GENERATIVE ARTIFICIAL INTELLIGENCE INCREASES SYNTHETIC IDENTITY FRAUD THREATS

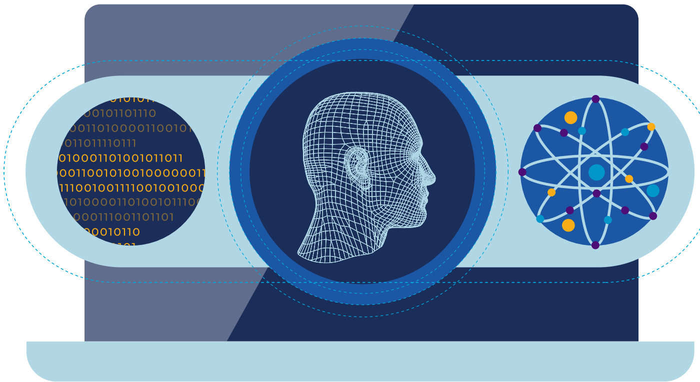
Bad actors are exploiting advances in generative artificial intelligence (Gen AI) to increase the speed, scale and effectiveness of synthetic identity fraud. Through this evolving technology, fraudsters can automate the creation of synthetic identities and make them appear more authentic based on support content. Financial institutions face the potential for increased losses from the malicious use of synthetic accounts with the intent to steal money, transfer illicit funds or gain access to bank products. Individuals and businesses are increasingly confronted by social engineering schemes that use AI-generated synthetic identities that can result in account takeovers, scam payments and compromised personal information.

Synthetic identity fraud is the use of a combination of personally identifiable information (PII) to fabricate a person or entity in order to commit a dishonest act for personal or financial gain.

Synthetic identity fraud losses continue to grow and are estimated at $35 billion in 2023.[1] Artificial intelligence enables computer systems and machines to perform complex tasks, such as decision-making or speech recognition that simulates human intelligence. It has become part of everyday life in many different forms, including customer service chatbots, ChatGPT and other online tools, and virtual assistants, such as Siri® and Alexa®. A more recent innovation, Gen AI can produce text, images, audio, synthetic data and other content. Gen AI can assist users to design, research, write, plan, organize and code based on a human user's request and inputs.

GEN AI SCALES UP SYNTHETIC IDENTITY FRAUD

The creation of synthetic identities typically starts with personal information stolen through data breaches, malware or social engineering. Personal information also is offered for sale on the dark web, on other internet sites and through messaging apps. Gen AI uses this information to maximize the total number of synthetic identities created from the source information by interchanging details – such as applicant name, mailing address, birthdate and Social Security number – and to invent personal details.



Gen AI can use the synthetic identities to apply for new accounts or credit cards. It can use the same synthetic identities across multiple financial institutions. And it can learn from its failures. An application from a 70-year-old synthetic identity with a newly established credit history is not likely to be approved, so Gen AI simply changes the birth year to create a younger identity.

GENERATIVE ARTIFICIAL INTELLIGENCE INCREASES SYNTHETIC IDENTITY FRAUD THREATS

To make synthetic identities appear legitimate, Gen AI can:

- Create authentic-looking documents to present along with a credit application to corroborate personal information, such as birth certificates, Social Security cards, pay stubs, bank statements, utility or phone bills.
- Use photos available online to create authentic-looking driver's licenses that include personal details required for credit approvals.
- Produce fake images, videos, or misleading voice recordings, called deepfakes. These digitally altered results can be sophisticated and may convincingly appear to be real people because of realistic Gen AI characteristics such as hand gestures and unique speech patterns. Real-time deepfakes are scripted but flexible enough to respond to unexpected questions or requests as part of an account opening process. The images or videos may be set up by fraudsters as an authentication factor to access accounts in the future using facial recognition.

These Gen AI features increase the number of accounts opened with synthetic identities that then can be used to steal money by making credit card purchases or overdrawing an account with no intent to repay. Fraudsters may choose to let accounts mature to obtain higher credit limits or apply for loans to increase the amount available to steal. The accounts can be used to receive and transfer money to support other criminal activities, such as fraud, scams and money laundering.

Fraudsters also use synthetic identities to conduct social engineering and facilitate scam activity. They contact and manipulate individuals to provide account login details, share personal information or make scam payments. They use Gen AI to launch large-scale attacks, contacting people and businesses through social media, phone, text messages and email. Gen AI is programmed to manage these communications to convince people to send money based on investment opportunities, romantic interests or other scams; share personal information or account login details; or download malware to their computers or devices. The personal information collected can be used to create more synthetic identities. Compromised account login credentials are used for account takeovers to gain access and send unauthorized payments from victims' accounts. Gen AI automation increases the scale of fraud and scams, since a fraudster's manual response is no longer needed. Furthermore, by using synthetic identities for outreach, fraudsters are insulated from the criminal activity and unlikely to be identified.

Although criminals are using Gen AI to increase their fraudulent activities, many organizations have found positive uses for the technology to help counter synthetic identity fraud.

GENERATIVE ARTIFICIAL INTELLIGENCE INCREASES SYNTHETIC IDENTITY FRAUD THREATS

FIGHTING FRAUD WITH AI AND GEN AI

AI tools and Gen AI can:

- Search for corroborating evidence that an applicant has an established history of credit, utility payments, related phone numbers and other inputs.
- Examine IDs and documents for missing or blurred wording and images, as well as check for special features, such as holograms.
- Scan for a live person and identify discrepancies, including incomplete hands and faces, missing lines or perspectives that appear to be inconsistent with the image.
- Generate fraud scenarios and data to improve model risk scores, enabling financial institutions to more quickly adapt to evolving fraud patterns without requiring human intervention. This feature allows fraud detection strategies to continually update based on new information.
- Support investigations by analyzing details to identify cases of synthetic identity fraud that may have been classified as credit losses or first-party fraud. Improved detection, even after the fact, increases financial institutions’ understanding of the occurrence and impact of synthetic identity fraud. The value of this information to benefit detection and mitigation tactics can be magnified when shared with other organizations.

CONCLUSION

As technology advances, financial institutions face evolving challenges to detect and prevent synthetic identity fraud. Criminals are using Gen AI to increase the scale of their attacks by automating the creation and execution of fraud and making synthetic identities appear real. While criminals evolve their tools and tactics, financial institutions may choose to use Gen AI to develop and test their detection and prevention approaches. Robust controls, detection tools and monitoring are needed at each point in the application and account opening processes and throughout a customer’s lifecycle. Many fraud prevention solutions include Gen AI technology because of its ability to adapt and respond to new or evolving fraud risks. As part of a layered approach, financial institutions can proactively evaluate their fraud controls to help counter the criminal uses of Gen AI.

[1] 2024 Synthetic Identity Fraud Report, FiVerity

Siri” is a registered trademark of Apple, Inc. “Alexa” is a registered trademark of Amazon Technologies, Inc.

The synthetic identity fraud mitigation toolkit was developed by the Federal Reserve to help educate the industry about synthetic identity 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.