data from across and between payment systems.

However, while the ISO 20022 standard presents a technical opportunity to tackle fraud and financial crime through more effective communication and analytical pathways, currently there is no internationally coordinated effort with public and private sector involvement to develop the shared definitions, standards and agreed use-cases to fully exploit the economic crime-risk management opportunities presented by ISO 20022 in a consistent manner across borders.

Despite ISO 20022 implementation data harmonisation being a priority action of the G20 Roadmap, this priority action does not - as yet – fully engage with fraud and financial crime use-cases.

The FATF Payments Transparency Consultations and broader ISO 20022 data standardisation work by the Bank for International Settlements are not, as yet, defining what data fields are required for different economic crime threat analysis (across fraud and AML specific threats); nor standardise how those fields are populated; nor take an interest in enabling risk model analytics over payments data, federated or privacy-preserving analysis across multiple payment systems, or cross-border tracing of money laundering dispersals, for example.

Despite some promising national-level initiatives in fraud prevention and detection capabilities within payments infrastructure, currently, there is no support at the international standard setting level for fraud detection and prevention use-cases as part of the ISO 20022 implementation process or through Payments Transparency Review at FATF.

Without greater international coordination there is a risk that the use of ISO 20022 for economic crime risk management purposes develops in a sporadic manner, presenting inconsistencies and undermining interoperability across borders.

This is a potential issue for the Forum to explore or for the Forum to secure appropriate technical support from BIS Innovation Hubs.

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.**

N/A

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?**

In some elements of the consultation document and the broader G20 Roadmap, there is an emphasis on the benefit from harmonised data standards in terms of enabling sanctions compliance checks. While this ‘data quality’ argument is important and can provide benefits, it is important for G20 policy makers to appreciate the limits of those benefits against the sanctions evasion risks of straight through processing.

From a sanctions use-case perspective, the gap between instruction and ultimate settlement is used to investigate cases where insufficient information is available to make an instantaneous decision on a sanction screening obligation.

As part of the FFIS study into payments systems in detecting economic crime, regulated entities reported concern that it will not be realistic to rely on the sender financial institution's screening for sanctions (and permit straight-through processing to their financial institution) without increasing the risk of sanctions breach.

Sanctions requirements, particularly related to U.S. imposed financial sanctions, are often more complex than screening for simple named legal entities and can relate to associated entities, business sectors and potential use of underlying products – all of which require investigation by inbound receiving financial institutions.

Without the time to screen and investigate inbound payments, financial institutions' ability to screen for sanctions in a comprehensive way will be severely degraded. As such, national security objectives associated to financial sanctions will be compromised.

There are projects in addition to list standardisation which could support a more effective role for payments infrastructure to contribute to sanctions detection that could be explored by the Forum.

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?**

Collectively, the FFIS research programme supports the recommendations a framework that can sufficiently balance policy objectives related to the protection of individuals' data privacy and the safety and efficiency of 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?**

Recommendation 9 proposed by the FSB seeks to address directly the challenges of fraud risk within cross-border payments. This recommendation is essential to achieve the vision of safe and secure, as well as efficient payment system design.

The link between faster payments and faster fraud is well established.

At the domestic level, fraudsters and money launderers are known to make use of faster payments to transfer the relevant funds on to other accounts quickly, reducing the opportunity for an intervention to restrain and recover the funds.

A survey conducted by Aite-Novarica Group, on behalf of Outseer, identified the link between faster payments systems and faster fraud across India, the UK, Malaysia, and Australia. According to the report, "57% of surveyed financial institutions noted an increase in mule activity over real-time payment rails in 2022 compared to 2021. Furthermore, 71% reported an increase in consumer Account Takeover (ATO) using real-time payment rails, while 62% observed a rise in consumer authorised push payment (APP) fraud via real-time payment rails." The authors conclude "These alarming statistics highlight the urgent need for robust measures to mitigate fraud risks within the context of faster payment systems."

The European Payments Council (EPC) '2023 Payment Threats and Fraud Trends Report' highlighted that the SEPA Instant Credit Transfer (SCT Inst) feature of "immediate execution followed by immediate clearing and settlement with funds instantly made available to the beneficiary, and continuous processing on a 24/7 basis" was being targeted to support economic crime.

The UK Payment Systems Regulator published in October 2023 its Authorised Push Payment (APP) scams performance report and identified that the UK Faster Payments System was used for 98% of APP fraud payments in the previous year.

The US Faster Payments Council explained "the speed of which the fraud has been carried out is a primary reason why fraudsters are attacking clients on Faster Payments rails."

The push towards faster payments cross-border, absent recommendation 9, would introduce substantial vulnerabilities to countries in terms of fraud as well as sanctions evasion and financial crime.

However, as described in this submission in the answer to question 2, there is no pre-existing international standard for fraud prevention and detection systems for cross-border payments.

We therefore recommend that the FSB survey national experiences to understand exactly how national domestic payment system operators are analysing and mitigating fraud and financial crime risks in their domestic payment market infrastructure. These learnings and use of innovation can then be applied at the cross-border payments level.

The FSB may draw also from the BIS Innovation Hub projects Hertha and Aurora which are examining relevant data attributes and use of technology for fraud and financial crime use-cases.

The Bank for International Settlements 'Project Aurora' in 2023, which established quantitative measures for the value of economic crime analysis taking place at the level of national and cross-border payments infrastructure and the utility/privacy trade-off considerations of use of privacy enhancing technology.

In 2022, the UK payment market infrastructure entity Pay.UK developed a pilot with Synectics, Featurespace and VISA to assess the viability and value of introducing a new fraud overlay service that could analyse money flows and use predictive intelligence to proactively detect APP fraud and prevent financial crime. The pilot found that relevant enhanced access to data and federated model development could improve detection rates by 13% with efficiency gains of 68%. Based on extrapolating results for 2023's APP fraud levels, the Pay.UK PoC as a whole showed that predictive analytics trained on shared payments data could see £273m more fraud detected each year. The annualised results using Approach 3 showed that for every 1,441 transactions fast tracked, only 1 scam was missed, meaning that 98.8% of customer transactions could be safety fast tracked. A related UK 'Enhanced Fraud Data' proof-of-concept on 6-months of historic transaction data, utilising enhanced data sharing through the payment system, identified that UK banks could have prevented, on average, 20% more fraud compared to what was identified without the additional data.

In 2023, though with a more limited capability focused on anomaly detection, EBA CLEARING have developed a pan-European Fraud Pattern and Anomaly Detection (FPAD) functionality and established a developer portal, including a sandbox, to support users in the development and testing of FPAD's application programming interfaces (APIs). In addition to an IBAN/name check, FPAD is intended to provide participants in the network with insights on patterns and anomalies from a central infrastructure level perspective, with anomalies qualified by feedback from participants.

In July 2023, the U.S. Federal Reserve announced that the FedNow Instant Payment Service will include analytical tools to assist participating financial institutions in detecting fraud risk, including :

- The ability for a financial institution to establish risk-based transaction value limits.

- The ability to specify certain conditions under which transactions would be rejected, such as by account number (a "negative list").

- Message signing, which will validate that the message contents have not been altered or modified.

- Reporting features and functionality, including reports on the number of payment messages that were rejected based on a participating financial institution's settings.

The Federal Reserve is reportedly exploring "other features that could be made available as part of future releases to aid participants in managing fraud risk, including, for example, value limits that could be tailored to certain uses, aggregate value or volume limits for specific periods (for example, per business day), and/or centralized monitoring performed by the FedNow Service such as functionality that leverages advanced statistical methods and historical patterns to identify potentially fraudulent payments."

This short synopsis of national examples can provide an indication of the depth of expertise available to the Forum and the FSB from national Payment Market Infrastructure attempts to develop appropriate fraud and financial crime risk information sharing.

Other national examples of fraud capabilities embedded in PMI include :

- Nigeria: Nigeria Inter-Bank Settlement System Plc (NIBSS) was incorporated in 1993 and is owned by all licensed banks including the Central Bank of Nigeria (CBN). NIBSS has specific responsibility delegated from the CBN for the provision of anti-fraud solutions and related services.

- South Africa: BankservAfrica is the official clearing house for electronic payments, appointed by the Payments Association of South Africa (PASA). BankservAfrica has reported aspirations to develop a transactional fraud mitigation system as well as an account verification service.

- India: The Reserve Bank of India (RBI) has encouraged payment system operators in India to put in place robust fraud and risk monitoring systems. In response the national clearing house, the National Payments Corporation of India, has designed and implemented a real-time transaction monitoring tool for fraud detection and prevention and offers this free of charge to its participants.

- South Korea: South Korea encourages a holistic approach to payments fraud prevention and resolution, where the South Korea regulator, the Financial Supervisory Service (FSS), plays a large role in payments fraud prevention and resolution.

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?**

-

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?**

We recommend that the Forum leverage the work of the BIS Innovation Hubs for this purpose.

The Bank for International Settlements major technical exercise 'Project Aurora' identified that:

"A holistic view of payments data is essential to effectively identify and combat suspicious activities that take place beyond the bounds of single financial institutions and national borders. Leveraging these data could lead to improvements in monitoring by opening up a holistic view on transaction networks that unveil money laundering networks… these approaches could be used by operators (eg central banks or private sector entities) of instant payment systems or potential CBDC systems that include AML monitoring and analysis capabilities. Operators of these systems could provide participants with additional tools and support to enhance their monitoring efficiency."

As Project Aurora set out, many elements of analytics and the capabilities described can be achieved without the underlying data travelling. Privacy enhancing technologies can allow for insights to travel and learning to be shared without having to share raw data.

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

This is a submission by the FFIS research programme to the Financial Stability Board consultation for 'Data Frameworks in the G20 Cross-Border Payments Plan' (July 2024).

The FFIS research programme is an independent research initiative, delivered within the Royal United Services Institute (RUSI) Centre for Finance and Security, focused on exploring innovation in public-private and private-to-private economic crime-related information sharing. FFIS delivers research projects, often in connection with research-based events, in the AML and fraud prevention policy-sphere.

Since its establishment in 2017, FFIS has published 7 major international comparative studies of financial information-sharing partnerships and platforms, produced several national-level papers and convened a large number of events with senior leaders in the AML/CTF and fraud prevention communities worldwide.

This submission is primarily based on the findings of an 18-month FFIS research project into ‘The role of payment infrastructure in the detection of economic crime’ and the FFIS policy paper: The case for the G20 cross-border payments reform ‘Roadmap’ to embed economic crime security by design (January 2024). References have not been saved in this submission form, but are available on request and many can be found in the papers in the project page here: https://www.future-fis.com/payments.html