Generative AI and Its Impact on Fraud and Identity Verification

The technology used to combat identity theft and limit fraud is constantly evolving. Unfortunately, bad actors also use emerging technologies to create new opportunities for fraud. Generative AI has already had a massive impact on the threat landscape and is set to create more complications in the future.

Deloitte predicts that generative AI could cause fraud losses to hit $40 billion in the US by 2027. That's up from only $12.3 billion last year. A recent global fraud study by my company found that executives listed generative AI as the biggest trend in identity verification over the next three to five years.

Generative AI presents you with a new threat because it allows fraudsters to easily fabricate realistic synthetic identities, text and email messages, and other documents used to carry out fraudulent activities.

The Rise of Generative AI Threats in 2024

Since ChatGPT's release in late 2022, the generative AI market has boomed and more people than ever have access to AI and machine learning tools. We are still in the early adoption stages of this technology and see more sophisticated applications daily.

Deepfakes and other fraud technologies are available on the dark web for small fees, giving more threat actors access to sophisticated AI tools. Generative AI also makes identity theft and creating synthetic identities much more scalable. This has the potential to expand the threat landscape exponentially. I expect the next several years to introduce new generative AI applications that further complicate fraud detection and identity verification.

Threat Vectors Influenced by Generative AI

Generative AI uses advanced machine learning algorithms to generate highly convincing outputs, often indistinguishable from human-created content. It can rapidly produce human-like text, realistic images, and even deepfake videos at scale. This capability enables fraudsters to easily craft believable synthetic identities, phishing emails, and texts, making it harder for you to detect their schemes.

Here are some of the most familiar types of fraud that are influenced by generative AI.

More Accurate Synthetic Identities

The ability to combine real and fake, AI-generated data creates a much higher risk for synthetic identity fraud (SIF). My company's recent fraud report found 51% of companies have seen SIF increase or stay the same and 39% are unsure whether SIF has increased. This is why 45% of

companies are worried about generative AI's ability to create more accurate synthetic identities and 74% are concerned about the potential for SIF to increase.
One limiter for SIF in the past was the amount of information needed to create believable identities. Now fraudsters can easily generate personal histories, photos, and social media profiles and build realistic synthetic identities over months or years with little effort.

Increased Volume of Phishing and Smishing

According to the FBI, there were 21,832 instances of business email fraud in 2022 with total losses of $2.7 billion. Deloitte estimates that generative AI could cause this number to increase to $11.5 billion by 2027.

Phishing involves scammers sending emails to get the recipient to click on a link containing malware, to reveal sensitive information, or to transfer money. Smishing (SMS phishing) involves a similar social engineering attack over text messages. While you have probably learned to look for warning signs when reading suspicious emails or texts, generative AI can mimic the writing style of trusted individuals and limit those common warning signs. Research shows that since ChatGPT was released, phishing emails have shown significant growth in linguistic complexity, volume of text, punctuation, and sentence length.

Deepfakes and Voice Deception

Generative AI can be used to create deepfakes by mimicking the face or voice of trusted individuals to create highly realistic videos, images, or voice messages. IDology's fraud study found an increase in the use of deepfakes for fraud across all industries, with gaming (46%), retail (43%), and banking (42%) as the most prevalent.

Voice deception can be an especially threatening tactic that allows fraudsters access to secure systems, financial theft, or other forms of social engineering. According to McAfee, 77% of respondents targeted by an AI voice clone lost money.

Using AI for Identity Verification and Fraud Management

Generative AI presents significant challenges and a much larger threat landscape. However, AI and machine learning solutions can also help mitigate these risks. Just as AI is used to increase the volume and sophistication of fraud, you can use AI to scale and automate risk management.

AI can be used to quickly process large volumes of data to identify patterns and uncover suspicious activity. Velocity alerts are used to create real-time notifications of specific patterns or activity that are known to be suspicious. With fraudsters increasing the use of generative AI, even more patterns emerge in their attacks.

While AI can streamline fraud management and help fast-track trusted identities, there still needs to be human oversight. Human fraud experts bring transparency, oversight, and

continuous improvement to AI which will improve machine learning models and increase protection.

I expect the threat landscape to move pretty fast over the next several years. AI offers new efficiencies and the ability to monitor much larger data sets. This will allow businesses to better combat the continuously evolving use of generative AI for fraud and identity theft.