FinCEN ALERT

FIN-2024-Alert004

November 13, 2024

FinCEN Alert on Fraud Schemes Involving Deepfake Media Targeting Financial Institutions

Suspicious Activity Report (SAR) Filing Request:

FinCEN requests that financial institutions reference this alert in SAR field 2 (Filing Institution Note to FinCEN) and the narrative by including the key term **"FIN-2024-DEEPFAKEFRAUD"**.

The U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) is issuing this alert to help financial institutions[1] identify fraud schemes associated with the use of deepfake media[2] created with generative artificial intelligence (GenAI) tools.[3] This alert explains typologies associated with these schemes, provides red flag indicators to assist with identifying and reporting related suspicious activity, and reminds financial institutions of their reporting requirements under the Bank Secrecy Act (BSA). This alert is also part of the U.S. Department of the Treasury's broader effort to provide financial institutions with information on the opportunities and challenges that may arise from the use of AI.[4]

Beginning in 2023 and continuing in 2024, FinCEN has observed an increase in suspicious activity reporting by financial institutions describing the suspected use of deepfake media in fraud schemes targeting their institutions and customers. These schemes often involve criminals altering or creating fraudulent identity documents to circumvent identity verification and authentication methods.[5] The potential for deepfake media to be used in fraud schemes is one of several risks associated with

[1] *See* 31 U.S.C. § 5312(a)(2); 31 CFR § 1010.100(t).

[2] Deepfake media, or "deepfakes," are a type of synthetic content that use artificial intelligence/machine learning to create realistic but inauthentic videos, pictures, audio, and text. *See* Department of Homeland Security (DHS), "Increasing Threat of Deepfake Identities" ("DHS report"). As noted further by DHS, the threat of deepfakes and synthetic media comes not from the technology used to create it, but from people's natural inclination to believe what they see, and as a result, deepfakes and synthetic media do not need to be particularly advanced or believable to be effective in spreading misinformation or disinformation.

[3] Artificial intelligence is a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. The term "generative AI" means the class of AI models that emulate 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. *See* White House, Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, (Oct. 30, 2023) ("E.O. 14110").

[4] U.S. Department of the Treasury (Treasury), Treasury and Artificial Intelligence.

[5] Identity-related exploitations are a major cybercrime and fraud concern for financial institutions. FinCEN created and published an Identity Financial Trend Analysis in January 2024 that outlines a framework for considering exploitations of various identity processes at account opening, account access, and during transactions. *See* FinCEN, "Financial Trend Analysis: Identity-Related Suspicious Activity: 2021 Threats and Trends," (Jan. 9, 2024).

emerging GenAI technologies that financial institutions and their customers may face.[6] Further, the abuse of deepfake and GenAI media contribute to fraud and cybercrime, which are two of FinCEN's Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) National Priorities.[7]

The information contained in this alert is derived from FinCEN's analysis of BSA data, open-source reporting, and information from law enforcement and interagency partners.

Recent Developments in Publicly Available GenAI Tools

GenAI tools have greatly reduced the resources required to produce high-quality synthetic content, meaning media that has either been created through digital or artificial means or media that has been modified or otherwise manipulated through technology, whether analog or digital.[8] In many cases, GenAI can now produce synthetic content that is difficult to distinguish from unmodified or human-generated outputs. GenAI-rendered content that is highly realistic is commonly referred to as "deepfake" content, or "deepfakes." Deepfakes can manufacture what appear to be real events, such as a person doing or saying something they did not actually do or say.[9]

Leading developers and companies producing GenAI tools have committed to implementing oversight and controls intended to mitigate malicious deepfakes and other misuse.[10] Criminals, however, may develop methods to evade these safeguards. In addition, some AI tools are open-source, allowing any user to access and modify the tools' code and potentially circumvent controls.

Creation and Use of Deepfake Fraudulent Identities

Criminals use new and rapidly evolving technologies, like GenAI, to lower the cost, time, and resources needed to exploit financial institutions' identity verification processes. FinCEN's analysis of BSA data indicates that criminals have used GenAI to create falsified documents, photographs, and videos to circumvent financial institutions' customer identification and verification[11] and customer

[6] In response to E.O. 14110, Treasury published a report in March 2024 which focuses on the current state of AI-related cybersecurity and fraud risks in financial services, including an overview of current AI use cases, trends of threats and risks, best-practice recommendations, and challenges and opportunities. *See* Treasury, "Managing Artificial Intelligence-Specific Risks in the Financial Services Sector," (Mar. 2024).

[7] FinCEN, "Anti-Money Laundering and Countering the Financing of Terrorism National Priorities," (Jun. 30, 2021).

[8] DHS report, *supra* note 2, at p. 5.

[9] *See* DHS report, *supra* note 2. *See also* National Security Agency (NSA), Federal Bureau of Investigation (FBI), and Cybersecurity and Infrastructure Agency (CISA) Cybersecurity Information Sheet, "Contextualizing Deepfake Threats to Organizations," (Sept. 2023), ("Interagency Cybersecurity Information Sheet"), at p. 2.

[10] *See, e.g.*, White House, "FACT SHEET: Biden-Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI," (Jul. 21, 2023). *See also* Interagency Cybersecurity Information Sheet, *supra* note 9, at pp. 6–7.

[11] As part of their customer identity verification procedures under the Customer Identification Program (CIP) Rule, financial institutions may collect an unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as a driver's license or passport. *See, e.g.*, 31 CFR § 1020.220 (CIP requirements for banks). Under the BSA and FinCEN's regulations, the term "bank" includes each agent, agency, branch, or office within the United States of a bank, savings association, credit union, or foreign bank. 31 CFR § 1010.100(d).

due diligence (CDD) controls.[12] For example, some financial institutions have reported that criminals employed GenAI to alter or generate images used for identification documents, such as driver's licenses or passport cards and books.[13] Criminals can create these deepfake images by modifying an authentic source image or creating a synthetic image. Criminals have also combined GenAI images with stolen personal identifiable information (PII) or entirely fake PII to create synthetic identities.[14]

FinCEN analysis of BSA data also shows that malicious actors have successfully opened accounts using fraudulent identities suspected to have been produced with GenAI and used those accounts to receive and launder the proceeds of other fraud schemes. These fraud schemes include online scams and consumer fraud such as check fraud, credit card fraud, authorized push payment fraud,[15] loan fraud,[16] or unemployment fraud.[17] Criminals have also opened fraudulent accounts using GenAI-created identity documents and used them as funnel accounts, according to BSA reporting.[18]

Detecting and Mitigating Deepfake Identity Documents

FinCEN's analysis of BSA data indicates that financial institutions often detect GenAI and synthetic content in identity documents by conducting re-reviews of a customer's account opening documents. When investigating a suspected deepfake image, reverse image searches and other open-source research may reveal that an identity photo matches an image in an online gallery of faces created with

[12] Financial institutions' compliance obligations under the BSA vary depending on financial institution type. For example, pursuant to 31 CFR § 1020.210(a)(2)(v), banks must implement appropriate risk-based procedures for conducting ongoing customer due diligence that, among other things, enable banks to (i) understand the nature and purpose of customer relationships for the purpose of developing a customer risk profile, and (ii) conduct ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information. Board of Governors of the Federal Reserve System (FRB), Federal Deposit Insurance Corporation (FDIC), FinCEN, National Credit Union Administration, Office of the Comptroller of the Currency (OCC), "Joint Statement on the Risk-Based Approach to Assessing Customer Relationships and Conducting Customer Due Diligence," (July 6, 2022).

[13] For additional information on the use of counterfeit U.S. passport cards, *see* FinCEN, "FinCEN Notice on the Use of Counterfeit U.S. Passport Cards to Perpetrate Identity Theft and Fraud Schemes at Financial Institutions," (Apr. 15, 2024).

[14] "Synthetic identity" refers to the use of a combination of real and fake PII to fabricate a person or entity to pass validation processes. FinCEN, *supra* note 5, at p. 6.

[15] Authorized push payment fraud occurs when a customer is misled into authorizing a payment to a criminal. These fraud schemes are also known as "credit-push scams." Federal Reserve Bank of Atlanta, "The Cold Reality of Authorized Push-Payment Fraud," (Jan. 29, 2024). *See also* Federal Reserve Bank of Atlanta, "Curtailing Authorized Push Payment Fraud Means Curtailing Phone Scammers," (Mar. 4, 2024).

[16] *See* FinCEN, "Suspicious Activity Related to Mortgage Loan Fraud," (Aug. 16, 2012).

[17] For additional information on fraud schemes, *see also* FinCEN, "FinCEN Alert on COVID-19 Employee Retention Credit Fraud," (Nov. 22, 2023); FinCEN, "FinCEN Alert on Prevalent Virtual Currency Investment Scam Commonly Known as "Pig Butchering"," (Sep. 8, 2023); FinCEN, "FinCEN Alert on Nationwide Surge in Mail Theft-Related Check Fraud Schemes Targeting the U.S. Mail," (Feb. 27, 2023); FinCEN, "Advisory on Imposter Scams and Money Mule Schemes Related to Coronavirus Disease 2019 (COVID-19)," (July 7, 2020); and FinCEN, "FinCEN Alerts Financial Institutions to Convertible Virtual Currency Scam Involving Twitter," (July 16, 2020).

[18] Funnel accounts are bank accounts used to collect deposits from various locations. Multiple individuals deposit cash in a bank account available to other members of the criminal network in another part of the country. Criminal actors use funnel accounts to assist in structuring transactions to circumvent Currency Transaction Report (CTR) thresholds and other BSA obligations to facilitate money laundering. Treasury, "2024 National Money Laundering Risk Assessment," (Feb. 2024), p. 47.

GenAI. Financial institutions and third-party providers[19] of identity verification solutions may also use more technically sophisticated techniques to identify potential deepfakes, such as examining an image's metadata or using software designed to detect possible deepfakes or specific manipulations.[20] While not conclusive of inauthentic documents, indicators that additional scrutiny might be warranted include the following:

- Inconsistencies among multiple identity documents submitted by the customer;
- A customer's inability to satisfactorily authenticate their identity, source of income, or another aspect of their profile; and
- Inconsistencies between the identity document and other aspects of the customer's profile.

Beyond account opening, financial institutions detected deepfake identity documents through enhanced due diligence on accounts that exhibited separate indicators of suspicious activity. While not dispositive of suspicious activity, indicators warranting further due diligence may include the following:

- Access to an account from an IP address that is inconsistent with the customer's profile;
- Patterns of apparent coordinated activity among multiple similar accounts;
- High payment volumes to potentially higher-risk payees, such as gambling websites or digital asset exchanges;
- High volumes of chargebacks or rejected payments;
- Patterns of rapid transactions by a newly opened account or an account with little prior transaction history; and
- Patterns of withdrawing funds immediately after deposit and in manners that make payments difficult to reverse in cases of suspected fraud, such as through international bank transfers or payments to offshore digital asset exchanges and gambling sites.

FinCEN has identified certain best practices that may help financial institutions reduce their vulnerability to deepfake identity documents. For example, multifactor authentication (MFA),[21] including phishing-resistant MFA,[22] and live verification checks in which a customer is prompted to confirm their identity through audio or video, are two such processes. Although illicit actors may be able to respond to live verification prompts or access tools that generate synthetic audio and video responses on their behalf, their responses may reveal inconsistencies in the deepfake identity.[23] Consequently, malign actors using deepfake identities may attempt to avoid or circumvent live verification checks. For example, a criminal actor attempting to open an account with a GenAI-produced identity document may claim to be experiencing repeated technical glitches or request to

[19] Financial institutions that use third-party services should develop and implement risk-management practices for all stages in the life cycle of any such third-party relationships. *See* FDIC, FRB, OCC, 88 Fed. Reg. 37920, "Interagency Guidance on Third-Party Relationships: Risk Management," (June 6, 2023). Additionally, DHS's Remote Identity Validation Technology Demonstration is conducting independent testing of onboarding solutions' ability to detect fake documents, match selfies, and test for liveness. DHS, "Remote Identity Validation Technology Demonstration."

[20] Interagency Cybersecurity Information Sheet, s*upra* note 9, at p. 12.

[21] Multifactor authentication means that users are required to authenticate their identity using two or more factors (e.g. a password and a text message) rather than just a password. CISA, "More than a Password."

[22] *See* CISA, "Implementing Phishing-Resistant MFA," (Oct. 2022).

[23] Interagency Cybersecurity Information Sheet, *supra* note 9, at p. 11.

change communication methods during a verification check. Some identity verification solutions may also flag possible attempts to circumvent verification checks, such as the use of third-party webcam plugins, which can let a customer display previously generated video rather than live video.

Use of Deepfake Media in Phishing Attacks and Scams

Criminals may also target financial institution customers and employees through sophisticated, GenAI-enabled social engineering attempts in support of other scams and fraud typologies, such as business email compromise (BEC) schemes, spear phishing attacks, elder financial exploitation, romance scams, and virtual currency investment scams.[24] For example, in family emergency schemes, scammers may use deepfake voices or videos to impersonate a victim's family member, friend, or other trusted individual.[25] Similarly, criminals have reportedly used GenAI tools to target companies by impersonating an executive or other trusted employee and then instructing victims to transfer large sums or make payments to accounts ultimately under the scammer's control.[26]

Financial Red Flag Indicators of Deepfake Media Abuse

FinCEN identified the following red flag indicators to help financial institutions detect, prevent, and report potential suspicious activity related to the use of GenAI tools for illicit purposes. As no single red flag is necessarily indicative of illicit or suspicious activity, financial institutions should consider the surrounding facts and circumstances before determining whether a specific transaction is suspicious or associated with illicit use of GenAI tools.

1 A customer's photo is internally inconsistent (e.g., shows visual tells of being altered) or is inconsistent with their other identifying information (e.g., a customer's date of birth indicates that they are much older or younger than the photo would suggest).

2 A customer presents multiple identity documents that are inconsistent with each other.

[24] In BEC schemes, criminals use compromised or spoofed accounts, often those actually or purportedly belonging to company leadership, vendors, or lawyers, to target employees with access to a company's finances to induce them to transfer funds to bank accounts thought to belong to trusted partners. Treasury, *supra* note 18, at p. 17. Methods such as spear phishing enable BEC perpetrators and other identity processes vulnerable to compromise. *See* FinCEN, "Financial Trend Analysis: Business Email Compromise in the Real Estate Sector: Threat Pattern and Trend information" (Mar. 30, 2023); FinCEN, "Updated Advisory on Email Compromise Fraud Schemes Targeting Vulnerable Business Processes," (July 16, 2019); *see also* Interagency Cybersecurity Information Sheet, *supra* note 9, at p. 8; FinCEN, "Advisory on Elder Financial Exploitation," ("FinCEN EFE Advisory") (June 15, 2022) at p. 6; FinCEN, "FinCEN Alert on Prevalent Virtual Currency Investment Scam Commonly Known as "Pig Butchering"," (Sept. 8, 2023).

[25] *See* U.S. Securities and Exchange Commission, Artificial Intelligence (AI) and Investment Fraud: Investor Alert (Jan. 25, 2024) and Federal Trade Commission, Scammers use AI to enhance their family emergency schemes | Consumer Advice, (March 20, 2023). *See also* FinCEN EFE Advisory, *supra* note 24. Scammers perpetrating this scheme are known to target elder individuals.

[26] *See* DHS, "Increasing Threat of Deepfake Identities," at p. 20 and NSA, FBI, CISA, "Contextualizing Deepfake Threats to Organizations," at p. 9. *See also* Treasury, "Managing Artificial Intelligence-Specific Risks in the Financial Services Sector," (Mar. 2024), at p. 18; CNN, "Finance worker pays out $25 million after video call with deepfake 'chief financial officer'" (Feb. 2024); CNBC, "Deepfake scams have robbed companies of millions. Experts warn it could get worse," (May 27, 2024).

3. A customer uses a third-party webcam plugin during a live verification check. Alternatively, a customer attempts to change communication methods during a live verification check due to excessive or suspicious technological glitches during remote verification of their identity.

4. A customer declines to use multifactor authentication to verify their identity.

5. A reverse-image lookup or open-source search of an identity photo matches an image in an online gallery of GenAI-produced faces.

6. A customer's photo or video is flagged by commercial or open-source deepfake detection software.

7. GenAI-detection software flags the potential use of GenAI text in a customer's profile or responses to prompts.

8. A customer's geographic or device data is inconsistent with the customer's identity documents.

9. A newly opened account or an account with little prior transaction history has a pattern of rapid transactions; high payment volumes to potentially risky payees, such as gambling websites or digital asset exchanges; or high volumes of chargebacks or rejected payments.

FinCEN requests that financial institutions reference this alert by including the key term "**FIN-2024-DEEPFAKEFRAUD**" in SAR field 2 ("Filing Institutions Note to FinCEN") and in the narrative to indicate a connection between the suspicious activity being reported and this alert. Financial institutions should also include any applicable key terms indicating the underlying typology in the narrative.

The mission of the Financial Crimes Enforcement Network is to safeguard the financial system from illicit activity, counter money laundering and the financing of terrorism, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.

The information contained in this alert is derived from FinCEN's analysis of BSA data, open-source reporting, and information provided by law enforcement partners.

Questions or comments regarding the contents of this alert should be sent to frc@fincen.gov.