EPIF response to the inception impact assessment on EU Scheme for online transactions

September 2020

ABOUT EPIF (EUROPEAN PAYMENT INSTITUTIONS FEDERATION)

EPIF, founded in 2011, represents the interests of the non-bank payment sector at the European level. We currently have over 190 authorised payment institutions and other non-bank payment providers as our members offering services in every part of Europe. **EPIF** thus represents roughly one third of all authorized Payment Institutions ("PI") in Europe. All of our members operate online. Our diverse membership includes a broad range of business models, including:

- Three-party Card Network Schemes
- E-Money Providers
- E-Payment Service Providers and Gateways
- Money Transfer Operators
- Acquirers
- Digital Wallets
- FX Payment Providers and Operators
- Payment Processing Services
- Card Issuers
- Independent Card Processors
- Third Party Providers
- Payment Collectors

EPIF seeks to represent the voice of the PI industry and the non-bank payment sector with EU institutions, policy-makers and stakeholders. We aim to play a constructive role in shaping and developing market conditions for payments in a modern and constantly evolving environment. It is our desire to promote a single EU payments market via the removal of excessive regulatory obstacles.

We wish to be seen as a provider for efficient payments in that single market and it is our aim to increase payment product diversification and innovation tailored to the needs of payment users (e.g. via mobile and internet).

Introduction

EPIF welcomes the opportunity to comment on the Commission's Inception Impact Assessment on the Revision of the eIDAS Regulation aimed at improving its effectiveness, extend its application to the private sector and promote trusted digital identities for all Europeans.

EPIF welcomes the Commission's position that universally accepted public electronic identity (eID) is necessary for consumers and businesses to have access to their data and securely use the products and services they want without having to use unrelated platforms to do so and unnecessarily sharing personal data with them and agrees that European digital identity that allows for a simple, trusted, secure and accessible to all public system for citizens and businesses to identify themselves and share identity related information in the digital space can be designed efficiently only at EU level.

Despite the eIDAS framework, the national rules on provision of digital identity services remain fragmented in or undeveloped across the EU. It is important that the EU sets the right regulatory framework to make sure that the Single Market is fit for the digital age and fosters the development of digital players.

EPIF is fully supportive of having Pan-European e-identification mechanisms that are secure, reliable, user-friendly and interoperable and welcome the work of the Commission on this area.

EPIF's preferred policy option would be to introduce a European Digital Identity scheme (EUid) complementary with eIDAS. We would also support option three, to extend the scope of eID regulation under eIDAS to the private sector.

We are moving into a digital world where digital identity is becoming an essential requirement. Digital identity (ID) technologies are evolving rapidly, giving rise to a variety of digital ID systems. It is key that these systems are interoperable across Members States to make sure that we allow innovation and digital payments to grow in a secure manner. A harmonised e-ID system would significantly reduce the cost of compliance for digital businesses and would offer new opportunities for companies to meet their compliance obligations.

EPIF does not see additional risks associated with the use of electronic identity. On the contrary, we believe this brings many opportunities. It will enable the raise of new services, improve security against fraud, help financial institutions better manage client risk through information sharing such as through the cross-border unique identifier noted below, allow connectivity among digital services and contribute to the economy as a whole.

A Digital ID and strong authentication can provide security of data and more explicitly assign ownership of the data to consumers. It would also promote the development of open finance and cut the costs of KYC by simplifying processes and reducing duplication.

The developments surrounding digital identity verification are one of the most promising uses of RegTech in recent years. Online verification procedures and KYC are far more convenient for users than traditional methods; without compromising security.

The lack of a harmonized, EU-wide, secure and reliable, digital identity framework also poses a significant barrier to the development of FinTech solutions, particularly those solutions which can be used across national borders.

A harmonised EU wide online (i.e. non-face-to -face) KYC framework would facilitate the introduction of a truly cross-border financial services market, and markedly reduce the cost of compliance for digital businesses.

This would significantly reduce the compliance costs for payment institutions involved in electronic payments, including one-off payments. It is crucial to ensure technological neutrality due to speed of technology progress and FinTech developments. It would reduce the inherent bias towards non-face-to-face payments. It would help reduce fraud and increase the commercial incentives for industry to develop and invest in more efficient technologies to deal with e-ID. All this would facilitate cross-border trade and the Single Market.

Regarding the list of attributes, we believe that technology should be able to be replicated from country to country and it should be scalable. We also support the idea of unique identifier that would be attached to the identified

persons across border. This would facilitate the KYC process. We are also in favour of replication of Nordics countries model where the Banks allow third party to access their data in order to simplify the KYC process. We would also like point out the fact that physical verification's option should be maintained to allow certain types of clients to access financial services, i.e. migrants, unbanked population. The framework should, however, incentivize and support the transfer to digital alternatives over the medium to long term.

With regard to the recognition of behavioural analysis as a (component of) Digital ID, we would like to point out that, to a large extent, most firms have already taken a multi-factored approach to identification, authentication and verification of customers in non face-to-face transactions within their own ecosystems. Companies are employing elements of behavioural analysis to assign customer risk ratings, augment their understanding of the customer's identity, such as expected log-in channels, geolocation, frequency of usage, type of usage, IP addresses and biometric markers. After all, Digital Identity, at its very core, is not about what the customer knows or is willing to share, but rather, what the customer "is" in the absence of physical evidence.

EPIF would like to point out to the efficiency of Digital ID across all AML/CFT measures. Reliance on Digital ID systems is in effect, reliance on a multi-factored approach to identification, authentication and verification of customers in non face-to-face transactions through independent and reliable sources. As such then, the records obtained for Digital ID verification may overlap with the types of records relied up for ongoing due diligence and transaction monitoring today. The data can be useful across a range of AML/CFT measures and not be considered in silos.

Finally, EPIF believes that a risk based approach is the most efficient method to manage AML/CFT. The level of CDD required should be linked to the risk rating assigned to the customer. Since these risk ratings consider the products used by the customer and are consistently assessed based on the customer's behavior, the information collected and verified as part of a customer's Digital ID should also be done using this risk-based approach. Under this approach, the quantity of customer information collected and verified would be aligned to the risk rating assigned to the customer and thus allow FIs to consistently and constantly assess the user and mitigate any risk.