Comments to the Office of the Comptroller of the Currency (OCC), Federal Reserve System (FRS), and Federal Deposit Insurance Corporation (FDIC)

Request for Information on Potential Actions To Address Payments Fraud

September 2025

The Better Identity Coalition appreciates the opportunity to provide comments to the Office of the Comptroller of the Currency (OCC), Federal Reserve System (FRS), and Federal Deposit Insurance Corporation (FDIC on its *Request for Information on Potential Actions To Address Payments 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 – 21 companies in total – are recognized leaders from different sectors of the economy, encompassing firms in financial services, health care, technology, fintech, payments, and security.

Up front, we note that of our 21 members, roughly half are either financial institutions, fintech or payments firms; many of our other members create the solutions that are used by these firms to vet, validate, and authenticate digital identity. This unique mix of members allows the Coalition to weigh in from the perspective both of the firms that will be most impacted by any new action from financial regulators, as well as those who be asked to deliver solutions to help these firms comply.

The coalition was launched in February 2018 as an initiative of the Center for Cybersecurity Policy & Law, a non-profit 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 U.S. government to take to improve the state of digital identity. In the Blueprint, we specifically called on the Treasury Department and financial regulators to take a leadership role in driving the adoption of more resilient digital identity solutions across the financial services market. We published an updated version of this Blueprint in January with a set of recommendations for the new Administration, and which reiterated this point.

On this front, we have been encouraged by Treasury's recent work around digital identity – including raising questions about digital identity verification in last month's RFI on Innovative Methods to Detect Illicit Activity Involving Digital Assets, and also highlighting the importance of digital identity in the Administration's recent report on Strengthening American Leadership in Digital Financial Technology.

With regard to this RFI, we believe the key point for OCC, the FRS, and FDIC to understand is that a significant portion of payments fraud is tied to compromises of identity or authentication – and that the government has a significant role to play in addressing deficiencies in identity and authentication infrastructure that have made it easy for adversaries to perpetrate this fraud.

While exact statistics on the amount of payment fraud tied to identity are hard to come by, there are a set of reports from the U.S. government that together make clear that weak identity and authentication infrastructure presents a serious problem in payments fraud and other financial crimes.

- The Financial Crimes Enforcement Network (FinCEN) has noted that $212 billion worth of suspicious financial transactions in 2021 was tied to some form of identity compromise;[1] at a 2024 conference, they revealed that this number had exploded in 2023 - covering over 70% of all Suspicious Activity Reports (SARs) filed by banks, tied to $394 billion of transactions.[2]

- The Government Accountability Office (GAO) estimates that fraud losses cost the government $233 billion-$521 billion annually; GAO noted that pandemic unemployment insurance fraud losses alone totaled $100-135 billion, and that most of these losses were tied to identity fraud.[3]

- Chinese state-sponsored attackers have stolen billions through identity-centric attacks;[4] the Justice Department has noted North Korea stole more than $2 billion to fund its nuclear program through similar attacks targeted against banks and crypto exchanges,[5] and more recently spoofed identities to place North Koreans in remote IT jobs to generate additional money to fuel its weapons of mass destruction.[6]

Against this backdrop, we are now seeing the rise of new, more sophisticated attacks on identity such as AI-powered deepfakes that, if unaddressed, threaten to push losses from identity-related cybercrime and payments fraud to new levels and undermine confidence in our increasingly digital economy. As fraud and scams continue to rapidly evolve, policymakers must prioritize a cross-sector, whole-of-government, public-private approach — including social media and telecom companies, banks, fintech, nonprofits, law enforcement, and government officials at all levels — to stop criminals and better protect consumers. Industries must have the flexibility to innovate in response to these growing threats, especially as new technologies and AI tools make deceptive communications appear more legitimate.

Given the focus of our coalition on identity and authentication issues, we are limiting our responses to a subset of questions (10, 16, 23, 24, 25) from the RFI.

---

[1] See https://www.fincen.gov/sites/default/files/shared/FTA_Identity_Final508.pdf and https://www.fincen.gov/sites/default/files/2024-06/PREPARED-REMARKS-IDENTITY-PROJECT-COLLOQUIUM-FINAL-508_0.pdf

[2] As detailed in a FinCEN speech at the 2024 Fed ID Forum – see https://events.afcea.org/FedID24/Public/SessionDetails.aspx?FromPage=Sessions.aspx&SessionID=11005&SessionDateID=747

[3] See https://www.gao.gov/products/gao-24-105833 and https://www.gao.gov/blog/more-fraud-has-been-found-federal-covid-funding-how-much-was-lost-under-unemployment-insurance-programs

[4] See https://www.justice.gov/opa/pr/seven-hackers-associated-chinese-government-charged-computer-intrusions-targetingperceived

[5] See https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commitcyberattacks-and and https://www.reuters.com/article/world/north-korea-took-2-billion-in-cyberattacks-to-fund-weaponsprogram-un-report-idUSKCN1UV1ZX/

[6] https://www.fbi.gov/wanted/cyber/dprk-it-workers

10. The Board, FDIC, and OCC have issued supervisory guidance on numerous topics that relate to payments fraud detection, prevention, and mitigation. Is existing supervisory guidance related to payments fraud sufficient and clear? If not, what new or revised supervisory guidance should the Board, FDIC, and OCC consider issuing on this topic within the respective authorities?

There are several areas that would benefit from additional insight to facilitate fraud prevention, improve detection, and expedite mitigation. One area where our members continue to raise concerns is around the use of new identity verification and authentication technologies – specifically, how regulators will respond to a financial services firm that decides to use them.

We were pleased to see that FDIC recently weighed in with new supervisory guidance on the use of pre-populated information for purposes of meeting Customer Identification Program (CIP) requirements,[7] which helped to clarify that financial institutions are allowed to use these solutions.

Another area where regulatory ambiguities may be inhibiting the adoption of new, more secure identity verification solutions by financial institutions to satisfy CIP requirements is around the use of "mobile Driver's Licenses" (mDLs).

In recent years, states have started to issue mDLs – a digital counterpart to the plastic credentials that states issue their residents today. Whereas someone might carry their physical driver's license in their wallet, pocket, or purse, mDLs are typically carried in a "digital wallet," which may be developed by the manufacturer of a smartphone or a third party. In some states, the state itself is the supplier of the digital wallet app.

While current CIP guidance makes clear that banks can take a risk-based approach to customer identification – and does not preclude the use of new identification technologies – the new and novel nature of mDLs had led many of our members to report that their compliance teams are not comfortable with using a mDL as part of meeting CIP requirements unless regulators indicate that it is permitted or encouraged. Much of the concern seems to spring from the fact that an examiner may, from time to time, question the use of new and novel tools as being "unproven." With this, our members are concerned about the potential risks involved with a new tool such as a mDL.

From our perspective, regulators should be embracing mDLs:

- They are more secure than plastic driver's licenses, given that they are cryptographically signed by the state government issuers and stored – in most cases – in trusted hardware inside consumer smartphones.

[7] See https://www.fdic.gov/news/financial-institution-letters/2025/fdic-supervisory-approach-regarding-use-pre-populated

- The REAL ID Modernization Act of 2020[8] specifically recognizes that a mDL can be used to meet REAL ID Act requirements – and the Department of Homeland Security (DHS) has published updated REAL ID regulations outlining the requirements mDLs must implement to be accepted by Federal agencies.[9]
- At a time when identity-related financial fraud and cybercrime is rising (per the FinCEN analysis discussed earlier), mDLs offer a way for consumers to prove who they are for online account opening in a way that is more secure and convenient than many of the legacy solutions used today to support this requirement.
- mDLs can also be better for consumer privacy – in that they allow for a consumer to only choose to share certain data fields from their mDL. A bank should in most cases only need to know the name, date of birth, address, and identification number from a consumer's driver's license, but they should have no need to see a consumer's height or weight, or whether they are an organ donor.

Despite any regulatory uncertainty, banks are very interested in using mDLs. Seven major financial institutions have partnered with the National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) on a new project to accelerate the adoption of mDL standards and best practices, and build a reference architecture demonstrating real world business use cases, integrating mDLs with commercially available technology and into business processes including those tied to account opening.[10]

As NIST prepares to publish the outputs of this project later this fall, our members are very eager to see a clear statement from financial regulators that they are permitted to look to make use of mDLs to meet CIP requirements. Supervisory guidance similar to what FDIC just issued around pre-fill would remove any regulatory ambiguities and put a policy foundation in place for banks to start to adopt more secure, convenient, privacy-preserving identity verification tools in account opening processes.

16. Broadly, how could payments fraud data collection and information sharing be improved?

While the work FinCEN has done to date does not apply only to payments fraud data, FinCEN's efforts to quantify the percentage and dollar value of SARs that are tied to some sort of compromise of identity or authentication has been incredibly valuable, in that it is the first time that any source – government or industry – has been able to measure the impact of deficiencies in identity and authentication infrastructure on the financial services sector.

[8] See https://www.dhs.gov/archive/real-id/news/2020/12/28/dhs-modernizes-critical-identification-requirements-after-congress-passes-real-id
[9] See https://www.federalregister.gov/documents/2024/10/25/2024-23881/minimum-standards-for-drivers-licenses-and-identification-cards-acceptable-by-federal-agencies-for
[10] See https://www.nccoe.nist.gov/projects/digital-identities-mdl

By defining the size and scope of the problem – and breaking down different attack vectors used in identity-related financial crime – industry and government now have a common understanding of the issues at play.

We would like to see FinCEN continue its work here, and would suggest:

- FinCEN should publish an annual report that analyzes SARs from the previous year, and details what has changed
- With this annual report, FinCEN should start to incorporate details on the number SARs that are tied to payments fraud – and break down what percentage and value of those SARs are of identity-related
- FinCEN should start to report on the number and value of SARs that are tied to deepfakes, in accordance with its alert last year on this topic[11] and request for financial institutions to start including the term "FIN-2024-DEEPFAKEFRAUD" in SARs where a deepfake is believed to have played a role.

Additionally, wider use of cross sector, multi-jurisdiction identification sharing platforms would improve verification of customer identity credentials. For example, the agencies should encourage states to participate in the American Association of Motor Vehicle Administration (AAMVA) Driver's License Data Verification (DLDV) service, which uses real-time driver's license/identity information verification methods. Data sharing here is most effective when all states are participating; however, currently, there are at least seven states that are not fully participating in the DLDV service, including Alaska, California, Louisiana, Minnesota, New York, Pennsylvania, and Utah. By not having this type of information verification method, consumers are more prone to identity theft and fraud.

In general, structured verification outputs (i.e., "match", "close match" "match") and behavioral analytics tools that categorize anomalies in account data can support more actionable data that can improve fraud detection. DLDV is just one example of the tools that are out there, but there are private sector tools that can assist as well, and that can help in identifying mismatches between account names and numbers or other identifying information. These insights can be used to support internal fraud monitoring systems and inform regulatory reporting.

[11] https://www.fincen.gov/sites/default/files/shared/FinCEN-Alert-DeepFakes-Alert508FINAL.pdf

23. What types of payments fraud have most impacted your organization and its stakeholders? What tactics have criminals employed when perpetrating these types of payments fraud?

In line with FinCEN's recent analysis, our members – both financial services firms and the vendors that support them – have noted that they are seeing payments fraud perpetrated using a variety of tactics tied to compromises of identity and authentication. These include:

- Compromises of authentication leading to account takeovers
- Phishing – where an attacker tricks an individual into a variety of things, including:
  - Sharing their password
  - Sharing the one-time passcode that serves as a second factor to protect their account, and/or tricking someone into pushing an "approve" button on a push notification used as a second factor
  - Sharing payment information – such as credit card numbers paired with expiration dates, CCV codes, and zip codes – with an attacker who is spoofing a merchant or other organization
- Impersonation attacks – convincing a consumer that the attacker is somebody that they are not. These attacks often include scams focused on tricking consumers to instantly send money through payment apps
- Traditional identity theft – where an attacker steals someone identity and then opens an account in their name used to make payments.
- Use of synthetic identities to establish new accounts used to commit payments fraud

An important trend for FDIC, FRS, and OCC to be aware of is the increasing use of deepfakes in these attacks. Increasingly, deepfakes are being used to spoof voices, photos, and videos, as well to craft sophisticated phishing and impersonation attacks that can more easily dupe consumers. Our members report seeing a sharp increase over the last 18 months in deepfake attacks; attacks that used to be very difficult and resource-intensive to launch are now becoming commoditized, thanks to tools offered by criminal services that have made it cheap and easy for even amateurs to create a convincing deepfake.

We appreciate FinCEN flagging these concerns in last year's alert; we believe more attention will be needed on this issue as deepfakes become increasingly commoditized and more difficult to detect.

24. What measures, including technological solutions or services, have been most effective in identifying, preventing, and mitigating payments fraud at your institution? Are there actions that consumers can take that help institutions? For example, do financial institutions find it helpful when consumers alert the institution in advance when making large purchases, transferring large amounts of money, and traveling abroad?

At a high level, we are seeing financial institutions, technology companies, and third-party service providers leveraging a variety of tools to mitigate potential fraud risks. These include multi-layered, advanced digital identity solutions that make use of tools including:

- Phishing-resistant authentication rooted in public key cryptography. Phishing attacks that are focused on stealing both passwords and multifactor authentication (MFA) codes have been on the rise in recent years; the FinCEN report we referenced earlier noted that *"18%, or approximately 446,000 identity-related BSA reports, report that attackers used compromised credentials to gain unauthorized access or misused their authorized access to generate illicit proceeds. Compromises are disproportionally costly as they accounted for 32% of the total suspicious activity amount or $112 billion."*

  Phishing attacks are now being supercharged by generative AI tools that significantly simplify the creation of compelling phishing campaigns at scale. This, in turn, is making it much easier for adversaries to compromise legacy MFA tools and creating an imperative to implement phishing-resistant authentication for users, such as tools that use PKI or the FIDO standards, both of which leverage asymmetric public key cryptography to block phishing attacks.

  Here we note that the emergence of passkeys which enable passwordless logins using the FIDO standards are very promising, and NIST recently issued guidance making clear that passkeys meet Authentication Assurance Level 2 (AAL2) requirements for MFA.[12] However, despite the NIST guidance, we continue to hear from financial services firms that there is regulatory uncertainty about whether and when passkeys can be used. This is an area where clearer guidance from Treasury and the financial regulators would be most welcome.

  We note that while phishing-resistant MFA is the strongest form of MFA, organizations continue to use a variety of types of MFA to guard against different attacks, including some powered by AI, that seek to compromise the authentication process – in many cases pairing "traditional" MFA (i.e., something you have, know, or are) with the risk analytics tools described in the next bullet.

- Risk analytics engines. These technologies will look at multiple attributes of a user attempting to access a system, such as IP address, device information, geolocation, past user behavior, and other metadata from the user and create a score that the individual is who they claim to be. As with liveness detection, many of the best tools that are being used in risk analytics engines make use of AI themselves. These tools often employ point-in-time assessments at different parts of the identity lifecycle to identify anomalies, deviations, and other risks. Because most of these tools run "behind the scenes," they can be a relatively frictionless way to apply enhanced security measures

[12] See https://pages.nist.gov/800-63-4/sp800-63b.html

without degrading the user experience. Real-time account verification and anomaly detection tools have proven effective in identifying fraud vectors such as synthetic identities and Authorized Push Payment (APP) scams, which are increasingly used in conjunction with deepfake typologies. Likewise, real-time verification tools that validate account ownership before transactions are initiated can enhance compliance with AML and KYC frameworks, while also reducing fraud risk in domestic and cross-border payments.

- Remote document authentication and "selfie-match" technologies. On the identity proofing side, many of our members have augmented knowledge-based verification tools which have been traditionally used to support CIP requirements in remote account opening with newer technologies, such as those that ask a customer to take a photo of their driver's license, state ID card, or passport, and then submit a "selfie" photo. These solutions analyze whether the credential appears to be legitimate, as well as whether the photo on the ID matches the selfie (by conducting a 1:1 biometric verification against the photo on the credential). Performance varies among different products; DHS's Science and Technology Directorate has launched a program to test these products,[13] and the FIDO Alliance has launched an industry-led program that partners with accredited test labs to test and certify that products meet expected performance requirements.[14]

- Liveness detection for biometrics. Generative AI has made it much easier for adversaries to create convincing fake photos, voices, and videos, and many firms are finding themselves in an arms race with these adversaries to counter the new attacks. The use of liveness detection technologies can help organizations determine if a biometric sample comes from a live person or a modified or generated representation, and has become a best practice when biometrics are being captured in a remote setting. Many of the best tools that are being used for liveness detection make use of AI themselves.

  Of note, liveness detection technologies broadly address two types of attacks on biometrics: "presentation attacks," which look to use a physical replica of a biometric such as a photo, mask, fake or fake fingerprint to trick a biometric system, and "injection attacks," which look to bypass the camera or biometric sensor completely to inject a fake image into the system. Of the two, it is injection attacks that are used in deepfake attacks – and thus liveness detection technology that can detect and block injection attacks is quickly becoming the more important of the two. The best injection attack solutions confirm three things simultaneously: the user is the right person (matching the ID), a real person (live, not a spoof), and submitting their photo or video right now (proving the authentication is not a replay or deepfake attack).

[13] See https://www.dhs.gov/science-and-technology/remote-identity-validation-rally
[14] See https://fidoalliance.org/fido-alliance-addresses-accuracy-bias-in-remote-biometric-identity-verification-technologies-industry-first-testing-certification-program/ and https://fidoalliance.org/certification/identity-verification/document-authenticity/

In addition to leveraging predictive tools used in identity proofing, firms have also started to leverage deterministic tools that tie back to authoritative identity sources, such as those run by government.

One example of a deterministic tool is the Social Security Administration's electronic Consent Based Social Security Number Verification (eCBSV) Service, which was launched after Congress directed SSA to do so in 2018; today, financial institutions use it to validate whether someone's name, date of birth, and SSN match the data that is on file in the SSA's systems. This has been a very helpful tool in the fight against synthetic identity fraud, as it is the first time SSA has offered this service through digital channels via an API. At present time, SSA is responding to more than 9 million queries each month. Beyond helping to stop identity fraud, eCBSV has proven to be a valuable tool to improve financial inclusion – in that many "thin file" applicants for credit who previously might have been flagged by predictive-based fraud engines as being potential synthetic fraudsters now have a clearer path to credit, based on SSA's validation that data submitted corresponds to a real identity. Our members report a 2-4% lift in new credit approvals thanks to eCBSV – proof that better identity solutions offer material benefits to consumers and industry beyond security.

mDLs (which we discussed in our answer to question 10) offer another exciting opportunity to tap into deterministic, authoritative sources of identity. Moreover the fact that they are built around asymmetric public key cryptography makes them one of the best emerging tools as we seek solutions that can stand up to emerging deepfake attacks.[15] Deepfakes may be able to spoof many biometric tools, but they cannot spoof possession of a private cryptographic key – and so a mDL that relies on public key cryptography can provide a tool for identity proofing/CIP purposes that is not only very secure and privacy-preserving, but also quite easy for consumers to use. As we noted earlier, we believe regulatory guidance on the use of mDLs would help to clear up regulatory ambiguities that are inhibiting the adoptions of these tools by financial institutions.

25. To the extent not already addressed here, are there other actions that would support stakeholders in identifying, preventing, and mitigating payments fraud?

As we noted earlier, the Better Identity Coalition has published a Policy Blueprint that outlines a comprehensive 22-point action plan for the U.S. government to take to improve the state of digital identity and authentication – in a way that will help to prevent payments

[15] We note that use of public key cryptography alone will not blunt every attack, in that ideally, an identity system will verify the correct individual person is actually in control of the device the credential is bound to; if a device falls into the wrong hands, some attacks are possible. The tools used to mitigate identity-related risks for a $500 transaction may differ from the tools used to protect a $500,000 transaction. The strongest verification and authentication solutions will pair cryptography for device and data authentication with biometrics for user authentication.

fraud, as well as many other related crimes including identity theft and identity-related cybercrime.

A core point we make in the Blueprint is that is the same organized criminals and hostile nation states exploiting the same core weaknesses in digital identity infrastructure to steal billions not just from government – but also banks, healthcare, retailers, fintech services, and cryptocurrency exchanges.

In other words, this is not just a "payments fraud problem," but rather, a national security problem – and thus needs to be addressed not just by Treasury and financial regulators, but with a whole-of-government approach.

Our members are heavily invested in state-of-the-art security tools and education campaigns to safeguard consumers and foster trust; however, more is needed. To address the immense complexity and scale of these criminal attacks, private industry alongside overnment and law enforcement must jointly prioritize fraud and scam prevention to recognize and avoid threats.

We greatly appreciate the willingness of FDIC, the FRS, and OCC 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.