

The Honorable Pete Sessions

Chairman
Subcommittee on Government Operations
Committee on Oversight and Government Reform
U.S. House of Representatives

The Honorable Kweisi Mfume

Ranking Member
Subcommittee on Government Operations
Committee on Oversight and Government Reform
U.S. House of Representatives

Dear Chairman Sessions and Ranking Member Mfume:

On behalf of the Better Identity Coalition—an organization of 18 financial services, health, technology, FinTech, payments, and security companies focused on working with policymakers to improve the way Americans establish, protect, and verify their identities when they're online—we appreciate your attention to emerging fraud threats and the evolving fraud landscape and write to highlight how mobile driver's licenses (mDLs) and other digital identity credentials can help combat fraud."

We appreciate the Subcommittee's continued attention to combating fraud and strengthening the security of government and private sector services. As fraud schemes become increasingly sophisticated—particularly through the use of artificial intelligence—we believe Congress has an opportunity to modernize America's digital identity infrastructure in ways that will significantly reduce fraud while enhancing privacy, security, and consumer convenience.

Identity has become one of the primary attack surfaces for organized criminal enterprises and hostile nation-state actors. Today's fraud is increasingly enabled not through technical exploits alone, but through the compromise or impersonation of legitimate identities. Artificial intelligence has dramatically accelerated this trend. Generative AI now enables criminals to produce convincing deepfake videos, voice clones, synthetic identities, and highly personalized phishing campaigns at minimal cost, enabling attacks that once required sophisticated capabilities to be launched at scale against financial institutions, government agencies, and individual Americans. As outlined in the Financial Services Sector Coordinating Council's (FSSCC) recent publication, *Mitigating AI-Powered Attacks Against Identity and Authentication*, the financial sector is already experiencing significant increases in AI-enabled identity attacks, with deepfake incidents increasing dramatically and fraud losses projected to continue rising unless stronger identity infrastructure is deployed.¹

The financial data underscore the magnitude of the challenge. In January 2024, the Financial Crimes Enforcement Network (FinCEN) analyzed identity-related Suspicious Activity Reports (SARs) and found that approximately 1.6 million SARs—representing 42 percent of all SARs filed in 2021—were tied to compromises of identity or authentication, involving approximately \$212 billion in

¹ <https://fsscc.org/wp-content/uploads/2026/02/AI-IA-Workstream-Mitigations.pdf>



suspicious transactions.² More recently, FinCEN issued an alert warning financial institutions that generative AI-powered deepfakes are creating entirely new fraud typologies and established a dedicated reporting code to improve tracking of these attacks. The data make clear that weaknesses in digital identity infrastructure are no longer simply a cybersecurity issue—they represent one of the largest fraud vectors affecting the U.S. economy.

One of the most promising tools available to address this challenge is the broader deployment of mDLs and other government-issued digital credentials. Unlike traditional remote identity verification methods that rely on scanned documents and biometric comparisons — which AI increasingly can defeat — properly implemented mDLs are built upon cryptographic foundations that enable relying parties to verify that credentials originated from an authoritative government issuer and have not been altered. Rather than asking organizations to determine whether an uploaded image appears authentic, digital credentials enable consumers to securely present verified identity attributes directly from the issuing authority, substantially reducing opportunities for fraud while improving user privacy through selective disclosure of only the information necessary for a transaction.

Remote identity proofing remains one of the weakest points in today's fraud ecosystem, and AI has only amplified these vulnerabilities. Government-issued digital credentials, combined with authoritative attribute validation services and phishing-resistant authentication technologies, provide a path toward dramatically reducing synthetic identity fraud, account takeovers, and deepfake-enabled impersonation attacks. The FSSCC likewise concludes that next-generation digital credentials should become foundational elements of America's strategy to defend against AI-enabled fraud. Accordingly, we respectfully encourage Congress to support policies that accelerate the deployment of secure digital identity infrastructure. These priorities include directing greater federal attention toward online use cases for mDLs. Together, these initiatives would significantly strengthen the nation's ability to combat identity fraud while improving security, privacy, interoperability, and consumer choice.

The U.S. has invested heavily in protecting physical identity credentials over many decades. Yet our economy increasingly depends on digital transactions, while much of our identity infrastructure remains rooted in paper and plastic credentials designed for in-person use. As artificial intelligence continues to reshape the fraud landscape, modernizing America's digital identity ecosystem is no longer simply a technology initiative—it is an economic security imperative. We appreciate the Subcommittee's leadership on fraud prevention and would welcome the opportunity to work with Congress to advance practical, privacy-protective solutions that strengthen trust in digital commerce and government services.

Thank you for your consideration.

Respectfully,

Jeremy Grant, Coordinator
Better Identity Coalition

² <https://www.centerforcybersecuritypolicy.org/insights-and-research/fincen-212-billion-in-likely-financial-crimes-linked-to-identity-verification-breakdowns>