Recommendations for Policymakers:

Mitigating AI-Powered Attacks Against Identity and Authentication

American Bankers Association®

BETTER IDENTITY COALITION

FSSCC

Table of Contents

Executive Summary

The emergence of generative artificial intelligence (Gen AI) has helped to supercharge the ability of attackers to fake likenesses and identities.[1] Attacks that were once resource-intensive and difficult to execute have now become commoditized — with cheap or free deepfake tools powered by GenAI now able to spoof video, images and voices. Paired with Gen AI-composed phishing emails, FIs and their customers are now seeing a new wave of attacks that are largely indistinguishable to human perception — and can also fool many automated security tools.

Deepfake incidents in the fintech sector increased by 700% in 2023 compared to the previous year.[2] In January 2024, the Financial Crimes Enforcement Network (FinCEN) issued a Financial Trend Analysis on information linked to identity-related suspicious activity in Bank Secrecy Act reports filed in 2021 and found that 1.6 million, which represents 42 percent of Suspicious Activity Reports (SARs) filed that year, were tied to a compromise of identity or authentication.[3] And Deloitte's Center for Financial Services

[1] Generative AI is defined as the class of AI that emulates the structure and characteristics of input data in order to generate derived synthetic content. This can include images, videos, audio, text, and other digital content.

[2] https://www.wsj.com/articles/deepfakes-are-coming-for-the-financial-sector-0c72d1e5

[3] https://www.fincen.gov/news/news-releases/fincen-issues-analysis-identity-related-suspicious-activity

predicts that Gen AI could enable fraud losses to reach $40 billion in the United States by 2027, up from $12.3 billion in 2023, representing a compound annual growth rate of 32%.[4]

A companion FSSCC white paper to this piece outlines the top threats to FIs and details the tools that they can use to try to mitigate these threats. However, FIs and their security partners are not able to address these threats alone; doing so will require assistance from and partnership with government. Government needs to play a role for these two reasons:

- First, identity and authentication are heavily regulated in the financial services sector, with rules governing how FIs verify the identity of new customers, as well as how they authenticate customers signing into their accounts online.[5] Some of these rules need to be updated — or in some cases, regulators need to clarify their intent — for FIs to feel comfortable in embracing newer tools such as passkeys or mobile driver's licenses (mDLs) that can thwart Gen AI-powered attacks.

- Second, government — through a mix of Federal, state, and local agencies — is the only authoritative issuer of identity credentials in the United States. While those credentials can be used by customers in-person at an FI, there is in most cases no digital counterpart to those paper and plastic credentials that are suited for the online world. At a time when many industry security tools that try to predict whether someone is who they claim to be are coming under attack from Gen AI, the need is greater than ever for government to help close the gap between physical and digital credentials.

This paper outlines 20 distinct actions for policymakers and regulators — spread across four key initiatives — that would collectively help FIs defend against current and emerging attacks powered by Gen AI that target FI identity and authentication systems. We also include a rationale for how each of these initiatives would help financial institutions defend against Gen AI-enabled attacks.

> **Initiative 1: Prioritize the development and deployment of next-generation remote identity proofing and verification systems.** Adversaries have caught up with many of the tools that financial institutions have relied on for remote identity proofing and verification. Government action can help spur the development, deployment, and use of next-generation solutions like mDLs and attribute validation services that are not only more resilient in the face of Gen AI-powered attacks, but also more convenient for consumers.

[4] https://www2.deloitte.com/us/en/insights/industry/financial-services/financial-services-industry-predictions/2024/deepfake-banking-fraud-risk-on-the-rise.html

[5] For identity verification, FIs are subject to the Bank Secrecy Act and Customer Identification Program (CIP) regulations. For authentication, FFIEC guidance on Authentication and Access to Financial Institution Services and Systems regulates the tools and methods that FIs use.

Initiative 2: Promote and prioritize the use of strong authentication. Passwords and some legacy forms of multifactor authentication (MFA) have become easy to phish, and the introduction of AI-powered tools is enabling adversaries to launch new, more sophisticated attacks on authentication, more cheaply and at scale. Regulators and policymakers can encourage FIs to adopt phishing-resistant authentication and make it easier to use risk-based tools that can leverage data and AI to prevent fraud by detecting deepfake attacks.

Initiative 3: Coordinate with other countries and harmonize requirements. Consumers and businesses operate in environments beyond American borders, and other countries are also contemplating innovative approaches to making identity better and battling the threats of Gen AI. The U.S. should look for ways to coordinate with other countries and harmonize requirements, standards, or frameworks where feasible and compatible with American values.

Initiative 4: Educate consumers and businesses about better identity and emerging identity threats. Americans must be aware of new identity solutions and how to best use them. The government should partner with industry to educate both consumers and businesses, with an eye toward promoting best practices.

While FIs will remain the first line of defense, federal and state governments have a material role to play in helping protect FIs and their customers against Gen-AI-powered attacks. These recommendations — if enacted and funded — will position the American FIs to address security challenges and enable trusted digital financial services in a way that enhances security, privacy, convenience and innovation.

Purpose

The purpose of this paper is to highlight the role that policymakers can play in helping financial institutions (FIs) defend against current and emerging attacks powered by Generative Artificial Intelligence (Gen AI) that target FI identity and authentication systems. This paper is a deliverable of the Financial Services Sector Coordinating Council's Artificial Intelligence and Identity and Authentication Workstream (AI-IA). [6]

Artificial intelligence is the predominant term used to describe technologies that can learn, analyze and predict based on data. Gen AI extends this capability and generates new content based on that information. In the context of digital identity, Gen AI — by enabling more sophisticated deepfakes and phishing emails — poses the core threat, not just to FIs, but to the safety and soundness of our financial system.

A complementary paper in this series outlines 10 current and emerging attacks against identity and authentication systems from Gen AI powered attacks, along with recommended mitigation strategies. However, FIs might not be able to address the full range of these risks, as various aspects of threat mitigation will require government action — including changes to policy — to effectively detect and block Gen-AI-enabled attacks.

Audience

This paper is intended for policymakers at agencies — both regulatory and non-regulatory — and in legislative bodies who play a role in safeguarding the financial services sector and other critical infrastructure sectors from the risks posed by Gen AI.

[6] The FSSCC is an industry-led, non-profit organization that coordinates critical infrastructure and homeland security activities within the financial services industry. Their members consist of financial trade associations, financial utilities, and the most critical financial firms. https://fsscc.org/

Overview

The rise of Gen AI-powered attacks against U.S. digital identity systems is laying bare the deficiencies of America's existing digital identity and authentication infrastructure. Gen AI has enabled adversaries to launch cheaper, more convincing phishing and deepfake attacks targeting financial services firms and their customers. New waves of attacks from both organized criminals and hostile nations, like China and North Korea, exploit weaknesses in current digital identity and authentication solutions that financial services firms depend on to fulfill both identity proofing requirements tied to the Bank Secrecy Act, and fraud-fighting and authentication requirements needed to securely control access for employees, customers and third parties.

Gen AI is being used today in a variety of ways to undermine FI digital identity systems. Common attacks include:

1. Deepfake Attacks on Identity Verification
2. Social Engineering Using Deepfakes Against a Financial Services Call Center
3. Use of Generative AI to Compose Realistic Phishing Campaigns for Credential Compromise
4. Deepfakes for Job Interviews and Applications
5. Social Engineering to Exploit Vulnerabilities Using Deepfakes Against a Company/Individual
6. Deepfakes Used Against Authentication
7. Using Gen AI to Create Holistic, Synthetic Identities
8. Cross-Channel Deepfake Attacks
9. Real-Time Deepfake Fraud
10. Using AI Agents for Account Takeovers

The risk of these attacks to FIs is immense. Employees and customers need to be vigilant when reviewing emails, as 60% of people have fallen victim to AI-automated phishing.[7] While the percentage of successful attacks is, to date, on par with other phishing attempts, AI enables fraudsters to conduct these attacks at scale, faster and cheaper. The entire phishing process can be automated using Large Language Models (LLMs), which

[7] https://hbr.org/2024/05/ai-will-increase-the-quantity-and-quality-of-phishing-scams

reduce the costs of phishing attacks by more than 95% while achieving equal or greater success rates.[8]

While phishing poses a consistent threat, deepfake attacks are also rising in prominence. Deepfake incidents in the fintech sector increased by 700% in 2023 compared to the previous year.[9] Deloitte's Center for Financial Services predicts that Gen AI could enable fraud losses to reach $40 billion in the United States by 2027, up from $12.3 billion in 2023, representing a compound annual growth rate of 32%.[10]

These attacks are enabled by weaknesses in America's digital identity and authentication infrastructure, which is becoming increasingly easy for adversaries to exploit. In simple terms, adversaries have caught up with the legacy tools FIs use to secure identity and authentication, and the emergence of Gen AI has enabled adversaries to increase the sophistication and scale of their attacks. Adding to that complexity is the emergence of AI agents, which will seek to conduct financial transactions on behalf of customers posing a new array of challenges and threats to FIs. The longer the delay in addressing these weaknesses and challenges, the greater the possibility that problems will fester, and fraud and cybercrime losses will mount. There is also the risk that the solutions to mitigate threats will fall short when it comes to privacy, security, civil liberties, accessibility and interoperability.

A strategic plan is needed to address core deficiencies in America's digital identity infrastructure — in a way that not only enhances security, but also focuses on privacy, civil liberties, accessibility and interoperability.

States have already started to invest in mobile driver license (mDL) technology, which could be one solution to help FIs better ascertain the identity of a customer transacting over an open network. As noted in the companion to this paper, mDLs are rooted in asymmetric public key cryptography, which can stand up to most Gen-AI-powered deepfake attacks, since a deepfake cannot spoof possession of a private cryptographic key.[11] However, the online use cases for mDL technology are nascent and need more attention and investment from the government, along with the enabling technologies for them to be used online. Likewise, the government providing more tools and resources to encourage greater issuance and use of mDLs and other emerging digital identity tools

[8] https://hbr.org/2024/05/ai-will-increase-the-quantity-and-quality-of-phishing-scams

[9] https://www.wsj.com/articles/deepfakes-are-coming-for-the-financial-sector-0c72d1e5

[10] https://www2.deloitte.com/us/en/insights/industry/financial-services/financial-services-industry-predictions/2024/deepfake-banking-fraud-risk-on-the-rise.html

[11] Note that mDLs – like all solutions that use asymmetric public key cryptography – will have to migrate to using new NIST-approved quantum-resistant algorithms in the years to come to address threats that are likely to emerge from quantum computers that will be able to break many legacy algorithms. However, concerns about future threats from quantum computing should not deter organizations from using cryptography-based solutions that can stop deepfake attacks today.

would help accelerate deployment and use more robust digital identity technologies that can stand up to the threats posed by Gen-AI-powered attacks.

Beyond mDLs, the Federal government today has started to make available identity attribute validation services, such as the Social Security Administration's Electronic Consent-based Social Security Number Verification System (eCBSV)[12], which has helped to reduce synthetic identity fraud and improve financial inclusion. But there is a need for similar systems in other agencies and for eCBSV to be improved. And as agentic AI applications start to emerge in financial services, FIs face myriad new challenges in addressing identity, authentication and authorization requirements associated with agents — raising a new set of policy, regulatory and standards issues that government will need to play a role in addressing.

While this paper outlines actions that policymakers should consider, there are no "moonshot" items in this paper. This is by design; history has shown that lofty identity initiatives that aim to solve every problem struggle to get traction, given their complexity and difficulty. Instead, this paper outlines a set of proposals that are both significant in impact and achievable — should government choose to act on them — in the next two to three years.

A Path to Better Identity

Below, we outline 20 distinct actions for policymakers — spread across four key initiatives — that would collectively help FIs defend against current and emerging attacks powered by Generative Artificial Intelligence (Gen AI) that target FI identity and authentication systems. We also include a rationale for how each of these initiatives would help financial institutions defend against Gen AI-enabled attacks.

Initiative 1: Prioritize the development and deployment of next-generation remote identity proofing and verification systems. Adversaries have caught up with many of the tools that financial institutions have relied on for remote identity proofing and verification. Government action can help spur the development, deployment and use of next-generation solutions that are not only more resilient but also more convenient for consumers.	
Action	Rationale
1. Establish a Treasury Department-led task force charged with bringing federal, state and local agencies together to develop a coordinated plan to close the	While federal, state and local agencies all issue nationally recognized, authoritative credentials — such as passports, driver's licenses and birth certificates — that can be used to prove identity in person, agencies have never created digital counterparts that can be used to prove

[12] https://www.ssa.gov/dataexchange/eCBSV/

gap between physical and digital credentials in a way that promotes security, privacy, equity and interoperability, and can drive the adoption of more resilient digital identity solutions across the financial services market that can help mitigate the threats of deepfake attacks.	identity when needed in the online world. The emergence of new verifiable digital credentials like mDLs, protected by public key cryptography, offers a promising way to close the gap between physical and digital credentials while also blocking deepfake attacks that are being used to successfully spoof identities. However, without a national strategy to ensure new digital credentials set a high bar for security and privacy — and work for all people — the U.S. is likely to fall short of these goals. Given the threats to the financial services sector from deepfakes, Treasury is the agency best suited to coordinate these efforts.
2. Direct the National Institute of Standards and Technology (NIST) and the U.S. Department of Homeland Security (DHS) to jointly accelerate the development of standards and guidance to enable states to launch remote identity proofing applications for mDLs and other digital credentials, as well as prioritize online use cases over in-person use cases in its work on mDLs.	Mobile driver licenses (mDLs) and other digital credentials rooted in public key cryptography can stand up to Gen AI attacks; however, FIs lack guidance and best practices on standardized ways they can use these credentials to help disrupt and defeat deepfake attacks on identity verification systems. Most government work on mDLs has focused on the in-person use cases of the technology, led by DHS. The threat from deepfakes, however, is unique to online use cases, which is more in the wheelhouse of NIST's cybersecurity division. A joint effort to prioritize standards and guidance around these online use cases — building off the work NIST is already leading on digital credentials in its National Cybersecurity Center of Excellence (NCCoE) — will help to speed more robust solutions to market.
3. Open up the Social Security Administration's (SSA) electronic Consent Based Social Security Number Verification (eCBSV) system, which is currently limited only	Attribute validation services like eCBSV enable FIs to validate identities against an authoritative government source and block attempts by adversaries to create and use synthetic identities. eCBSV is currently available to FIs for a limited subset of use

to a subset of credit-related financial services, to cover account opening use cases for government services, demand deposit accounts, background checks, and other use cases where a person might need to ask SSA to “vouch” for them by validating the information SSA has on them in SSA databases.	cases requiring identity validation, but it is not accessible to other applications that also need to validate identities. Opening this service to other use cases and sectors will help prevent the use of synthetic identities and provide FIs and others with a deterministic answer as to whether an identity exists. Additionally, increasing the number of transactions run through eCBSV will address longstanding cost challenges with the service identified in a 2024 GAO report[13] by enabling SSA to spread the operating costs across a wider array of transactions and users.
4. Address fundamental challenges tied to eCBSV’s current pricing model and data reporting structure that are discouraging financial services firms from using eCBSV more fully to reduce synthetic identity fraud.	Addressing these challenges (which were identified by GAO) will enable greater use of eCBSV and ensure that more FIs are using eCBSV to spot synthetic identities.
5. Support states with grants to accelerate the modernization of legacy identity infrastructure to support digital solutions. Tie Federal grant dollars to adherence to forthcoming NIST guidance for federal, state, and local agencies for creating new identity and attribute validation services.	mDLs and other digital credentials rooted in public key cryptography can stand up to Gen AI attacks, but only a handful of states have progressed down this path, and others lack the resources to move forward due to unaddressed funding needs.[14] A grant program would help states accelerate progress here. Tying the grant dollars to NIST guidance will ensure the credentials that states offer will set

[13] See GAO-24-106770: “Social Security Administration: Actions Needed to Help Ensure Success of Electronic Verification Service” at https://www.gao.gov/products/gao-24-106770

[14] This number is based on an analysis in https://www.betteridentity.org/s/Better_Identity_CoalitionBlueprint-July2018.pdf documenting that there is $2.5-3 billion in unaddressed funding needs across U.S. DMVs to support their transition to becoming digital identity providers. While the Federal government should not bear this full cost, states are unlikely to launch these modernizations without seed funding – and the security benefits of secure digital IDs merit a Federal investment to catalyze state activity.

	a high bar for security and privacy and ensure interoperability across states.
6. Establish additional consent-based attribute validation services at other agencies that hold authoritative identity data on Americans, such as the Internal Revenue Service, State Department and U.S. Postal Service (USPS).	Creating consent-based systems that enable Americans to ask the government to “vouch for them” when they need to prove their identity online will enable FIs to leverage authoritative government sources in a privacy-preserving way to detect synthetic identity fraud and block Gen-AI-powered attacks.
7. Direct the State Department to offer Americans the option of getting a digital counterpart to their paper passport, which can be stored securely in their smartphone like mDLs; ensure the State Department prioritizes the use of digital passports for online use cases rather than in-person ones.	Like mDLs, digital passports could serve as authoritative sources of truth for online transactions. Digital passports rooted in public key cryptography will offer American FIs and their customers another tool they can use to prove their identity more easily for online account opening and protect themselves from Gen-AI-powered attacks.
8. Authorize the USPS to offer in-person identity verification and related services for government agencies and the private sector.	Most Americans live within 10 miles of a post office, and the USPS already offers identity proofing services today for passport applicants and Login.gov. For consumers who are unable to easily prove their identity online, post offices provide a logical fallback option. This would also be an important service for digital-only financial institutions without a physical branch.
9. Direct financial regulators to issue guidance on how mDLs and other government digital credentials can be used by banks in their KYC/CIP process.	Additional clarity is needed from the prudential regulators on the use of mDLs and other emerging digital credentials as to how FIs can make use of them to meet Customer Identification Program (CIP) requirements.
10. Create a new NIST publication in the next 12 months detailing which biometric algorithms NIST testing has demonstrated to meet a high threshold for accuracy, and which work well	Face verification has become a primary way to conduct remote identity verification, and algorithms that work accurately and reliably across all demographic groups are necessary to ensure the technology works properly and is trusted by consumers.

across all demographic groups; direct agencies to use only those algorithms in identity solutions.	
11. Accelerate work at NIST to develop more robust guidance and criteria for liveness detection technology in biometrics, with an eye toward helping defenders stay ahead of emerging attacks such as those powered by deepfakes.	Liveness detection technology is a primary tool to detect and block deepfake attacks. However, the government's work on liveness has focused largely on "'presentation attacks" (such as the use of photos or masks to defeat biometrics), which are now outdated in the wake of the emergence of deepfake tools powered by "injection attacks" (which bypass cameras and other biometric sensors) to deliver cheaper and more convincing attacks. Additional research and guidance will help FIs, and their partners stay ahead of the attackers.
12. Develop a new, forward-looking investment strategy for R&D and standards work in identity that: 1) Focuses on addressing current and emerging threats tied to Gen AI, as well as threats and challenges associated with the use of AI agents 2) Ensures alignment in priorities across agencies, with a focus on addressing security, privacy, interoperability and equity; and 3) Ensures that the necessary work around identity is adequately funded.	Attackers continue to innovate as quickly as the defenders adapt, and the emergence of Gen AI and AI agents is introducing new challenges. An R&D strategy to help stay ahead of the attackers is needed.
13. Create a multi-agency task force to monitor and combat	Attackers are adapting to new defensive measures quickly. Relevant agencies need to

emerging, scalable threats to identity systems from deep fakes and other AI-generated attacks.	be brought together to stay up to date on the latest attacks so they can also plan mitigations.
14. Direct FinCEN to build off its initial 2024 assessment of identity-related SARs,[15] by publishing an annual report that details the percentage and dollar volume of SARs tied to compromises of identity.	By defining the size and scope of the problem — and breaking down different attack vectors used in identity-related financial crime — FinCEN has provided a valuable tool to ensure that industry and government now have a common understanding of the issues at play. Turning this assessment into an annual report would ensure that policymakers have up-to-date data to make decisions.

<table>
<tr><td colspan="2"><b>Initiative 2: Promote and prioritize the use of strong authentication.</b> Passwords are not sufficient to secure online accounts. Various forms of multifactor authentication (MFA) — Short Message Service (SMS), one-time passcodes and push-based authenticator apps — have become easy to phish, and the introduction of AI-powered tools is enabling adversaries to launch new, more sophisticated attacks on authentication, more cheaply and at scale. With phishing attacks on the rise, FIs and other organizations need to focus on implementing phishing-resistant authentication and moving away from weaker forms of MFA and other easily compromised authenticators, such as passwords and other “shared secrets.”</td></tr>
<tr><td>Initiative</td><td>Rationale</td></tr>
<tr><td>1. Strongly encourage FIs to use only phishing-resistant authentication — such as FIDO security keys and passkeys — in enterprise applications and offer that same technology for all public-facing applications.[16]</td><td>Deepfake-powered phishing attacks fail if accounts are protected by authentication tools that use public key cryptography, as there are no credentials that can be shared or phished.</td></tr>
<tr><td>2. Avoid creating new restrictions that might preclude the use of promising technologies like data analytics for risk-</td><td>Layering various risk-based technologies that pull data from various sources is a critical tool in</td></tr>
</table>

[15] https://www.fincen.gov/sites/default/files/shared/FTA_Identity_Final508.pdf

[16] NIST has defined phishing-resistance in Section 3.2.5 of NIST SP 800-63B-4 at https://pages.nist.gov/800-63-4/sp800-63b.html#verifimpers

based authentication that can help security and prevent fraud, such as by detecting AI-powered deepfake attacks. Continue to promote CISA’s “More than a Password” campaign, which helps educate the private sector on best practices for MFA and the importance of phishing-resistant MFA.	defeating attacks against authentication. Restricting how these data analysis tools can be used for detecting fraud will give attackers an advantage.

Initiative 3: Coordinate with other countries and seek to harmonize requirements. Consumers and businesses operate in environments beyond American borders, and other countries are also contemplating innovative approaches to making identity better and battling the threats of Gen AI. The U.S. should look for ways to coordinate with other countries and harmonize requirements, standards, or frameworks where feasible and compatible with American values.	
Initiative	Rationale
1. As the European Union and other countries move forward with digital wallet initiatives, NIST, DHS and Treasury should actively engage with their government counterparts to identify opportunities for collaboration and interoperability, and share lessons learned and best practices.	Digital wallets — and the credentials held within — combined with phishing-resistant authentication will be key to fighting deepfake attacks. Collaborating with the EU and other partners will help ensure that innovative solutions are interoperable across borders and provide additional resources to enable more resilient solutions.
2. Engage in broader standards work — NIST and DHS are engaged in international digital identity standards bodies, but presence is limited in part by budget and resource constraints. Properly funding these efforts would enable the U.S. to take a larger leadership role alongside peer countries on the global standards stage,	China and other adversaries are increasingly leveraging standards bodies to undermine U.S. security interests, including in bodies that work on digital identity and authentication. As new standards initiatives launch around topics such as deepfakes and identity, authentication, and authorization

ensuring that new standards reflect American priorities and values.	issues tied to use of AI agents, American interests need to be well-represented.

<table>
<tr><td colspan="2"><b>Initiative 4: Educate consumers and businesses about better identity and emerging identity threats.</b> As part of improving the identity ecosystem, Americans must be aware of new identity solutions and how to best use them. They also need to be aware of emerging threats and how to counter them. The U.S. government should partner with industry to educate both consumers and businesses, with an eye toward promoting best practices.</td></tr>
<tr><td>Initiative</td><td>Rationale</td></tr>
<tr><td>1. Treasury should collaborate with CISA and FIs to create a campaign to educate the public about the threats of deepfakes and how to counter them.</td><td>As new threats emerge, it will be important to educate businesses and individuals about best practices in detecting and defending against Gen-AI-powered deepfake threats.</td></tr>
<tr><td>2. Create a public awareness campaign around the use of phishing-resistant authentication.</td><td>As phishing campaigns become more convincing, it will be important to encourage the public to adopt phishing-resistant authentication technologies such as passkeys.</td></tr>
</table>

Conclusion

As organized criminal enterprises and nation state adversaries intensify their attacks on identity systems, and AI-powered deepfakes become more readily available, digital identity and authentication must become a top-tier priority.

While FIs will remain the first line of defense, federal and state governments have a material role to play in helping protect FIs and their customers against Gen-AI-powered attacks. These recommendations — if enacted and funded — will position the U.S. to address security challenges and enable trusted digital financial services in a way that enhances security, privacy, convenience and innovation.