FRA0071

Written evidence submitted by OneID Ltd

OneID Ltd is a UK fintech that provides a digital identity service that enables anyone to prove who they are online by consenting to share identity data from their bank to another 3rd party. We are regulated by the Financial Conduct Authority (FCA) for Open Banking and are working with many of the UK's high street banks. We are also certified under the Department of Science, Innovation and Technology (DSIT) Digital Identity and Attributes Trust Framework as an identity provider and orchestrator (data broker role).

The prevalence of fraud

How offenders are committing fraud and the impact of this fraud on victims.

Fraudsters take advantage of a lack of reliable identity on the internet and human vulnerabilities to pretend to be people they are not, or to work for organisations that they are not connected to.

Within Financial Services, a fraud known as Authorised Push Payments (APP) fraud occurs when fraudsters trick people into sending them payments, usually via the UK's Faster Payments scheme. APP fraud cost UK banks and customers £485m in 2022; money which went to organised crime to fund drug smuggling, people trafficking and other huge social problems. Fraud is not the 'victimless' crime that some in politics like to portray it as; victims can be left traumatised, embarrassed, and ashamed that they have been duped.

How the emergence of new types of technology, such as artificial intelligence, is being used to commit fraud.

AI is already being used by fraudsters to create 'synthetic identities' (combining data from a real person with a generated picture, for instance) to open accounts and commit fraud. A digital identity can be used to prove that someone is a real human.
We have published a paper on the role of digital identity in helping to govern AI; we believe that individuals and corporates who use AI should have accountability for what the AI does, or content that it produces, and any IP rights that are used in the creation of new content. Digital identity provides a mechanism to see 'who is accountable' for the bot/content via watermarking, digital certificates and other 'stamps' that can be traceable back to the humans/corporates in charge. AI without an owner can then be treated as suspicious, not allowed to connect or turned off from social media feeds as being unverified or unsafe.

The role of internet providers and social media providers in enabling or preventing fraud and actions they could take.

The Financial Services industry has argued that since most fraud originates on social media platforms (see LBG report and NWG report), the platforms should be doing more to prevent the harm and costs from occurring, but they currently have no incentive to do so.

We believe that the imminent Online Safety Act is a good start to shifting focus and responsibility to Big Tech; for example, requiring platforms to do age verification of their

users to protect children online. Social media platforms could adopt identity verification from the UK's existing certified identity industry, to ensure that account owners are humans and can be held accountable for their actions. To maximise the benefits, identity verification should be done by the platforms as a cost of running their platform and offered to all users, rather than being a 'premium' paid service. And 'verification' should be to a defined standard; Ofcom could define this by leveraging the DSIT identity framework.

Further legislation will likely be necessary to increase the pressure on platforms for positive change. This will take time, so for now, effective solutions to combat fraud should also be introduced by the FS sector.

New processes can be introduced to prevent scams; OneID would like to see UK banks trying a different approach to counter APP fraud, in line with the Payment Systems Regulator's (PSR) view that "*We want to see PSPs develop new processes to prevent scams from happening*." The focus should be on fraud prevention as well as detection and reporting.

Banks can act today by enabling a bank-based digital identity check in customer journeys when customers interact with unknown parties over insecure channels (platforms, email, messaging etc.). The payer can share a link for the payee to verify themselves to the sending bank (via a digital identity and Strong Customer Authentication), before any payment is initiated, creating a more secure 'new beneficiary' journey.

Reporting, investigating and prosecuting fraud

Given that it is estimated 70% of fraud either originates aboard or has an international element, what is being done to prevent fraud arising through those international channels?

OneID enables any of the 50 million UK citizens who use online banking to prove who they are online. If social media and other platforms adopted these simple checks, they could prevent the majority of the 70% from getting through the process, as they wouldn't have a UK bank account.

What other countries are achieving in terms of detection, prevention and prosecution of fraud.

The introduction of a bank-based identity system in Norway, called BankID, has led to the reduction of fraud to only 0.00042% of payment volumes. BankID is used by most people for most interactions online, thus keeping the fraudsters out.

How better to collect and use data on the scale, cost and nature of fraud.

By some estimates fraud could be as much as £219bn in the UK (Crowe/University of Portsmouth). Better categorisation and consistency of recording fraud could help to bring more confidence to assessing the scale of the UK's fraud problem.

FRA0071

Fraud reporting is fragmented in the UK, and not consistent across the different reporting bodies such as ONS, Action Fraud, Cifas and UK Finance. Agreeing on the categorisation and terminology of fraud typologies, and using the same terms consistently, will help to align meanings and comparability of data across them. This would enable the impacts of anti-fraud initiatives to be measured over time.

Fraud reporting for payment systems could also be improved by UK Finance. Fraud is currently reported as an absolute value (e.g., £485m for APP fraud), but this does not reflect any change in payment volumes; a fraud figure as a percentage of payment volumes would give a more complete picture of whether anti-fraud measures were working. Fraud on card networks is typically around 6 basis points, for instance, and is stable as payment volumes grow, indicating that card fraud is relatively under control.

The Payment Systems Regulator (PRS) has made recommendations for improving fraud reporting. It would be ideal if a fraud reporting framework could be designed that could be applied to all payment schemes (including any future-regulated ones such as the digital pound or stablecoins), which would enable comparison between payment rails and incentivise shifts towards those which deliver better fraud controls.

OneID is committed to making the world a safer place, which includes stopping people from becoming victims of online scams; our focus is on fraud prevention, upstream of the payment, where the fraud occurs. We will continue to work with banks and platforms to improve customer journeys to help keep customers safe online and stop fraud. More support from the government in the form of awareness of the DSIT framework, and requiring adoption of better digital identity technology, will help reduce fraud further.

For details on how digital identity can help with AI governance:
https://oneid.uk/news-and-events/how-digital-identity-can-protect-against-misuse-of-ai

For details on APP fraud, please see our recent paper on the topic:
https://oneid.uk/news-and-events/digital-identity-verification-supporting-the-financial-services-sector-in-the-fight-against-fraud

October 2023