



# Diving Into Deepfake

## The Misuse of Synthetic Media

The use of generative artificial intelligence (GenAI), synthetic media and deepfake content for Money Laundering (ML), Terrorist Financing (TF) and the Financing of the Proliferation of weapons of mass destruction (PF) has become a critical threat to the global financial system.

**Synthetic Media** includes all types of media that has either been created through digital or artificial means or media that has been changed or manipulated with the use of technology.

**GenAI** refers to intelligence that can create new content like text, images or music based on patterns learned from data. Traditional artificial intelligence analyzes existing data but GenAI produces original content by monitoring patterns.

**Deepfakes** use artificial intelligence to create content that appear to be genuine, human generated events that actually did not happen or do not exist.

### Characteristics of Deepfakes and Synthetic Media

- **Realism.** GenAI can rapidly create realistic-looking images. Moreover, the technology has shed common imperfections from its earliest stages. This means fewer strange-looking fingers, distorted faces, or stretched-out arms that were once deepfake giveaways.
- **Accessibility.** You do not need a degree in AI or artistic design to use GenAI to create deepfakes. The barrier to entry is lower than ever.
- **Scalability:** Thanks to cloud computing, criminals can launch multiple attacks simultaneously or create a large volume of synthetic content for a targeted campaign, such as in spear fishing fraud.

### The Use of Deepfakes to Commit Financial Crimes

**Account Takeover Fraud.** By mimicking an account holder's appearance, voice, and mannerisms, fraudsters can convince a customer service representative to grant them access to someone else's account.

**Phishing Scams.** Spelling and grammar mistakes were once obvious red flags of phishing scams. However, thanks to GenAI, criminals are less likely to make these errors. Fraudsters can craft highly convincing phishing messages that are grammatically correct, contextually relevant and contain perfect spelling.

**Impersonation Attacks.** Fraudsters can convincingly imitate individuals in professional settings like meetings or legal proceedings to commit fraud. In personal settings, they can pretend to be a loved one in need of financial or medical help, such as in a romance or grandparent scam.



## Deepfake at Work: Meet Mark

Mark, who works in his company's finance department, suddenly receives an urgent email from what appears to be the CEO. The message includes the company logo and the CEO's familiar email signature.

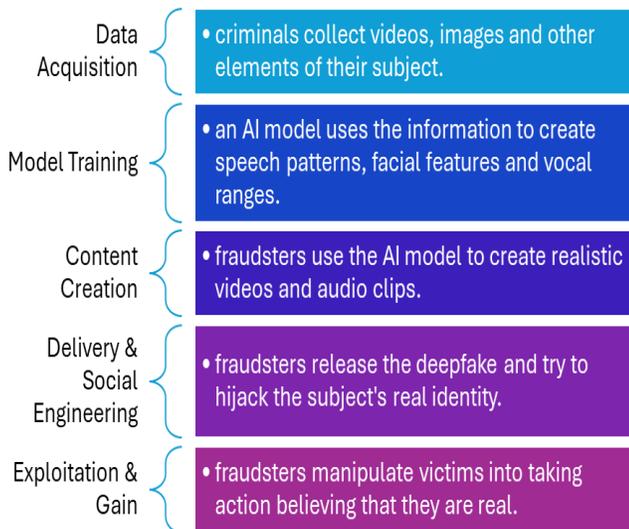
The email asks him to immediately process a large payment to a new vendor. Suddenly, his phone rings. The voice on the other end sounds just like his boss and provides specific details about the transfer.

Feeling the pressure to make his "boss" happy and believing the sincerity of the request, Mark authorizes the payment. He later learns the email and the phone call were both elaborate deepfakes, and the money is now in the hands of fraudsters.

Mark's story highlights how social engineering combined with realistic deepfakes can deceive even careful employees into making costly mistakes.

### Creating a Deepfake

Carrying out fraudulent activities involving Deepfakes involves several critical steps.



## How Financial Institutions Can Protect Against Deepfake Fraud

Protecting Financial Institutions (FIs) and Designated Non-Financial Businesses and Professions (DNFBPs) from deepfake fraud requires a proactive approach. Here are a few key steps to consider:

### Emphasize Intent Over Identity

Scammers coerce victims into authorizing transactions under false pretenses. This renders traditional authentication methods like SMS verification and questions like "Was this you?" obsolete. Instead, FIs and DNFBPs must understand the *intent* behind a transaction. This requires a move towards human-to-human interaction with trained agents equipped to ask the right questions and flag inconsistencies that may indicate fraud.

### Uncover Money Mule Accounts

Fraudsters use money mule accounts to move and launder stolen funds. They often try to convince or manipulate legitimate customers to act as money mules. Banks must proactively monitor both inbound and outbound transactions to identify suspicious activity, disrupt the flow of illicit funds and report it to the Financial Intelligence Unit (FIU). This comprehensive approach enables FIs and DNFBPs to reduce and disassemble mule networks and mitigate the impact of deepfake fraud.

### Empower Customers Through Education

Teach customers about how deepfakes work to help them better protect themselves. FIs and DNFBPs should launch campaigns to raise awareness of known deepfake scams, including romance scams and grandparent scams. Some key lessons to convey to customers include:

- Ask the person on camera or speaker to repeat a very specific sentence to see if the audio follows along.
- Ask someone on video to wave or move his/her arms in a specific manner to confirm he/she is real, not pre-recorded.
- Have a secret code known only to family members to verify identity before making any serious financial decisions.

## References

- ◆ CFATF Research Desk: ML and TF through the Misuse of Synthetic Content and Deepfake Media. April 16th 2025
- ◆ What are Deepfakes and How Do They Impact Fraud? | Feedzai