
# Comments to the Basel Committee on Banking Supervision

# Discussion Paper on Digital Fraud and Banking

**February 2024**

**Introduction**

The Better Identity Coalition appreciates the opportunity to provide comments to the Basel Committee on its Discussion Paper on Digital Fraud

As background, the Better Identity Coalition is an organization focused on developing and advancing consensus-driven, cross-sector policy solutions that promote the development and adoption of better solutions for identity verification and authentication. Our members – 23 companies in total – are recognized leaders from different sectors, encompassing firms in banking, fintech, payments, health care, technology, and security.

The coalition was launched in February 2018 as an initiative of the Center for Cybersecurity Policy & Law, a non-profit organization dedicated to promoting education and collaboration with policymakers on policies related to cybersecurity. More on the Coalition is available at https://www.betteridentity.org/.

In 2018, we published "Better Identity in America: A Blueprint for Policymakers" – a document that outlined a comprehensive action plan for the government to take to improve the state of digital identity in the US.

While the Coalition initially focused on the US, most of our members operate globally, and international coordination between the US and other government on digital identity issues is one of our five key priorities. Given this, the Basel Committee's recent discussion paper on digital fraud in banking is of particular interest to the Coalition.

Up front, we note that we are pleased to see the Basel Committee focus on this issue. Digital fraud rates have been rising in recent years, and while the sophistication of our defenses against attacks have been growing, so have the capabilities of our adversaries. As the paper rightly notes:

> *Criminals are exploiting digitalisation to commit online fraud at a greater scale and scope than previously – notwithstanding important data caveats and gaps – as digitalisation enables fraudsters to be more agile.*

This will remain a challenging issue for the financial services industry for the foreseeable future.

With regard to the discussion paper, we offer two comments:

1) We believe the paper underemphasizes the role of inadequate digital identity infrastructure in fueling attacks that lead to digital fraud.

2) With this, we believe the paper should highlight that the burden in addressing digital identity infrastructure is not just a private sector issue, but one where governments across the globe must also play an increased role.

We detail each of these issues below.

1) **The paper underemphasizes the role of inadequate digital identity infrastructure in fueling attacks that lead to digital fraud.**

We appreciate that the paper touches on digital identity challenges in several places:

- In discussing the root of fraud, the paper rightly notes: "Digital fraud relies on the inability to verify who is at the origin of the action, due in part to the lack of appropriate authentication technology to identify the legitimacy of counterparties."
- The paper also talks about ways that compromises of identity tools can be used to commit digital fraud through customers' data or banks' systems, noting: "The opening of bank accounts and/or applying for credit cards using stolen identities (eg bought on the dark web) or false identities."
- It also makes reference to the Committee's 2003 "Risk Management Principles for Electronic Banking" which notes: "Banks should take appropriate measures to authenticate the identity and authorisation of customers with whom they conduct business over the internet."
- The paper also notes in several places that legacy authentication approaches such as two-factor authentication based on one-time passcodes (OTPs) are now being bypassed, as adversaries have innovated and found ways to defeat tools that were at one time considered relatively secure.

While all of these data points focus on different aspects of exploits of digital identity infrastructure, the fact that these references to identity challenges are sprinkled throughout the document – rather than called out as a standalone category – is a mistake, in our view.

Exploits of insufficient identity infrastructure have been a rapidly growing attack vector in financial services, as well as online service more generally. And with the emergence of generative AI that can help attackers craft more sophisticated phishing attacks or defeat some biometric verification systems through deepfakes, this threat will only become more of a problem in the years to come.

This point was made crystal clear last month in a report from the U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN), who published a Financial Trend Analysis[1] that – for the first time ever – look to quantify the impact of identity-related attacks on financial crime. Their analysis of how adversaries are leveraging identity as an attack vector was astounding: in reviewing Suspicious Activity Reports (SARs) filed by financial institutions in 2021, they discovered that approximately 1.6 million, or 42% of around 3.8 million total

[1] See "Identity-Related Suspicious Activity: 2021 Threats and Trends" posted at https://www.fincen.gov/sites/default/files/shared/FTA_Identity_Final508.pdf

Bank Secrecy Act (BSA) reports, equivalent to $212 billion in suspicious activity, related to identity.

These numbers track with what our Coalition's members have been seeing, with attacks that look to exploit different layers of digital identity infrastructure skyrocketing.

Accordingly, we believe this is a trend that is important enough that the Basel Committee should highlight it separately, rather than spread data points that only tell part of the story throughout the paper.

2) **With this, we believe the paper should highlight that the burden in addressing digital identity infrastructure is not just a private sector issue, but one where governments across the globe must also play an increased role.**

The draft paper right flags that banks need better tools here, noting:

> *Banks should take appropriate measures to authenticate the identity and authorisation of customers with whom they conduct business over the internet. Failure on the part of the bank to adequately authenticate customers could result in unauthorised individuals gaining access to electronic banking (e-banking) accounts and ultimately financial loss and reputational damage to the bank through fraud, disclosure of confidential information or inadvertent involvement in criminal activity.*

However, framing this issue solely as one that banks need to address – without acknowledging the critical role that governments play in identity – means that the Committee's paper is overlooking a key element of the solution.

Put simply, governments are the only authoritative issuer of identity. There are a number of industry solutions used by banks that effectively try to guess what the government knows – some quite accurately – but there is a gap between the nationally recognized, authoritative credentials issued around the globe which work in the physical world, and the absence (in most countries) of any digital counterpart to those credentials that can be used by consumers to prove who they are in the online world.

It is this gap that is being increasingly exploited by organized criminals and hostile nation-states to leverage spoofed identities or stolen identity data to steal hundreds of billions of dollars each year. As such, it is impossible to discuss solving identity-related fraud without discussing the need for governments across the globe to focus on initiatives to close this "identity gap." Portraying this issue solely as a bank responsibility oversimplifies the problem set, and more importantly, might prompt governments to overlook the essential role they play in solving digital fraud challenges.

Our Coalition has put forth a Policy Blueprint that suggests government can help to improve the current ecosystem of industry solutions by creating new digital identity tools that close the identity gap – by allowing consumers that were already issued a credential by an agency for use in the physical world to ask that agency to "vouch" for them when they need to prove who they are in the online world – by validating the information from that credential.

Across the globe there are different versions of this model starting to get attention from policymakers – from the introduction of the "Improving Digital Identity Act" in the U.S. House and Senate, to the European Union's new initiative to create digital identity wallets for its residents. Given that the Basel Committee's work here will be highly influential in driving what other governments do on this front, it is critical that the Committee call out the unique role government has to play in fighting digital fraud by improving identity infrastructure.

We greatly appreciate your willingness to consider our comments and suggestions, and welcome the opportunity to have further discussions. Should you have any questions on our feedback, please contact the Better Identity Coalition's coordinator, Jeremy Grant, at jeremy.grant@venable.com.