Call for a comprehensive and harmonised EU regulatory framework for digital identity verification

Introduction to Onfido

Onfido is the global digital identity verification provider that works with 1,600 organisations worldwide, including many of the EU's FinTech's and innovative startups. We employ over 50 people in the EU and 350 globally, with offices in Paris, Lisbon, London and Berlin. Onfido embraces the opportunity to share our frontline experience and help develop regulatory reforms to foster innovation, accessibility and financial inclusion for all across national borders. Onfido is a founding member of the Better Identity Coalition in the US and a member of the FIDO alliance.

Digital identity verification enables access to financial services and tech ecosystems

*Digital identity verification is a key enabler for the financial services and tech ecosystems in Europe***.** It is a critical and foundational piece of the infrastructure required to complete the EU's vision of a Digital Single Market and Capital Markets Union. By verifying that a customer is who they say they are online as part of the onboarding process, European businesses from the tech, financial services, mobility, telecommunications, as well as other sectors, are able to register, onboard, authenticate, re-verify customers at scale quickly and securely. This in turn helps businesses to grow, create more jobs, and fuels their global competitiveness.

Onfido supports businesses across the EU

At Onfido, we help our clients fight fraud, supercharge onboarding and increase revenue through an innovative approach to identity verification**.** This includes:

- For Dutch independent neobank Bunq, who employs over 140 people in the EU and provides services in all EU Member States, our solution enabled the verification and onboarding of 5x more users with the same onboarding team. 80% of these users were approved in seconds and the rest within 5 minutes. Bunq previously relied on video calls, which lacked consistency, made the onboarding process too lengthy and an uncomfortable experience for users who didn't necessarily want to be on live camera.
- For French car-sharing service Getaround (previously Drivy), who employs over 400 people globally with offices in Paris, Berlin and Barcelona, our solution has driven user drop-off down by 23%.
- Finally, Onfido's solution has allowed AR24, the first provider of Certified Registered Mail in France (30 employees), to digitally onboard hundreds of thousands of French citizens, that are now enabled to receive Registered Mail in a reliable, fast, economical, and environmentally-friendly way.

Challenges arising from globalisation enhance the need for an EU-wide framework for digital identity verification

Living in a globalised world poses challenges, as well as opportunities. The *ongoing global health crisis following the COVID-19 outbreak, indicates the need for businesses around the world to become even more flexible and digital.* Consequently, there is an increase in demand for digital identity verification across a diversity of sectors including financial services, e-commerce, remittances, healthcare, online education, and online voting.

Digital identity verification also plays a key role in immunity passports, which are the linchpin of a new normality in a post-COVID19 society. Following significant restrictions because of the pandemic, for many EU countries reopening access through the safe movement of people is critical to economic growth and recovery. Immunity

passports are at the heart of this and for safety reasons, it is imperative that they cannot be traded. As such, a robust system to bind the identity of an individual to their immunity passport is crucial.

In addition, businesses that already rely on identity verification for the provision of their services, such as banks, are needing to quickly switch from using multiple channels including face-to-face and live-video link identification, to a single, fully digitalised channel due to the closure of branches and call centres.

More than ever, the crisis underlines the need for the EU to take action and create a harmonised EU-wide framework that supports digital identity verification and enables digital identity verification providers to bolster organisations across the EU in adopting safe and robust digital solutions.

Shortcomings of the current EU regime

Effectively, the lack of harmonised cross-border digital identity verification standards at EU level hinders the uptake of digital identity verification methods by businesses as they operate and expand across borders. The European Commission is increasingly aware of the importance of digital identities and the need to create a regulatory framework that supports cross-border digital identity verification solutions. The Digital Finance Strategy as well as the upcoming reviews of eIDAS and AML, provide an opportune moment to look at digital identity verification more broadly and put in place *a comprehensive, unified, highly robust, standardised, and certifiable framework which promotes user convenience, inclusiveness, and innovation.*

Our call/ the ideal solution for an EU-wide framework for digital identity verification

1. A framework that supports all digital / online use cases, across all sectors and markets

To ensure consumers can enjoy all the benefits that digital identity verification provides, *an EU-wide framework should be comprehensive, covering all aspects and use-cases of digital identity verification*. Digital identity verification is an essential enabler of the Digital Single Market and digital identity verification solutions will contribute to shaping the society of the future. *The Commission should therefore look to create a comprehensive framework for digital identity verification, not restricted to specific components and sectors.*

Digital identity verification solutions are progressively adopted by a wide range of businesses as a reliable source for verifying customers' identities in non-face-to-face settings. In financial services, digital identity verification is widely recognised as a valid method of validating a customer's identity. Other examples include age verification for online gambling, verification of identities for e-Pharmacies and telemedicine, as well as for car rental and home sharing in the travel sector. In addition*, digital identity verification solutions enable easier access to products for consumers***,** including by providing greater flexibility and accessibility for particular services such as hotel check-ins, airport bag drop, visa checks and events as well as social media and online dating. In addition, governments are starting to adopt E-voting solutions, which is particularly important in view of the ongoing crisis.

A digital identity verification framework should apply to all these different use cases, in addition to more well-known examples in the financial services industry, including payments, fundraising, investing, crowdfunding, as well as crypto-related activities and crowdfunding.

2. A highly standardised framework, certifiable around predefined Levels of Assurance

The Commission should look to create an EU-wide certification scheme, including certifiable standards and strictly associated with measurable “levels of assurance”.

To ensure the highest level of robustness, harmonised rules should raise the bar on minimum identity verification standards. We believe that a robust two-factor verification should be included in the Digital Finance Strategy, as well as a future eIDAS revision, with a minimum bar / threshold that's higher than identity record (as is currently used by Member State regulators including the UK FCA).

Robustness of the two-factor approach can be ensured by linking the carbon-based human being, to their ‘official’ or legal identity anchor:

1. Legal identity (ID or passport)
2. Biometrics / face

The Commission should adopt minimum standards to ensure all market participants operate above the bar. Setting harmonised EU digital identity verification standards will benefit businesses and consumers alike, by giving guarantees that accepted digital identity verification solutions within the EU are robust.

Through the creation of harmonised standards, *the Commission can ensure that businesses will no longer need to implement tailored models in each jurisdiction, leading to a reduction in costs and making the market more accessible to new innovative solutions*. Furthermore, this will strengthen the position of European digital identity verification providers who will be able to access more Member States, technologies and consumers, *which in turn will strengthen Europe’s competitiveness in the field of digital identity verification.*

Robustness: manual vs. machine driven

In the old world of offline and in-branch interactions, face-to-face was deemed the “golden standard” in verifying the identities of individuals accessing products. As the world moves online and access to services goes digital, face-to-face verification is increasingly shown to be unfit for purpose.

Machine-led identity verification comes out on top against traditional face-to-face methods for biometrics. Studies have shown that human agents miss up to 14% of fraud when comparing the face in front of them to the photo on an ID. Unlike manual agents, our algorithms do not tire or succumb to individual biases, with just one instance of face-matching fraud per 1,000 checks, which is 140x better than a human. Algorithms furthermore evolve over time, with every data point for consistent improvement and performance.

With this in mind, *we strongly disagree with the recent FATF recommendation on digital identity verification, that the strongest Level of Assurance would require a mandatory live video interaction with an operator.* Supported by evidence, we believe that an hybrid approach, which leverages the best of human experts and Artificial Intelligence, is more robust, catching more fraud than either method alone and ensuring a balance of security and user experience for digital interactions.

Knowing the risks of a risk-based approach

The Financial Action Task Force promotes a risk-based approach. *While we agree there are benefits to a risk-based approach, the danger is that by only responding to risks when these are exposed, the bar for digital identity verification providers is not set high enough.*

Crucially, credit rating agencies have become sources of identity information against which people can be verified when using an identity verification service. However, these are sub-optimal methods of identity verification considering the centralised databases have frequently been hacked and their 'knowledge-based questions' methodology is no longer secure. In addition, credit bureaus present accessibility challenges as younger clients or migrants might not always appear on the databases as they do not have a well enough established credit record. *We believe that the bar for digital identity verification should be set high and that unsafe knowledge-based solutions should be strictly limited in use.*

3. Mandatory and harmonised framework across the EU27 and sectors

The current regulatory fragmentation around eKYC standards causes digital identity verification providers to face significant operational and technical difficulties. *The patchwork of standards that exists across Member States causes a high level of uncertainty for businesses and effectively blocks consumers in some EU Member States from using safe and user-friendly digital identity verification solutions in other Member States.*

To illustrate this point, while some EU Member States accept facial checks with video or static images, other Member States only accept identification via a synchronous video call. For digital identity verification providers, being unable to operate under the same conditions across borders means that we can only operate in certain countries in the EU.

We believe that a future EU-wide certification scheme should provide for mutual recognition, with Member States required to accept solutions that are considered safe in others to ensure continuity for consumers and businesses alike. Uniform EU-wide rules should govern the conditions under which verified identities may be mutually recognised, based on certifiable standards.

It is again worth noting that *digital identity verification is not restricted to financial services and is increasingly used in other sectors* such as healthcare, education, online voting, e-Commerce and social media. An EU-wide framework should provide for the diversity of use cases in which digital identity verification is or can become an integral part of business models.

Regulators across all sectors should be made aware of the benefits of digital identity verification and ensure that EU-wide digital identity verification standards are implemented appropriately to facilitate the uptake of digital identity verification solutions across all markets and in all Member States.

4. Rules are framed around tech neutrality and performance/outcome for business and end users

A functioning Digital Single Market must keep the door open to benefits of new RegTech technologies, standards and processes. Global developments have indicated the importance of digital solutions in a diversity of sectors, which increases the need for robust digital identities**.** *Recommendations adopted in the Digital Finance Strategy should result in putting in place a regulatory framework for digital identity verification that is proportionate to the risks presented, ensuring that solutions can remain user-friendly.*

While setting the bar high for harmonised EU digital identity verification standards, a future framework should be principled-based, and not overly prescriptive in order to keep the door open to new robust European technologies.

Restrictive and technology-specific models are harming competition by prohibiting new, innovative solutions from entering some markets while having been accepted as safe and robust in others. There should be a joint standard across the EU which allows innovative RegTechs, FinTechs and startups to access all markets across the EU.

A principled-based framework should be based on a performance driven standard, founded on user experience parameters and a maximum false acceptance rate (the likelihood that the system in place will incorrectly let in fraudsters).

Portable digital identity

The Commission should take note of developments in the market and ensure that a regulatory framework is technology-neutral and allow for the future adoption of innovative solutions. One trend that the Commission should take into consideration is the move towards portable digital identity solutions, which empowers users to reuse their verified electronic identity for multiple domains.

Portable identity solutions provide significant benefits to users, giving them control over their personal data and promoting a user-friendly experience. Rather than having to re-enter personal data when accessing a new service, users can reuse their already verified identity, which promotes safety, interoperability and accessibility.

An EU-wide certification scheme should keep the door open to portable identities. We should work towards a credentialed portable identity model issued by third parties, giving users ownership of their digital identity. This includes:

- An EU-wide certification scheme, which allows for portability.
- The bar for the initial verification should remain high, excluding unsafe knowledge-based solutions.
- A substantial or high Level of Assurance should be the minimum for a solution to be accepted across Member States.
- Third party private actors should be assigned by Member State competent authorities or the EU as suitable to provide the best service to users. Digital identity verification providers should be covered under the scope and be able to certify under the Levels of Assurance.
- Users should be able to utilise their portable identity for a diversity of domains, including financial institutions but also other services, such as age verification, healthcare, online education and social media networks.