Digital Identity – Call for Evidence

Consultation response by Efficient Frontiers International Ltd.

SEPTEMBER 13, 2019

EFFICIENT FRONTIERS INTERNATIONAL

We are grateful for the opportunity to contribute to this open call for evidence on enabling a digital identity system fit for the UK's growing digital economy.

We have organised our response by identifying the relevant questions identified in the call for evidence document dated July 2019, to which our comments relate.

Efficient Frontiers International ("EFI")

Efficient Frontiers International (EFI) is a client-focused services organisation, partnering with Financial Institutions to deliver Expertise and Capability and give clients confidence in a complex regulatory and business environment.

Our strategic capabilities cover three principle areas: consultancy and advisory; operations; and technology and data. This blend of abilities allows us to partner with clients through from insightful advice on emerging regulation, to detailed technical and operational implementation, either as a delivery partner or a managed service provider. Maintaining the regulatory traceability, rigour and client confidence throughout.

Section 4 – Needs and Problems

2. What are the economic or social benefits or costs from developing a digital identity system in the UK which meets these needs? Can you provide examples?

3. What are the costs and burdens of current identity verification processes?

6. Where do you see opportunities for a reusable digital identity to add value to services? Could you provide examples

We answer the above questions collectively below.

1.1 Re-Use of Digital Identification – Anti-Money Laundering Requirements

The ability to accurately identify and verify the identity of customers, their beneficial owners and controllers (**"ID&V"**) is at the heart of know your customer (**"KYC"**) activities that we undertake on behalf of our customers. It is the cornerstone of an effective financial crime prevention programme.

Previous papers have noted the challenges experienced by financial services customers during the KYC process.[1] For some customers, accessing financial services is made even more frustrating when they are asked to provide the same ID&V information again and again each time they try to access services from different financial institutions.

These duplicative efforts often occur because financial institutions must ensure they are able to demonstrate their compliance with KYC requirements under the Money Laundering Regulations 2017 (**"MERs"**).[2] For those organisations that operate in other European jurisdictions, this problem is compounded in needing to ensure that KYC requirements of each jurisdiction are complied with.[3]

[1]See: Thomson Reuters (now Refinitiv) (2017). "KYC compliance: the rising challenge for corporates". [online] Available at: https://www.refinitiv.com/content/dam/marketing/en_us/documents/reports/kyc-compliance- the-rising-challenge-for-corporates-special-report.pdf

[2] The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017. [online] Available at: http://www.legislation.gov.uk/uksi/2017/692/made#regulation-28

[3] Note 1.

Several organisations have attempted to quantify the cost undertaking KYC and CDD.[4] These costs are incurred not only by financial institutions. Costs in relation to the time, inconvenience and delays in accessing financial services can be otherwise restrict customer access to financial services, especially so for those who may otherwise be considered low risk, for financial crime purposes.[5]

One aspect of the ID&V process which illustrates this is where a customer is asked to provide a copy of their passport. Some organisations will ask a customer to provide a certified copy of their passport.[6] The copy must be certified by an approved person that the copy provided is a true likeness of the individual and that they have seen the original passport.[7] The requirement is intended to mitigate the fraud risks of impersonation or concealment of an individual's true identity.

This requirement may seem straightforward for customers who work with or personally know someone who is an "approved person" who will readily provide the necessary certification, for free. However, this process is not so easy for others. In some cases, customers must seek out a professional or organisation considered appropriate. They may need to travel to another location where the approved person is located. And some approved bodies, such as the Royal mail, charge a fee for each copy they are asked to certify.

Also, certified copies for ID&V purposes, do not remain "valid" forever. Some financial institutions will only accept a certified copy of a passport which is less than 3 to 6 months old from the date on which the certification takes place. This means that a customer who seeks services from a different financial institution must repeat the process and seek out, and again possibly pay, to obtain a fresh certified copy of their passport.

Certification of identification documentation is but one example of some of the ID&V challenges related to KYC, but it does help to illustrate the unintended impact upon both financial institutions and consumers.

The ability to re-use a digital identity may help to address these types of ID&V challenges, while still allowing financial institutions to comply with the MERs. It would

allow customers to produce a single source of information to the various institutions from whom it seeks services, including banking, insurance, investment, legal advice and real estate-related services. The consumer would not carry the burden of needing to obtain multiple certifications of their passport in order to access financial services. And organisations required to undertake ID&V under the MERs could have confidence in knowing that they are all relying on a single source of reliable identification common across them in relation to the same customer.

The possible re-use of digital identification as part of KYC requirements by financial institutions has previously been explored.[8] Several potential benefits were identified in relation to digital identities offered under the GOV.UK Verify ID programme. The value of digital identity to the financial sector was also reinforced in a joint report on the subject,

"Both the government and the private sector believe that the marketplace for identity should not be sector specific and that economies of scale could be reached through the reuse of a trusted citizen digital identity, driving down the cost of identity for the UK as a whole."[9]

This was also considered more broadly across European jurisdictions in terms of leveraging eIDAS programmes to allow for its usage by financial institutions as part of their KYC processes.[10]

---

[4] See, for example: LexisNexis Risk Solutions (2019). "On the Frontline: The UK's Fight Against Money Laundering". [online] Available at: https://risk.lexisnexis.co.uk/insights-resources/white-paper/on-the- frontline-the-uks-fight-against-money-laundering/ ; Consult Hyperion (2018) "White Paper: The cost of compliance and how to reduce it". [online] Available at: https://www.miteksystems.com/innovation- hub/white-papers/whitepaper-the-cost-of-compliance-and-how-to-reduce-it

[5] Note 1.

[6] See: Joint Money Laundering Steering Group (JMLSG). Guidelines, Section 5.3. Similar guidelines are now provided in relation to the electronic verification. [online] Available at: http://www.jmlsg.org.uk/.

[7] See, for example: https://www.gov.uk/certifying-a-document which reflects the standard also required of organisations required to comply with regulation 28 of the MERs.

[8] Open Identity Exchange (OIX) (January 2017) "How Digital Identities Which Meet Government Standards Could be Used as Part of UK Banks' Customer Onboarding and KYC Requirements". [online] Available at: https://oixuk.org/wp-content/uploads/2017/02/How-Digital-Identities-which-meet-Government-Standards- could-be-used-as-part-of-UK-Banks'-Customer-On-boarding-and-KYC-Requirements-FINAL.pdf

[9] Open Identity Exchange. (December 2016) "The value of digital identity to the financial services sector: Exploring the reuse of a GOV.UK Verify digital identity in a financial service application process". [online] Available at: http://www.innovateidentity.com/wp-content/uploads/2017/01/The-value-of-digital-identity-to- the-financial-service-sector-Full.pdf

[10] European Commission. (2018). "Study on eID and digital onboarding: mapping and analysis of existing onboarding practices across the EU". [online] Available at: https://ec.europa.eu/futurium/en/system/files/ged/study_on_eid_digital_onboarding_executive_summary.p df ; https://ec.europa.eu/futurium/en/system/files/ged/study_on_eid_digital_onboarding_final_report.pdf

The re-use of digital identification as part of the KYC process is therefore something that has been the subject of extensive discussion over the last few years. There is clearly an appetite to consider its possible usage. The European reach of business for many UK financial institutions would benefit from this proposal, which is also under consideration by other European jurisdictions.

1.2 Re-Use of Digital Identification – Companies House Registry

A second opportunity for the re-use of digital identification is beneficial owners and controller information on the Companies House Registry.

A consultation was undertaken earlier this summer, as part of the transposition of the amendments to the 4th Anti-Money Laundering Directive ("5AMLD"). The consultation considered the role of Companies House in maintaining an accurate register of information about individuals who are the beneficial owners of legal entities recorded on the register.[11]

Earlier this summer, EFI responded to the consultation undertaken by Companies House, as part of both its broader digital strategy and implementation of 5AMLD amendments requiring the recording of identification information about company beneficial owners on the Companies House registry ("Registry"). The consultation also considered whether Companies House should conduct ID&V on those individuals.

The Registry information is frequently accessed by financial institutions when conducting KYC. Under the 5AMLD, and subject to the outcome of the Companies House consultation, financial institutions in the UK will be required to notify Companies House about any discrepancies in the information they may hold about an individual who is a beneficial owner identified on the Register.

[11] See: Corporate transparency and register reform. Available at: https://www.gov.uk/government/consultations/corporate-transparency-and-register-reform.

We see an opportunity to improve consistency of ID&V information shared between financial institutions and Companies House by allowing digital identification to be used by both stakeholders. This would help to set a "base line" standard of ID&V and allow Companies House to verify the identity of UK individuals recorded on the register in a more streamlined fashion.

1.3 Re-Use of Digital Identification – Payment Services Directive 2 ("PSD2")

We also see positive benefits to assessing whether digital identification might be reused in relation to the strong customer authentication requirements, leveraging existing research undertaken in this topic.[12]

Considering the regulatory ecosystem in which UK financial systems operate, there is value in considering the various areas in which ID&V requirements exist and whether the reuse of digital identification would be both viable and beneficial to both organisations and their customers.

1. Section 5 – Criteria for Trust / Sections 6 and 7 – Questions on the Role of Government / Role of the Private Sector

12. What's the best model to set the "rules of the road" to ensure creation of this trusted market?

13. Who do you think should be involved in setting these rules?

18. What legislation and guidance requires updating to enable greater use of digital identities?

21. What is the private sector's role in helping to create a trust model (based on the criteria for trust in section 5), and how should they remain involved in its long-term sustainability (for example funding, helping create the rules of the road)?

We again answer the following questions collectively below.

[12] See Michael Adams, eIDAS Observatory, "PSD2's use of eIDAS certificates for the identification of PSPs: A suggestion with respect to mobile apps. [online] Accessed on 13 Sept 2019 at: https://ec.europa.eu/futurium/en/eidas-observatory/psd2s-use-eidas-certificates-identification-psps-suggestion-respect-mobile-apps

2.1 "Rules of the Road" Development

EFI's financial institution clients provide products and services both in the UK and to the European jurisdictions. From our experience, it is essential to ensure that any regulatory framework on digital identification reuse facilitates the UK's ability keep pace with the evolving digital identity landscape, while ensuring that financial crime risks can continue to be effectively detected and prevented.

In developing a model for the "rules of the road", there is an opportunity to leverage and learn from other digital identification reuse models being considered or used by other European jurisdictions. Jurisdictions such as Sweden, have been developed in which financial institutions can rely upon a digital identity issued under its eIDAS programme.

The intentions of Article 13 under the 5AMLD suggest that the providers of digital identification should not be limited to the eIDAS programme, but also include other parties as may be recognised by relevant national authorities:

1. Customer due diligence measures shall comprise:

(a) identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source, **including, where available, electronic identification means, relevant trust services as set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council (*) or any other secure, remote or electronic identification process regulated, recognised, approved or accepted by the relevant national authorities**; [**Emphasis added**]

A roadmap developed for the UK should ensure that controls are in place to mitigate fraud, cyber security and data protection risks, while also ensuring that innovation can take place, as the service evolves. Other regulatory authorities have considered the types of controls that might be used to mitigate these risks, including the European Supervisory Authorities in its opinion of January 2018.[13]. The JMLSG has also established the groundwork for such standards in relation to parties who undertake electronic verification of identity.[14]

[13] 23 January 2018. "Opinion on the use of innovative solutions by credit and financial institutions in the customer due diligence process". [online] Available at: https://esas-joint- committee.europa.eu/Publications/Opinions/Opinion%20on%20the%20use%20of%20innovative%20solutions %20by%20credit%20and%20financial%20institutions%20(JC-2017-81).pdf

[14] Note 6. JMLSG Guidance at 5.3.5

2.2 Guidance Development and Stakeholder Engagement

We would encourage the formation of a stakeholder body at which both "the rules of the road" and "lessons learnt" can be reviewed and acted upon to ensure that the digital identification programme remains relevant and fit for purpose. We have also seen in the case of financial crime prevention how collaborative initiatives, such as the JMLIT, have resulted in positive returns, in the area of financial crime detection and prevention.

We would encourage the development of guidance, in conjunction with other stakeholders including the regulated financial sector, managed services providers such as EFI and digital ID&V providers, to ensure that standards are complimentary to and aligned to any existing regulatory obligations under regulation 28 of the MERS and guidance on characteristics and evidence of identity in the JMLSG guidance.[15] Alignment of the Cabinet Office and Treasury has been previously identified as an important element of allowing digital identity reuse.[16]

We would also encourage the leveraging of previous working group feedback about frameworks of engagement in relation to the reuse of digital identity by the regulated financial services sector.[17]

We would encourage a broader dialogue with both HM Treasury, the Department for Business, Energy and Industrial Strategy, the FCA and the Payment Systems Regulator, to enable the reuse of digital identification.

[15] Note 6.
[16] Note 9.
[17] See Note 9.

2.3 Possible Regulatory Amendments

Several regulations may need to be amended order to permit financial institutions to rely upon digital identification. However, this would not require significant change to the regulatory framework of the MERs. Organisations required to comply with Regulation 28 could elect whether to accept digital identification as part of its KYC processes, and would still be required to undertake additional enquiries on a risk-basis.

Secondary instruments may require amendment to allow individuals to empower Companies House to undertake ID&V by relying on digital identification.

EFI thanks Companies House again for the opportunity to respond to this Call for Evidence. EFI would be more than pleased to take part in any further detailed discussions around formulating standards and guidance in support of the regulated financial sector's ability to rely upon digital identities.

Response prepared by Samantha Sheen, Financial Crime Adviser at Efficient Frontiers International, supported by Rob Windle.