FinCEN Warns Financial Institutions of Fraud Schemes Arising from Deepfake Media Using Generative Artificial Intelligence

Anton Janik, Jr.
ajanik@mwlaw.com
(501) 688.8888

11/13/2024

Today the U.S. Department of Treasury's Financial Crimes Enforcement Network (FinCEN) issued an Alert to help financial institutions identify fraud schemes relying in part on the use of deepfake media created through generative artificial intelligence (GenAI). FinCEN specifically notes seeing "an increased in suspicious activity reporting by financial institutions describing the suspected use of deepfake media, particularly the use of fraudulent identity documents to circumvent identity verification and authentication methods."

The FinCEN Alert states that beginning in 2023 and continuing into this year, FinCEN has noted an uptick in suspicious activity reporting by financial institutions that describe the use of deepfake media in fraud schemes targeting their institutions and customers. The schemes include the altering or creation of fraudulent identity documents to circumvent authentication and verification mechanisms, which has been enabled by the recent rise of GenAI tools. Using those tools, perpetrators can create high-quality deepfakes (highly-realistic GenAI-generated content), including false identity documents and false video content for secondary visual identification, that is indistinguishable from documents or interactions with actual verifiable humans. "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. 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."

FinCEN is aware of situations where accounts have been successfully opened using such fraudulent identities and have been used to receive and launder the proceeds of other fraudulent schemes, including "online scams and consumer fraud such as check fraud, credit card fraud, authorized push payment fraud, loan fraud, or unemployment fraud. Criminals have also opened fraudulent accounts using GenAI created identity documents and used them as funnel accounts."

FinCEN advises re-reviews of account opening documents, including performing a reverse image search of identity photos to see if they match any online galleries of faces created with GenAI. To the extent capable, financial institutions may find examining the image metadata or using software engineered to find deepfakes to be assistive. FinCEN cautions financial institutions to watch for identity discrepancies between account documents, consider evaluating IP address discrepancies from normal customer IP address usage, patterns of coordinated activity among multiple similar accounts, high volume payments to gambling websites or digital asset exchanges, high volumes of chargebacks or rejected payments, patterns of rapid transactions in newly opened accounts, and patterns of withdrawing funds immediately after depositing funds in situations where the ability to reverse a payment difficult (including through use of international bank transfers or payments to offshore digital asset exchanges and gambling websites).

FinCEN identifies certain best practices to help financial institutions reduce their risk, including the use of multifactor authentication and phishing-resistant multifactor authentication as well as live verification checks where identity is confirmed using live video or audio. When live video or audio is used, FinCEN advises watching for claimed technical glitches preventing such verification, and the same during such video or audio verification, which may help identify that GenAI is in use.

FinCEN continues to investigate the scope of this issue and 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” when reporting suspected deepfake activity.

Attorney Anton Janik has a specialized practice in complex litigation, tax controversies and information privacy, security and data rights law. He is an a Certified Information Privacy Professional/United States (CIPP/US) and a Certified Information Privacy Professional/Europe (CIPP/E).