OFFICE OF INSPECTOR GENERAL
LSC America's Partner for Equal Justice
LEGAL SERVICES CORPORATION

Office of Inspector General
Legal Services Corporation
Thomas E. Yatsco, Inspector General
202.295.1660
www.oig.lsc.gov

FRAUD ADVISORY
25-0098-A-FA

TO: Executive Directors and Board Chairs

FROM: Thomas E. Yatsco
Inspector General

DATE: March 6, 2025

SUBJECT: Avoiding Artificial Intelligence (AI) Fraud Schemes in Civil Legal Aid

Know the Risks: AI in the Legal Aid Community

- Artificial Intelligence (AI)[1] offers numerous benefits to our civil legal aid community. As legal aid organizations begin to incorporate AI into their business operations, you should also be aware of the potential fraud and cyber risks posed by the use of AI.

- By understanding the ways fraudsters use AI to effect fraud schemes and taking action to combat them, your legal aid organizations can help mitigate risks associated with AI-Driven Fraud.

- The Legal Services Corporation (LSC) Office of Inspector General (OIG) urges you and your staff to familiarize yourself with these schemes and review the resources and articles available within this advisory, as you develop or mature your AI policies and processes.

As legal aid and nonprofit organizations, many of you are harnessing the technological advancements offered by AI to bring about significant efficiencies and increased productivity within your organizations. AI can assist legal professionals in drafting documents, offering real-time guidance, and

[1] Merriam Webster defines artificial intelligence as "the capability of computer systems or algorithms to imitate intelligent human behavior."

improving response times. AI is ultimately making it easier for legal professionals to bridge the justice gap and serve their clients faster and more efficiently. Even though AI can be a valuable tool within the legal aid sphere, it can also become a potential avenue for bad actors to commit fraud.

Through this fraud advisory, the OIG seeks to inform you of common AI fraud schemes, as well as actions and resources available to combat these risks. We suggest you share this advisory with your senior leaders, such as Chief Financial Officers, Information Technology (IT) professionals, and Human Resources Directors. Also, please feel free to disseminate it to your professional networks.

How AI Can be Misused or Exploited for Malicious Purposes

Advances in AI have not only created opportunities for new fraud schemes but have also expedited well-known and frequently used cyber schemes to larger populations and targets. Below you will find common AI cyber schemes to share with your employees.

Deepfake schemes occur when AI is used to create realistic, yet fake video or audio recordings. These videos or audio recordings impersonate trusted individuals with the goal of misleading the recipient into taking action that could ultimately cause harm to the individual and/or your organization.

Chatbot Schemes are fake online chat encounters in which an AI imitates a person, such as a customer support representative or technical support, on a known website. The AI chatbot typically asks the user for their personal information or other confidential information to further the scheme.

Automated Phishing Attacks use AI to reach a larger audience by crafting highly personalized phishing emails that are difficult to distinguish from legitimate communications. These phishing emails can be used to trick employees into revealing sensitive information about employees and clients or making unauthorized transactions that waste scarce resources.

Data Manipulation and Document Forgery can be achieved through AI. AI programs can be used to create fake bank statements, accounting documentation, board minutes, and can also be used to alter other documents such as financial records. These fake documents can be exploited for malicious purposes such as fraud, identity theft, and inducing fraudulent business transactions.

Malware Attacks can be increased and widely spread by scammers through AI. For example, a bad actor may use social media platforms to spread AI-generated videos that trick viewers into downloading malware or viruses. Malware can lead to significant financial losses by stealing sensitive information such as credit card details, banking credentials, or personally identifiable information

(PII). Ransomware (a type of malware) can also be used to lock users and organizations out of their data and systems. The threat actor will usually demand a ransom for access.

Synthetic Identity Fraud is a type of identity theft in which criminals combine both real and fake personal information to create a new, fictitious identity with fraudulent documents such as driver's licenses and employee ID cards, that can then be used for various identity-related schemes, such as obtaining credit or goods.

How to Combat AI-Driven Fraud

Educate and Train Staff: Implement regular training sessions on AI fraud schemes. You should strongly consider training your employees to act as the first line of defense by recognizing phishing attempts and other fraudulent activities. In the next section of this memorandum, we identify resources to assist you in educating and training your team.

Ensure Privacy and Confidentiality: Protect employee and client personally identifiable information (PII) and data. AI's utilization of user input data can pose privacy risks. As such, users must take reasonable steps to protect PII from falling into the hands of unintended recipients. Many AI applications retain queries and share entries with third parties; therefore, users should check the terms and conditions to prevent possible risk. Users should not share confidential or sensitive information and ensure the AI platform your organization uses has adequate data privacy and security safeguards in place. If not, any sensitive information could be retained within the AI system and accessed or sold to third parties.

Be Wary of Impersonation and Urgent Requests: Remain vigilant with any online interactions and communications, especially those asking you to take immediate action, and always employ two-step verification for any financial transactions or confidential information sharing.

Secure Your Devices: Scan your devices for malware using virus scanners approved by your Information Technology (IT) department and update your devices to ensure you have the latest security features.

Utilize Two-Factor Authentication for Online Accounts: Two identifying factors, such as a password entry and also a text sent to your phone to access your online account, would require a fraudster to obtain both—thereby diminishing the likelihood of becoming a victim.

Secure Your Organization's Social Media Profiles and Websites: Do not release more information than is necessary related to your employees' titles or contact information in the public sphere. This type of information is harnessed by cyber threat actors during social engineering and can be used to scam or imitate you or one of your employees.

Research the AI Company's Cybersecurity Policies: When using an AI tool, review whether the application experienced any recent data breaches or cybersecurity threats, as well as policies surrounding how the AI platform stores data and if that user data is shared with third parties.[2]

Review LSC's Technology Baselines: As you integrate AI into your legal services, consider how AI can be implemented within these baselines. LSC's Technology Baselines include policies and procedures related to technology security such as cloud computing, mobile device management, training, and incident response, among others.[3]

Continue to Make Procedural Improvements: Implement procedural controls to mitigate AI-powered social engineering attacks and ensure your organization's critical processes have a mandatory control that authenticates identity (e.g. a call back mechanism[4]).[5]

Report Cyber Incidents Promptly to the OIG Hotline: LSC Grant Terms and Conditions require grantees to report cyber incidents to the Office of Inspector General Hotline. As a follow-up to the hotline report, the OIG will request grantees also complete a form when the OIG requires additional information related to the cyber incident.

Report Any Scams to the Federal Trade Commission (FTC): The FTC collects reports of fraud, scams, and bad business practices, as well as cases of identity theft.

Resources and Articles

The following resources may prove helpful in preventing, detecting, or remediating an AI fraud scheme.

LSC OIG Cybersecurity Resources

[2] A2J Tech And LSNTAP. "AI for the Modern Legal Aid Organization: A Guide on What to Consider When Implementing AI in Your Legal Aid Organization." LSNTAP.org. www.lsntap.org/sites/lsntap.org/files/AI%20Guide%20for%20Legal%20Aids%20V2%20LSNTAP%20Logo.pdf

[3] LSC's Technology Baselines Guide

[4] A callback mechanism for authenticating identity is a process used in various authentication protocols, such as OAuth2 and OpenID Connect, to verify a user's identity.

[5] Info~Tech Research Group. "Deepfake-Powered Social Engineering Attacks – What, Me Worry?" Infotech.com. www.infotech.com/research/deepfake-powered-social-engineering-attacks-what-me-worry

Bureau of Consumer Protection | Federal Trade Commission

Fraud and scams | Consumer Financial Protection Bureau

TransUnion, Equifax, and Experian have options for placing a credit freeze on your accounts if you suspect or detect suspicious activity on your credit report. Additionally, if you are concerned that you have been a victim of identity theft, you can file a fraud alert at one of the three above-mentioned national credit bureaus' websites.

AI and Fraud: What CPAs Should Know

The Fraudsters Have AI, Too

AI and the Risk of Consumer Harm

Inside the FBI Podcast: Defending Against AI Threats

Are Chatbots the New Weapon of Online Scammers?

Questions and Contacts

If you have any questions or would like additional information about this or any other issue, please contact Daniel O'Rourke, Assistant Inspector General for Investigations, LSC OIG, at (202) 441-9948 or by email at dorourke@oig.lsc.gov.

Sign Up for LSC OIG Alerts & Advisories

If you would like to stay current with our most recent OIG fraud alerts and advisories, please follow the directions on our homepage at https://oig.lsc.gov/, see "Sign Up for Email Updates" to subscribe to new LSC OIG website postings.