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

Response to Consultation

DiArc

General

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

   The recommendations are to improve the current exchange model using identifiers (LEI) and common data sets. This does not solve the problems of data authenticity (Is the LEI really the Account Owner's LEI ?) and how the payer can get exact information about the Payee.

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?**

   1. Digitalise all endpoints in the financial ecosystem: Banks could provide digital "financial passports" to their account owners

   2. Support peer-to-peer protocols to enable the exchange of financial coordinates through the presentation of financial passports

   3. Add digital financial coordinates to payment messages

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?**

   There is a need for a trust architecture framework. The vLEI is the first "identity credential" available. It could be used to issue "eKYC" credentials, by which the issuer guarantees the verification of the local KYC rules.

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.**

   Data privacy can be supported by the selective disclosure features of KERI or W3C protocols. It means that a Financial Passport would give access to many information but a limited data set would be exposed depending on the role of the verifier. Typically, end users will see the information they need to make transactions (account number, official name, trade name), while Financial Institutions would access all information they need to verify compliance. This might go up to the Ultimate Beneficiaries.

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

   Standardisation (ISO20022) of the semantic / development of a financial identity Framework / selective disclosure

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

   We developed ISO20022 in 2000, and recommendations to use it twenty years later are a bit late, considering that technology and the environment have evolved. New opportunities are emerging from DID, Verifiable Credentials and secure peer-to-peer protocols. The current messaging model is based on the copy of the information (I am asked to copy the Payee's postal address in my payment initiation instruction). Better techniques are allowing to use digital certificates that are digitally signed and verifiable (I could reuse the financial passport received from the Payee and issued by the Payee's bank - all information required is then certified by the Payee's Bank)

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?**

   Using the LEI to verify, for example, the Payee's information imposes the Payer and the PSP to store the LEI in relation with an account number. This is complex while this information can be made available by the Payee in a digital, portable credential.

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.

ISO20022 Business Model can be used to specify the data requirements in business terms. Next, there is a need to standardise the verifiable credentials to be use in interoperability process.

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?**

   Sanctions list are also using names and AKA. Messages are screened to potentially detect a match. If all endpoints in the financial ecosystem had digital identities, the process would be much more efficient.

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?**

    No, there are still too much space for fraud or illicit data exposure. We should progressively apply the principle "Never Bank with an unknown" and always exchange digital identities before engaging in financial transactions. This goes back to the initial comment:

    1. Account Servicing Banks are issuing Financial Passports for their Account Servicers. The financial passport contains financial information and the identity of the owner.

    2. support P2P protocol to exchange financial coordinates

    3. use digital financial coordinates in payment instructions to allow any banks to verify the identity of the involved parties.

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?**

    No, we should adopt the "Zero-Trust" principle and focus on exchanging digitally signed and verifiable data.

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?**

    vLEI is the first example of Identity Credentials.

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?**

    Develop a framework based on decentralised technology, allowing the issuance of portable, verifiable credentials by trusted parties.

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

    -