Flash Report • February 2025

UNIVERSITY of SOUTH FLORIDA
Office of Internal Audit

Artificial Intelligence (AI) Fraud Risk

Artificial intelligence (AI) tools and techniques are being used more frequently by fraudsters to commit fraud and make their schemes more sophisticated. These tools are often used to fool employees into sharing sensitive information, authorizing transactions, or taking other inappropriate action because the employee believes the individual they are interacting with is known to them and trustworthy.

- **Deepfakes**
  - A video image created using AI that mimics a real person’s appearance and mannerisms. Deepfakes create the illusion that you are interacting with a real person or group of people.
- **Voice Cloning**
  - A real person’s voice is replicated using a sample of their speech obtained from a valid source. The cloned voice is then used to convince an employee to take inappropriate action.
- **AI-Enabled Chatbots**
  - By leveraging generative AI, sophisticated chatbots can be designed to manipulate victims by mimicking human-like interactions, thereby gaining their trust and credibility.
- **Social Engineering Attacks**
  - AI can increase the sophistication of social engineering attacks by gathering detailed information about an employee, enabling personalized and convincing scams.

Recommended Practices to Combat AI Fraud

- Validate any requests independently through an approved channel.
- Always ensure all tools being used are aligned to USF requirements; refer to the list of approved generative AI tools supported by USF IT.

Where can I find more information?

- USF Regulation 5.001: Fraud Prevention and Financial Detection
- USF Office of Internal Audit website: https://www.usf.edu/audit/

How can I report potential fraud or abuse?

- Notify your supervisor
- Contact the USF Office of Internal Audit at (813) 974-2705
- Report general USF fraud & abuse through the EthicsPoint hotline at (866) 974-8411