BALANCING THE RISKS AND BENEFITS OF GENERATIVE AI IN COMBATING CHECK FRAUD

Generative artificial intelligence (AI) models that can create new text, image, audio and video content have emerged as a risk that can amplify fraudulent activity used to commit check fraud. Continued improvements in, and adoption of, generative AI prompts a deeper dive into how it can be used by criminals and how financial institutions can use it to enhance their fraud mitigation processes.

Criminals may use generative AI to commit check fraud, either directly or indirectly. While many methods are indirect, such as employing generative AI-driven techniques to steal information later used for check fraud, other methods are more direct and use generative AI to create more convincing fraudulent checks.

GENERATIVE AI USED TO DIRECTLY FACILITATE CHECK FRAUD

Criminals are using generative AI to create more convincing fraudulent checks. Examples of this include:

Manipulating Stolen Checks

Generative AI can manipulate images of stolen checks, reducing typical signs of check washing.

Creating Counterfeit Checks

Stolen information can be used by generative AI to create convincing counterfeit checks based on legitimate images.

Forging Signatures on Checks

Maker signatures can be extracted from documents, then recreated by generative AI on items to appear legitimate.

CHECK FRAUD IS AUGMENTED INDIRECTLY BY GENERATIVE AI-DRIVEN EXPLOITS

Even more common than using generative AI directly to commit check fraud are indirect methods, where generative AI facilitates other fraud schemes that enable check fraud. These may include:

- **Phishing/spear phishing.** Generative AI can easily pull content and logos from public sources to craft convincing emails at scale.
- **Social engineering.** Generative AI amplifies phishing tactics to trick individuals into providing personally identifiable information, financial information or credentials, which can be used to steal more information, create fraudulent checks or open new accounts to deposit fraudulent checks.
- **Deepfakes.** Criminals use generative AI to create videos, images and audio that mimic real, trustworthy people to commit scams. Victims of scams may become involved in check fraud if the criminal convinces them to deposit or cash fraudulent checks.
- **Synthetic identities.** Manufactured identities created using generative AI may be used to open new accounts in a more scalable manner to facilitate check fraud.
- **Automation.** Bad actors use generative AI to create scripts to automate check processes, enabling them to make multiple deposits at different financial institutions before the first item can be flagged and returned.

BALANCING THE RISKS AND BENEFITS OF GENERATIVE AI IN COMBATING CHECK FRAUD

Financial Institutions Can Leverage Generative AI

Artificial Intelligence (AI) is not a new concept when it comes to fraud prevention. AI can be trained on historical patterns and use image analysis to quickly identify potentially fraudulent checks.

Now, generative AI can enhance investigations, identify potential crime rings and extract value from unstructured data. Financial institutions can consider exploring how generative AI can help them:

- **Summarize fraud investigations.** Compile case details from multiple sources and formulate an investigation summary or narrative using generative AI for further analysis.
- **Link unstructured data.** Generative AI can identify themes and summarize fraud trends across cases, supporting quicker identification of potential crime rings by linking similar activity.
- **Develop synthetic test data.** Generative AI can manufacture data that replicates the structure of real data without exposing customers' personally identifiable information. This data, known as synthetic data, can be used to create, mature and validate prevention models.
- **Curate targeted education.** Use generative AI to create educational content about current fraud trends to educate employees about fraudulent patterns and inform customers on relevant topics.

Please note: generative AI outputs should be reviewed to ensure accuracy and alignment with business standards.

BALANCING THE RISKS AND BENEFITS OF GENERATIVE AI IN COMBATING CHECK FRAUD

CONCLUSION

Generative AI is reshaping the check fraud landscape by increasing the speed, scale and sophistication of attempted fraud, such as improved creation and printing capabilities of a legitimate-looking checks that include security features. Simultaneously, generative AI can enhance fraud investigations and strengthen financial institutions' defenses. As criminals use generative AI to create seemingly realistic fraudulent checks and deepfakes, traditional detection methods may struggle to keep pace. In a world where generative AI elevates both opportunity and risk, preparedness, adaptability and innovation will define the future of effective check fraud mitigation.

The check fraud mitigation toolkit was developed by the Federal Reserve to help educate the industry about check fraud and outline potential ways to help detect and mitigate this fraud type. Insights for this toolkit were provided through interviews with industry experts, publicly available research, and team member expertise. This toolkit is not intended to result in any regulatory or reporting requirements, imply any liabilities for fraud loss, or confer any legal status, legal definitions, or legal rights or responsibilities. While use of this toolkit throughout the industry is encouraged, utilization of the toolkit is voluntary at the discretion of each individual entity. Absent written consent, this toolkit may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.