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

Response to Consultation

London Stock Exchange

General

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

The proposed scope of the recommendations is well defined and will address a lot of the frictions that currently exist in data frameworks related to cross-border payments.

There is however one exception we would like to highlight and elaborate further under question 2: The scope of Recommendation 2 should include the creation of common data standards globally around beneficial ownership registers, a critical component of the Anti-Money Laundering and Know-Your-Customer (KYC) obligations.

Beyond the need to address beneficial ownership standards noted above, the scope of the recommendations rightly focuses on the following data framework inconsistencies:

1. Sanctions (Recommendation 5): Since January 2017 the number of sanctioned persons has increased by 320% (1) and highlighted the inconsistencies of naming conventions and lack of identifiers and its impact on false positives and effectiveness. Given that there are 65 different sanction authorities globally, each having their own data formats, standardising these and making the sanction lists machine-readable is much needed to ensure the effectiveness of sanctions.

2. Data privacy (Recommendations 7, 8, 9): As stated by the World Economic Forum (2) , consistent minimum standards are essential in data protection regimes to ensure an effective payment processing, risk management, fraud and financial crime prevention. The report highlighted that, ‘Challenges identified during this multi-stakeholder collaboration include disparities in regulatory frameworks across jurisdictions, complexities in anti-money laundering/combatting the financing of terrorism (AML/CFT) compliance, stringent data privacy and security regulations, and regulatory barriers to accessing payment systems and infrastructure. Such challenges contribute to cost increases and impede transactions.’ (3)

Currently data protection laws are implemented at a national level and as a result there are several inconsistencies and fragmentation. While the OECD Privacy Principles and Convention 108+ provide a good basis for internationally agreed principles, an initiative by the Financial Stability Board to promote more consistency is welcomed.

Uncertainties about regulatory requirements and the challenges of non-interoperable payment systems pose challenges to data sharing even on an intra-group basis. Intra-group sharing must consider data localisation and data privacy laws, and regulatory divergences across jurisdictions, these make it difficult to establish a common data and compliance framework. The secrecy problem can be illustrated by the US Bank Secrecy Act (BSA) restrictions of sharing underlying data across a group, or the presence of a Suspicious Activity Report filing in a foreign branch of a US financial institutions, as foreign branches are not subject to BSA requirements. Instead, foreign branches can only share with the parent company.

3. Public-private partnerships (Recommendation 12): Promoting public-private partnerships (PPPs) and the sharing of best practices is needed. This is particularly relevant in the AML/CFT regimes as PPPs have demonstrated that they can provide dynamic information sharing on financial crime risks. It is estimated that money laundering, tax evasion and corruption combined to be around 7.2% of global GDP. (4)

FATF considers information sharing 'crucial' to fight money laundering and terrorist financing noting since financial crime networks operate across lines of business and are often transnational, data sharing has the potential to assist the private sector and authorities to reduce data collection and pinpoint suspicious payments activities with more accuracy. (5)

Benefits of public-private partnerships include:

- Less data collection by the industry and authorities.
- Enhancing data quality.
- Aiding in customer identification and verification.
- Verifying risk ratings.
- Augmenting dynamic risk management to reflect new information or changes in behaviours; and
- Sharing best practices and analytical techniques to optimise ways of working.

One example of a PPP is the Global Coalition to Fight Financial Crime (GCFFC), established in 2018 and composed of a network of senior experts across the law enforcement, banking, risk-intelligence, and Non-profit Organisations (NPOs) to advocate for the adoption of smarter international regulations, standards and measures to better fight financial crime. Through its engagement with FATF, the GCFFC has recommended for the Mutual Evaluation methodology to be revised and more explicitly embrace PPP in its assessment and increase its reliability of data by collaborating with academia and data providers. (6)

Another example of an innovative public-private information sharing partnership is the South African AML Integrated Taskforce (SAMLIT), established in 2019 and composed of regulatory authorities, represented by the Financial Intelligence Centre, the Prudential Authority of the South African Reserve Bank and international financial institutions and risk-intelligence providers to enhance understanding of financial crime risks. In 2021, SAMLIT established an expert working group on modern day slavery and human trafficking with three primary objectives: (7)

1. Understand payment flows relating to human trafficking including country of source, destination and the demographics of the various role players;

2. Develop a list of indicators to assist the financial sector to strengthen their ability to identify human trafficking; and

3. Build partnerships key stakeholders, including law enforcement to provide meaningful information on criminal networks.

(1) LSEG Risk Intelligence Global Sanctions Index – 3rd edition available at LRI3384941_3rd_edition_global_sanctions_index_1920x1080 (lseg.com)

(2) WEF, Overcoming Regulatory Friction in Cross-Border Payments (2023) https://www3.weforum.org/docs/WEF_Unlocking_Interoperability_2023.pdf

(3) WEF, Overcoming Regulatory Friction in Cross-Border Payments (2023) https://www3.weforum.org/docs/WEF_Unlocking_Interoperability_2023.pdf

(4) GCFFC, Fighting Financial Crime - Information Wall, 2021 available at https://www.gcffc.org/wp-content/uploads/2023/11/GCFFC-Financial-Crime-Information-Wall-2021.pdf

(5) Consolidated FATF Standards on Information Sharing available at https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Consolidated-fatf-standard-information-sharing.html

(6) Effectiveness Expert Working Group | FATF Subgroup Working Paper - Questions and Recommendations on Improving the Effectiveness of the FATF Mutual Evaluation Process available at https://www.gcffc.org/wp-content/uploads/2023/10/GCFFC-Effectiveness-Expert-Working-Group-_-FATF-Subgroup-Working-Paper-1.pdf

(7) LSEG RI, SAMLIT 2023 - FOLLOW THE MONEY How understanding financial flows and key indicators can help to fight modern slavery and human trafficking in South Africa available at https://www.lseg.com/content/dam/risk-intelligence/en_us/documents/reports/fighting-modern-slavery-south-africa.pdf

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?**

Reforming the data frameworks for beneficial ownership (BO) registers should be addressed as part of the broader efforts to create global interoperability and consistency. As part of the AML/CFT regimes to facilitate payments, knowing-your-customer is a vital part of that framework and regulatory harmonisation is needed to ensure interoperability, including access, minimum formatting and common data structures.

The value of BO information for fighting financial crime has been widely recognised by international standard-setting bodies, including the FATF, OECD, IMF, the World Bank, and the United Nations. Its flow across borders should now be promoted and enhanced through the effective recognition of all actors needing to access it and via standardised but innovative ways to access and process this data. In this sense, BO data users are currently facing a range of challenges in effectively using data to fulfil their anti-financial crime goals.

There are several other principles that should be considered to make beneficial ownership data more relevant and useful:

(a) Data should be accessible to all relevant parties and beneficial ownership should be defined consistently in regulations in terms of thresholds and scope;

(b) Disclosure should comprehensively cover all types of legal entities and natural persons;

(c) Information should be submitted in a timely manner and kept up-to-date;

(d) Historic records should be kept according to minimum data retention standards.

The G20 Roadmap for Enhancing Cross-border Payments is a welcome initiative to address harmonisation of cross border data exchange and payment message standards. An underexplored topic, from an AML/CTF perspective, is the sanctions data provided by regulatory bodies and its significant variation in format from one jurisdiction to another. Trying to achieve a higher degree of harmonisation in this respect would help to increase the speed of that part of the process and clear guidelines on how that data is used will provide for a more transparent cross-border payment environment.

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 Forum, as an international body, would ensure a more globally consistent approach to issues that cannot be resolved through national and/or regional forums. It is important that the Forum's output builds a solid foundation of recommendations that can be propagated globally. It is key to have strong representation in the forum from policy decision makers so we can bridge the gap between implementation challenges and the intent behind the laws.

We support the creation and work of formal forums in international and regional organisations, as well as industry groups containing key anti-money laundering/combatting the financing of terrorism (AML/CFT) and data protection and privacy organisations to streamline both current and evolving laws and regulations. We also support the development of best practices and consistent standards (including regulator-approved codes of conduct and certification schemes) across the cross-border payments ecosystem.

Specifically, the topics which should be considered by the Forum working group include:

1. Achieving greater legal and regulatory alignment, through:

a. Creating a public and private sector forum containing key ecosystem stakeholders;

b. Inclusion of language in regional and national legislation to embed and recognise the compliance systems identified by these forums/groups;

c. Development of best practices and consistent standards (including regulator-approved codes of conduct and certification schemes) for data and technology services providers (i.e. 3rd parties) covering AML/CFT and data privacy workflows.

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.

Information sharing is a critical and necessary part of good AML/CFT compliance. Without timely checks, businesses and individuals who are the subject of those checks, would not be able to access critical banking and payment systems in the largely frictionless manner that they do today. Where data sharing within the AML/CFT workflow is appropriately designed for compliance with both financial crime regulations and data privacy ones, the benefits can be significant. However, navigating the obligations for both is complex.

One recommendation would be to promote consistent standards for the storing, retention and processing of data across jurisdictions as these are key to encourage interoperability by making the technical process of sharing data across systems, corporate groups, private and public entities simpler.

Access to BO registers is an example of how the interplay between data privacy requirements and court decisions can lead to additional uncertainty for financial institutions (FIs) and service providers. For example, the EU's 6th Anti Money Laundering Directive (AMLD6) provides that (despite the clear cross-border aspects of good AML/CFT compliance) service providers hold a legitimate interest in accessing UBO information, provided that the data obtained from the EU register is offered to Obliged Entities and public authorities only in the European Union. To best support effective and accurate collection and sharing of data, in a manner compliant with data privacy regulations, there should be a consistent right for data access by service providers on the basis of controls which enshrine privacy protections. This problem is amplified when considered on a global level. Many Obliged Entities are global in reach, but AML/CFT and data privacy compliance regimes are localised on a per-region, per-country and sometimes even per-state basis, making reconciling all of the competing requirements an impossible task.

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 include both AML prudential supervisors, international standard-setting bodies (e.g. FATF), financial intelligence units (e.g. the Egmont Group), law enforcement (e.g. Interpol), data protection authorities and relevant industry stakeholders (e.g. banks, non-banks, including risk-intelligence data providers).

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

   Yes.

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?**

   We support the adoption of standardised legal identity identifiers and use of ISO standards. Developing consistent standards (including regulator-approved codes of conduct and certification schemes) for data and technology service providers across the financial crime ecosystem, brings together AML/CFT and data privacy experts and regulators for alignment in developing those standards and is an important step towards interoperability.

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.**

   See response to question 1

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?**

   Regulators often operate differently and there is no joint baseline for sanctions compliance, which forces financial institutions to navigate a complex regulatory environment in order to align with all expectations. Introducing a minimum set of standards and best practices would help to align:

   - Which data is screenable or not?

   - What are the standards expected during a regulatory review / audit?

   - What is considered ‘up to date'?

On the data front, the implementation of standards is key. Clear minimum data standards and processes for the source sanction data publication would be beneficial. Some examples include:

- Clear name categorisation (e.g., good quality vs low quality aliases)

o Categorisation can differ between regulators resulting in different expectations for the same name

- Notifications of sanctions updates with time stamps

o No push notifications for some regulators that source data changed, which impacts screening timelines.

- Provide data in machine readable formats

o Not all regulators provide data in a way that can be easily ingested.

- Provide guidance on what data is to be used for automated screening and what is supporting information for adjudication.

- Provide mapping from data in source lists and payment message placeholders for simpler integrations.

To exemplify some of the existing issues, in the context of new instant payments regulations such as those in the EU, the need for sanctions screenings is significantly increased. In general, financial institutions will likely struggle to be fully compliant with this legislation, as some of the requirements are quite challenging, in particular the concept of "immediate" screening. Some payment service providers (PSPs) will have very large customer bases, and the overall process will always take significant time. There are different readiness levels for this change, with smaller PSPs struggling to ramp up teams to perform 24/7 screening, particularly over the weekends. Larger institutions might have resources already prepared. Moreover, these screening changes only apply to SEPA instant payments. So, PSPs will need to keep existing screening processes, even for transactions that are not SEPA instant payments.

See also question 1 response for further details.

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?**

    See question 1 response

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?**

Fraud and cybercrime have been reported to be the most prevalent financial crimes, with online scams taking top spot according to our LSEG global fraud league table. (1) Reports of invoice and tax frauds take second and third spots respectively. Further studies by Interpol highlights that increased use of technology is 'enabling organised crime groups to better target victims around the world'. (2) Similarly, a report from the Global Coalition to Fight Financial Crime reports that scams generate estimates up to $177 billion. (3)

Despite these assessments of the well-recognized financial crime threat, there is no existing mechanism that enables both the public and private sectors to methodically assess this emerging threat cross-border through existing data transfer tools, beyond capabilities introduced by risk-intelligence providers. This information flow is only one-way as data providers provide the data to relevant public (e.g. Financial Intelligence Units) and financial services firms. But there is no mechanism for this information to be two-way, e.g. a data sharing mechanism between all parties.

(1) LSEG, Digital deception: how technology is changing fraud available at https://www.lseg.com/content/dam/risk-intelligence/en_us/documents/gated/white-papers/digital-deception-white-paper.pdf

(2) Interpol Financial Fraud Assessment 2024 available at https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-Financial-Fraud-assessment-A-global-threat-boosted-by-technology

(3) GCFFC Scams Report 2024 available at https://www.gcffc.org/wp-content/uploads/2024/06/GCFFC-Scams-Report-6June2024Pbd_V2.pdf

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?

The FSB should consider Interpol's Global Rapid Intervention of Payments (I-GRIP) stop-payment mechanism which was launched in 2022 and have already intercepted more than $200 million, stemming largely from cyber-enabled fraud. (1) This is the first initiative that FATF and the Egmont Group have joined forces to help identify and track criminal asset globally. Ensuring that initiatives like these should be supported by regulatory clarity on enabling cross-border data flows.

(1) https://www.interpol.int/en/News-and-Events/News/2023/FATF-INTERPOL-partnership-putting-trillions-in-illicit-profits-back-into-legitimate-economies

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 a measurable objective to be formed by the Forum working group that specifically promotes public & private sector innovation aligned to areas of reduction in payment fraud and making cross border payments significantly safer. Potential objective themes would be:

- Promoting innovation guiding principles

- Annual / semi organised events for public sector to showcase R&D efforts for the purposes of consultations and feedback

- Market research and market insights for the purposes of innovation ideation.

See also response to Question 2.

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

LSEG welcomes the Financial Stability Board Recommendations to promote alignment and interoperability across data frameworks related to cross-border payments. LSEG is committed to supporting a reliable framework which facilitates public interest activities such as the identification and prevention of financial crime, or other criminal or unlawful activity (for example, modern slavery, illegal trafficking, environmental crime) which can often be enabled through cross-border payments.

As a globally recognised provider of risk and compliance data, LSEG's World-Check services are used by our clients globally in the fight against money laundering to help them meet their legal and regulatory obligations and risk management procedures carried out in the public interest. Notably, LSEG is a founding member of the Global Coalition to Fight Financial Crime , together with public institutions such as Interpol.

About LSEG

With World-Check, LSEG has been at the forefront of supporting financial services firms, corporates, financial intelligence units and law enforcement organisations in the fight against financial crime in Europe and globally. Our data is used by more than 11,000 customers in more than 180 countries. Our risk intelligence database provides organisations with data from reliable public domain sources that helps entities carry out their due diligence and sanctions compliance obligations much more effectively.

We look at financial crime in the broad sense – not just money laundering, but also human trafficking, environmental crime, wildlife crime and other criminal activities such as terrorist financing taking place across the world. We promote proportionate information sharing and collaboration and support a number of partnerships that span public sector, civil society and private sectors and help organisations uncover hidden risk and fight financial and green crime efficiently and effectively to not only help organisations to detect these crimes but to enhance their global prevention in the public interest.