INSIGHTS

Financial Services

FinCEN Warns of Criminal Use of Deepfake Technology to Circumvent Controls

A recent FinCEN alert highlights an increase in reports of deepfake identity fraud and describes ways financial institutions can reduce risk and detect the illicit use of AI tools

By Thomas C. Kost, Filipp Kofman, Max Bonici, and Michael Treves

11.18.24

Generative artificial intelligence (AI) holds tremendous promise for financial institutions and their customers. But that promise comes with potential peril, as

highlighted in a recent alert issued by the U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN) regarding the misuse of AI by fraudsters.

Section 6206 of the Anti-Money Laundering Act of 2020 requires FinCEN to periodically publish threat pattern and trend information derived from Bank Secrecy Act (BSA) filings. Last week, FinCEN warned financial institutions about the growing use of deepfake media by criminals targeting financial institutions and their customers. Deepfake media, or "deepfakes," is a type of synthetic media, like videos, pictures, audio, or text, that use AI to fabricate or manipulate content in a highly realistic but inauthentic way. Fraudsters are increasingly leveraging these AI-generated deepfakes to bypass customer identification and verification and customer due diligence controls at financial institutions, and perpetrate fraud schemes and other financial crimes.

The FinCEN alert details how fraudsters are using deepfake technology to create fake identification documents, photographs, and even videos to access other individuals' accounts or open fraudulent accounts through which they can commit other crimes. The alert also highlights how criminals have used AI-enabled tools in support of other scams, such as business email compromise schemes, spear phishing attacks, elder financial exploitation, family emergency schemes, romance scams, and virtual currency investment scams.

Here are several key takeaways for financial institutions:

- **Deepfake identity fraud is on the rise.** FinCEN's analysis of BSA data shows a spike in suspicious activity reports (SARs) describing the suspected use of deepfake media in fraud schemes. These schemes often involve criminals altering or creating fraudulent identity documents to circumvent identity verification and authentication methods.

- **Deepfakes can circumvent identity verification.** Criminals can create deepfake images by modifying an authentic source image or creating a synthetic image by combining AI images with stolen or even entirely fake personal identifiable information. Financial institutions have

reported that criminals have employed AI to alter or generate images used for identification documents. Even advanced identity verification methods, like multifactor authentication and live video or audio checks, may be vulnerable to determined fraudsters.

- **Red flags for detecting deepfake fraud.** FinCEN highlights nine red flag indicators for suspicious activity related to the illicit use of AI tools, such as inconsistencies in identity documents, customers declining multifactor authentication or using a third-party webcam plugin during a live verification check, and reverse image searches matching the customer's photo to a gallery of AI-generated faces. Financial institutions should ensure that these red flags are incorporated into customer onboarding procedures and that all suspicious transactions or transactions that appear to be associated with the illicit use of AI tools are subject to additional scrutiny.

- **Recommendations for mitigation.** To reduce the risk of deepfake fraud, FinCEN suggests financial institutions re-review a customer's account opening documents, conduct a reverse image search and other open-source research, or subject identity documents to deepfake detection software. Financial institutions should also consider the use of advanced identity verification techniques recommended by the Department of Homeland Security, such as liveness checks and biometric authentication. Beyond account opening, institutions should closely monitor accounts for suspicious activity patterns, like rapid transactions, high payment volumes to high-risk payees, and frequent chargebacks, and subject those accounts to enhanced due diligence.

- **Institutions must report deepfake fraud.** FinCEN reminds financial institutions of their suspicious activity reporting requirements under the BSA. FinCEN requests that financial institutions reference the alert in SAR field 2 and in the narrative to indicate a connection between the suspicious activity being reported and the alert.

While deepfakes may seem like futuristic technology, the FinCEN alert reveals

that the threat is very real today. By understanding the tactics used by fraudsters and the red flags to watch for, financial institutions can implement the right controls to detect and prevent deepfake-enabled fraud and comply with the expectations of state and federal supervisory and enforcement agencies.

DWT's cross-functional team of AI and financial services experts are here to help. If you have any questions about the alert or your company's preparedness to combat deepfakes, please contact the authors or your DWT attorney contact.

Related Insights

10.10.25
INSIGHTS

Wolfsberg Report Casts Light on Path Forward for Crypto Risk Management

09.24.25
INSIGHTS

Tokenized and Stablecoins Initiative Announced by the CFTC

09.22.25

INSIGHTS

Don't Forget to File Your 2025 OFAC Annual Report of Blocked Property