Terrorist Use of AI to Facilitate Fraud Requires Adaptability

SCOPE: This product highlights considerations for public safety and private sector partners, including investigators and analysts, who may encounter terrorists using generative AI to facilitate fraudulent activity in support of their terrorist conduct. This product is not a response to a specific threat against the United States.

Terrorists may use rapid advancements in AI to supplement fraud efforts and to avoid detection, accelerating the need for countermeasures. Generative AI, which generates content based on user prompts, has been used for fraud for several years, but as the technology advances it may become harder for the human eye to detect in the future. Agentic AI, which is capable of executing complex and multistep tasks independently, may also make automated online fraud easier and attribution harder because of its ability to adapt to changing conditions and operate autonomously. These rapid advances make public safety awareness critical to detecting and deterring the use of AI technologies by terrorists.

- **Online Fraudulent Document Creation:** OnlyFake is a website that uses generative AI to help customers quickly and easily generate convincing ID documents. Customers can create a variety of documents, including passports and driver's licenses, and also generate these documents in bulk. These documents have been used to falsely authenticate individuals' identities when accessing financial institutions through know your customer (KYC)[a], identity verification, and document verification systems.
- **Cyber Fraud:** A cybercriminal with minimal programming expertise used AI-generated code to conduct a complex extortion scheme that used automated reconnaissance[b] and target discovery, live-network penetration operations,[c] malware with evasion capabilities, and data extraction and analysis to create personalized ransomware notes targeting multiple victims. While this actor was not a terrorist, this is an example of conduct that could be exploited by terrorists.
- **Deepfakes Enabled Extortion:** FTO-designated transnational criminal organizations along the US-Mexico border use AI-generated videos and voice generators to extort the families of missing migrants. They use authentic images of the migrants to create AI-generated videos of them being kidnapped or held hostage even though the group does not have custody of the missing person.

AI has also been used to create breeder documents. These documents are a set of original credentials, such as birth, death, and marriage certificates, used to establish an individual's identity, nationality, or other vital information. They are considered "source documents" because they are often used to obtain other documents, such as a passport, driver's license, or social security card.

Generative AI tools have reduced the resources required to produce content that has been modified or manipulated through analog or digital technology. This content is often difficult to distinguish and is highly realistic. Illicit use of this rapidly evolving technology creates detection challenges for law enforcement. Caution should be given when using third-party or open-source tools for investigative or research purposes, particularly if sensitive or proprietary data is involved.

AI can generate some aspects of a physical ID. It cannot supplement the specialized components required for physical documents, such as optically variable ink (OVI) ink and specialized paper types. Several forms of AI models can be used, such as generative AI, which creates new data, and discriminative AI, which separates and labels data.

AUTOMATED LAYER
Discriminative AI can insert and assemble information at a large scale.

GENERATED LAYER
Generative AI can be endlessly creative when generating these elements because consistency is not required.

SIGNATURE
Generative AI can learn how to plausibly recreate an individual's signature that may not be detected as fraudulent.

HOLOGRAM
Discriminative AI can assemble the overall ID, including the hologram. It cannot generate the hologram or place it onto the ID.

PORTRAIT
Generative AI can create an image of an individual that may be hard to identify by the naked eye as AI generated. This could be used for multiple purposes, such as matching the image to the details on the ID or adding a person to an ID that is not their own.

BACKGROUND
Generative AI can create a background containing the specific details used as security measures for an ID. It cannot replace OVI ink or specialized paper types.

TEXT
Discriminative AI can organize and assemble information used in the text of an ID. It cannot print the text onto the ID.

ID TEMPLATE
Discriminative AI can assign a pre-existing ID template to an ID in the assembly process. It cannot generate the ID template because these are created by the country or state that issues the ID.

Example of an AI-generated image of a physical ID

[a]A process used by banks and financial institutions to verify a customer's identity and assess risk to help prevent fraud, money laundering, and terrorist financing.

[b]Use of automated tools and techniques to gather information about a target's computer network, systems, and vulnerabilities.

[c]Cyber operations conducted on a target's computer network in real time.

NCTC-JFRT-2026-09877

16 JUNE 2026
AUTHORED BY NCTC, DHS, FBI

Terrorist Use of AI to Facilitate Fraud Requires Adaptability *(continued)*

Considerations

Verification as a Multi-Layered Approach: As AI advances, digital detection tools often lag behind illicit use, reducing their effectiveness. For example, AI image generator detectors identify subtle signals or unusual patterns, but they sometimes incorrectly label legitimate photos as AI-generated. A layered approach that combines multiple verification and detection methods is typically more effective for validating and authenticating potential AI content.

- Conduct open-source research, including reverse image searches, to identify photos or other images from online sources.
- Review source documents and materials for inconsistencies, including between the identity documents and other aspects of the persona.
- Multifactor authentication can help confirm identities; illicit actors may attempt to avoid or circumvent enhanced checks. Use one-time, unique password or PIN, or biometrics to strengthen identity proofing.
- Remain aware of visual or voice inconsistencies, like out-of-place shadows, audio filters or artifacts, refusals to conduct live checks, or irregular blinking or inconsistent facial micro expressions.
- Verify documents digitally instead of relying on scanned copies of documents and cross-check through a trusted platform.
- Compare voice or video to previous verified samples when available.
- Request interactive, unscripted prompts that only a live person could conduct and/or ask questions that are not easily answered through open-source research.

Enhancing Detection Through Technologies: While methods may evolve and contain some limitations, the following potential detection methods offer ways to leverage evolving technologies for analyzing and identifying potential AI-generated fraudulent documents and media. Methods should not be used on their own but may supplement other detection strategies when appropriate. Always follow departmental polices and guidance.

- **AI Detection:** Current detection capabilities could integrate tools to analyze documents and identify potential AI-generated content, including image analysis (document shading, layout, texture), metadata analysis (document creation date, author, editing history), and pattern recognition (linguistic or formatting patterns indicative of AI-generated content).
- **Biometrics:** Data such as facial biometrics, fingerprint analysis, or behavioral recognition can enhance visual verification.

Public and Tech Sector Partnerships

- Enhance awareness of trends in terrorist online activity using open-source resources from the tech sector, academia, and civil society organizations.
- Participate in, and contribute to, cross-sector discussions between public safety and tech sector officials to build common understanding of terrorist tactics, techniques, and procedures (TTPs).

Training and Engagement

- Collaborate with state or local vital records offices, clerk's offices, health departments, recorder offices, or similar offices to share TTPs and coordinate on investigations that may involve breeder documents.
- Train and develop a digitally literate workforce that incorporates detection techniques, reporting mechanisms, and response protocols for suspected fraudulent AI-generated content. Review and update policies on a recurring basis to account for evolving technologies.
- Law enforcement and prosecutors should work closely to develop a strategy for bringing a case involving AI-generated evidence to court, including ways to present evidence and the investigative techniques used to identify and analyze the documents.
- Strengthen digital forensics capabilities, updating processes and detection systems to maintain effectiveness.
- Test processes by using fraudulently generated AI content in multijurisdictional exercises and, when possible, stress test scenarios involving AI generated content.
- In the cases of document fraud, report instances of exploitation of official credentials and documents to law enforcement.

Policy and Planning: Evolving technologies exploited for illicit use requires public safety officials to maintain awareness of the threat environment and adjust mitigation strategies.

- Agencies may consider ensuring biometric data and digital signatures are included in definitions of personal identifying information (PII).
- Collaborate with state and local legislatures to ensure AI-generated media, deepfake technology, and any false impersonation records, including the unauthorized acquisition, use, or sale of PII for fraudulent purposes, are accounted for when developing policy, planning, and response capabilities.
- As AI continues to advance, it may be important to prioritize the acquisition and use of AI-enabled detection systems for fraudulent document and media detection.

Potential Indicators: The following information is a possible indication that generative AI was used to create, modify, manipulate, or disseminate content.

- Identifiable AI software watermarks or other inconsistent text or images
- Finding an image in an online gallery of generative AI-produced content after conducting a reverse image or open-source search
- Visual signs of alteration or inconsistent texture, shading, or other visual features that may be detected upon closer inspection
- Stripped metadata, which may indicate that media was potentially manipulated or obtained from social media or other processes that automatically removes metadata information
- Lack of security features, such as holograms, watermarks, microprinting, raised printing, laser engraving, or optically variable ink
- Information across multiple identity documents is inconsistent with each other (e.g., name, date of birth, address)
- Anomalies in the formatting, layout, or structure compared to an official document

Resources

FBI Field Offices

FBI Internet Crime Complaint Center (IC3) is the central site for victims to file a complaint or report cybercrime and receive training and updates about cyber threats.

Financial Crimes Enforcement Network provides support and resources to law enforcement to assist with investigations and provides training opportunities related to financial crimes.

JCAT: First Responder's Toolboxes provide information about terrorist tactics and response and mitigation considerations. These products can be found on JCAT's website, DHS's Homeland Security Information Network, or FBI's Law Enforcement Enterprise Portal.

- Evolving Landscape: Fraudulent Document Use To Circumvent Detection and Screening
- Violent Extremists' Use of Generative Artificial Intelligence

The Homeland Security Investigations (HSI) Forensic Laboratory provides a broad range of document and latent print-related forensic, intelligence, and investigative support services.

US Customs and Border Protection (CBP): CBP's Fraudulent Document Analysis Unit serves as a central repository and point of analysis for all fraudulent travel documents intercepted or recovered by CBP personnel. FDAU@cbp.dhs.gov

NCTC-JFRT-2026-09877

16 JUNE 2026
AUTHORED BY NCTC, DHS, FBI

JCAT

JOINT COUNTERTERRORISM ASSESSMENT TEAM

PRODUCT FEEDBACK

Please use the link below to complete a short survey. Your feedback will help JCAT develop counterterrorism products that support the public safety and private sector community.

https://www.JCAT-url.com

For further information, please email JCAT
jcat@odni.gov

(U) The Joint Counterterrorism Assessment Team (JCAT) is a collaboration by NCTC, DHS, FBI, state, local, tribal, and territorial government personnel to improve information sharing and enhance public safety. The First Responder's Toolbox is an ad hoc, unclassified reference aid intended to promote counterterrorism coordination among federal, state, local, tribal, and territorial government authorities and partnerships with private sector officials in deterring, preventing, disrupting, and responding to terrorist attacks.