Merchant Fraud Journal

# Generative AI Fraud Prevention: A Checklist for SMB Companies

Sponsored by FraudLabs Pro

FRAUDLABS PRO

www.merchantfraudjournal.com

# Table of Contents

## Generative AI Fraud Prevention: A Checklist for SMB Companies

Generative artificial intelligence (GAI) has exploded in popularity. It is hard to fathom the sheer magnitude of growth this type of AI experienced in recent years.

For context, the market value for generative tools jumped by an astonishing 100% growth rate between 2001 and 2023. Total users of AI tools surpassed 250 million in 2023, more than double the 2020 numbers. And the global generative AI market is valued at 45 billion in 2023, with expectations of $206 billion by 2030.

There is little wonder why McKinsey labeled 2023 the “break out year” of generative AI tools.

Such rapid acceptance of AI fundamentally alters the fraud economy. In essence, cognitive machines “democratize” fraud. Individuals (who before had few resources) now have easy access to a potent technology. Low-tech criminals can leverage GAI technology to enact sophisticated crimes. Not only did the pool of potential fraudsters expand, but so did the complexity of their schemes.

Luckily, generative AI also supports fraud prevention. Compared to static fraud tools, GAI offers new advancements in security protection. For example, you could use AI to develop simulations of possible attacks. Or think of smart algorithms and how they improve facial recognition. And cognitive machines can automate defenses, helping you scale.

In fact, the same type of democratization of fraud occurs for fraud prevention. Before, only large enterprises had the resources to build and deploy complex fraud tools. Now, companies of any size can access the benefits of generative AI.

That has specific applications to Small to Medium Sized Businesses (SMBs). High-quality fraud prevention is accessible—if you take the time to harness the benefits of generative AI. Of course, such tools also present risks, which any SMB should prepare for.

Let's explore generative AI fraud prevention and the steps merchants can take to prepare for AI-powered fraud.

## What is the relationship between generative AI and fraud?

Generative AI itself is neither good nor bad. As a tool, it simply offers new ways to manage data. Creative machines can take inputs and “generate” original content. It is a form of augmentation meant to simulate human creativity.
AI-powered generation has several positive applications. Machines can convert text to images, a type of data synthesis with many use cases in art or film. It can take large datasets and formulate predictions, a key benefit in the business world. Or it can replicate human speech, as seen with AI-driven chatbots in customer service.

But that same potential found within generative tools is exploited by criminals. Fraudsters can harness novel AI for nefarious purposes.

The most obvious example is synthetic fraud. Criminals no longer need to steal a credit card to assume an identity. Instead, they can simply generate that data with AI. Viable names, addresses, and social security numbers are easy to fabricate.

Or consider "Frankenstein IDs", cards with a mix of true and fake data elements designed to trick security systems. Already, American lenders have given $3 billion to nonexistent synthetic identities.

Another avenue of generative AI fraud involves the creation of fake content. There has been a 10x jump in detected deep fakes (digitally altered faces or bodies) between 2022 and 2023. Plus, AI can replicate the sound of your voice from telephone calls. And it can forge documents, such as bank statements or government releases.

The type and variety of AI-powered schemes are endless. Some fraudsters create synthetic fingerprints. Some will attempt to alter current financial data. Hackers use adversarial networks to map out system vulnerabilities and engage in large-scale data breaches. Smart algorithms drive new forms of fraud.

In summary, generative AI manipulates existing data. That manipulation, when used with an illegal intent, leads to fraud. Bad actors leverage the creative capabilities of AI to improve the execution of criminal activity. The basic fraud scheme, when armed with synthetic intelligence, becomes a sophisticated attack.

## What are some of the new strategic advantages generative AI will give to fraudsters?

No one wants to put a tool that increases the speed and velocity of fraud into the hands of criminals. But generative AI is a present technology that empowers whoever uses it—regardless of intent or motivation. That technical empowerment gives the average criminal several strategic advantages when it comes to perpetrating fraud:

- **Global collaboration:** First, gen-AI supports coordination between fraudsters. Fraud-as-a-Service (FaaS) is already on the rise, with 56% of fraud analysts citing activity from fraud rings in 2023. Digital tools are easy to share, and fraudsters can work together to develop AI-powered fraud schemes. Knowledge of successful attacks will spread quickly, leading to wide-scale deployments by many fraudsters. AI allows the lone criminal to benefit from the experiences of other fraudsters.

- **Speed of exploitation:** Second, AI tools increase the rate of fraud. Fraudsters can now automate several time-consuming tasks (i.e. content creation). GAI algorithms can also adapt in real-time to fraud countermeasures. Or consider the malicious use of chatbots to deceive unsuspecting victims. Gen-AI ramps up the speed and volume of fraud attacks.

- **Personalized attacks:** Third, generative AI enables fraudsters to customize their scams. Think of smart tools that can search through social media pages, chats, and shopping purchases. With a detailed victim profile, the same tool can write scripts, videos, and other custom content that trick the targeted user. For example, a Hong Kong company lost $25.6 million in such a scam. Fraudsters sent a deepfake video of the CEO, visual content that fully mimicked the voices and faces of all executives. The chosen employee, who believed they received a real video call from their boss, sent the money transfer. GAI will supercharge all social-engineering scams with high-quality personalization.

- **Vulnerability detection:** Fourth, AI lets criminals synthesize vast amounts of data and detect intricate patterns. That makes it far easier for bad actors to discover security flaws. For example, consider password spraying. It is a brute force attack, where fraudsters apply thousands of passwords or usernames in hopes of finding account access. Even with a password generator, the process is tedious. But with generative AI, the tool can search the internet to find contextual information (language, history, etc) about a user. That data helps find weak passwords and lowers the time to hack the passcodes. The computing power of generative AI allows criminals to pinpoint and exploit hidden vulnerabilities.

- **Adaptation to defenses:** Fifth, generative AI helps criminals develop countermeasures to security defenses. For example, a security team might tag a malware signature to limit any damage. To counter that security countermeasure, hackers then use gen-AI to create infinite malware versions with an infinite number of signatures. Such malware can persist much longer as security teams struggle to control and tag the numerous variations. The scale of gen-AI gives fraudsters access to advanced evasion techniques.

- **Ease of use:** Sixth, generative AI simplifies or removes technical barriers. When deployed with malicious intent, everyday criminals can now commit fraud with minimal effort. For example, consider WormGPT or the aptly named FraudGPT, two versions of ChatGPT free of all ethical boundaries. Would-be fraudsters can use these Large Language Model (LLM) generative AI chatbots as an automated fraud service. Simply make a request and receive phishing emails, malware code, and other scams. Weaponized AI offers low-effort modes of attack.

## Why generative AI is a problem for non-enterprise merchants

Clearly, generative AI offers new avenues of attack for criminals. Unfortunately, non-enterprise companies will feel a disproportionate impact from this grand change in the fraud economy. There are several reasons why:

### Lack of resources

Small to Medium-Sized Businesses (SMBs) typically have fewer resources to draw upon. That includes financial, technical, and human resource assets. Local outfits usually operate with less-advanced systems, exposing them to more complex GAI-enabled fraud. Tighter margins mean there are limited financial measures to fight fraud. And with small teams of employees, a non-enterprise business is underequipped—forget about creating dedicated fraud defense teams typical of large corporations.

But fraudsters do not scale down their scams. Instead, non-enterprise organizations present easy targets. Criminals know that small teams armed with manual defenses cannot handle the brute force of high-volume attacks. The Association of Fraud Defenders noted such a correlation, stating in 2023 that small businesses had the highest median fraud losses (and that those losses carry a more significant impact on smaller enterprises).

### Lack of specialized knowledge

Second, non-enterprise companies have less access to expertise. Gen-AI is a nascent technical field with complex use cases—that environment contributes to a known talent shortage. Yes, the tool started in the 1960s but only recently reached mainstream awareness (ChatGPT released for public use on November 30, 2022).

As a result, Deloitte notes that 68% of US companies have a moderate to extreme AI skills gap. The University of Oxford reports a nine-fold increase in demand for AI skills between 2015-2022. Generative AI job listings jumped by 306% in one year as of November 2023.

Unfortunately, small businesses do not have education offerings, intellectual/technical property, or finances to develop in-house talent. Large organizations will likely take the best in the field (and have already lowered experience requirements to entice recruits). Non-enterprise companies will be the last to find or hire AI cybersecurity experts. That exposes SMBs to more GAI-enabled scams.

### Limited access to data

Third, small organizations do not have the same volume of defensive data. AI finds vulnerabilities by processing large quantities of information. Smaller teams working in isolation do not have enough data—and cannot process it fast enough—to understand and respond effectively.

As a reference, Chat GPT-3 by OpenAI consumes nearly 175 billion parameters to perform its tasks. And training generative AI over millions of pictures (necessary for image-based generative AI tools), would require many terabytes of data storage. Non-enterprise companies do not have the computing power to build fraud defenses that defeat GAI-enabled fraud.

## Reliance on reactive defense measures

Fourth, non-enterprise companies often cannot adapt their defenses according to the speed of fraudsters.

Speed is critical for any defense posture. Timely detection and data retrieval limit financial damage. Swift containment prevents escalation. Customers value organizational speed to protect their accounts. Speedy responses let organizations adopt security patches and countermeasures against evolving threats.

But without the resources, data, and automated tools, most companies play a constant game of "catch up". At best, smaller outfits do what they can to survive, using reactive solutions to address attacks as they occur (not before). Defenses deployed after the fact come with far greater risk, causing reputational damage and extended financial losses.

## Consumer expectations and business reputation impact

Lastly, non-enterprise companies typically have a closer proximity to consumers. Direct interactions with local customers introduces more fraud risk, as fraudsters love to target humans (and their endpoint devices). Such a customer-facing business model exposes SMBs to GAI-enabled attacks.
And yet, consumers expect the same amount of security from a small business as an enterprise company—even if your team is not nearly as robust. If customers do not feel secure, your customer experience suffers significantly.

That has an extended impact on your business reputation. A lack of trust hurts local businesses that rely on positive word of mouth within small communities. SMBs lose significant lifetime sales value if a fraud scheme results in the loss of a priority client.

## How can you recognize the vulnerabilities your business currently has?

AI-enabled fraud means new defenses are needed. The industry must adapt to such wide-reaching changes within the fraud economy. Luckily, there are several known steps you can take. Here are some common ways to assess your defense posture:

- **Analyze your own transaction data:** Every business has a different customer base. That means you will experience fraud under unique circumstances.

  However, with data analysis, you can find the patterns that indicate fraud at your store. You can understand your specific vulnerabilities and take steps to fix such weak points. It is a proactive solution that uses historical data to better prepare for incoming attacks. Train your data solutions to look for signs typical of generative AI-powered attacks.

  Happily, such efforts also offer a productivity gain. Nvidia built a generative AI agent to assess software containers for vulnerabilities, and it sped up human analysis tasks by 4x.

- **Adapt your defenses post-attack:** Fraud attacks also present a learning opportunity. No one exposes security flaws better than criminals themselves. The minute you discover a data breach, a case of internal fraud, or the presence of false AI-generated content, take steps to patch such vulnerabilities.

  Fraud happens—those willing to assess their faults and make changes after an attack build a robust defense posture.

- **Benefit from the knowledge and experiences of other companies:** Fraudsters use generative AI to benefit from the knowledge of other fraudsters. You can do the same. Tap into the data of neighboring organizations and their fraud prevention programs.

  Data sharing on a large scale also presents an ideal solution for the issues related to margin-tight businesses. Large organizations have a wealth of high-quality data that most smaller outfits would have no hope of collecting on their own. But with intercompany data sharing, all industry players can access the appropriate data needed to prepare against unknown threats. When a new scam emerges, the entire industry can adapt, an act of collaborative protection.

  As proof, recent score risk profiles created by a data consortium identified up to 80% of fraud within a system. Protect your company from gen-AI scams by leveraging the data of partner companies.

- **Monitor:** Discover vulnerabilities with real-time monitoring tools. These data solutions constantly assess your business and consumer operations for suspicious activity.

Non-stop security evaluations provide the obvious benefits of detection and speed (a digital security guard that works 24/7 can catch more fraud). But more importantly, as you use AI monitoring tools, they define behavior thresholds. They will describe the criminal patterns that have a high likelihood of fraud. Insights of this kind point to weak points in your defense strategy that you can fix.

- **Use AI to defeat AI:** Preventive AI-powered algorithms can help you assess and patch security flaws.

  For example, AI defense tools can cross-reference customer behavior, banking data, public databases, and your own business data to find anomalies. Or think about biometric data (processed by AI) to shore up identification. Advanced solutions can also detect genuine consumer actions versus generated or synthetic activity.

  Just as criminals use generative AI for nefarious means, you can use AI tools to seek out vulnerabilties. Use GAI to conduct risk assessments, detect patterns, simulate fraud scenarios, and detect fraudsters in real time.

## Merchant Checklist: Generative AI Fraud Prevention

A good vulnerability assessment will expose flaws in your security profile. But what should you do to actually defend yourself from generative AI-enabled fraud? Use the following action steps to protect your business and customers:

- **Educate staff:** Generative AI brings about new forms of fraud. Many employees will need training in order to identify and deflect novel AI-enabled scams, such as synthetic identities, deep fakes, and forgeries. If possible, bring in experts to conduct seminars and workshops.

- **Collaborate with peers:** AI-enabled fraud is too complex for a siloed business to manage. Instead, connect with vendors, technical services, and fraud solution providers. The community-based approach allows you to leverage the expertise and skill of AI-specialized services. More importantly, a network of trusted partners connects you to important shared data and threat intelligence.

- **Stay informed:** The speed and velocity of fraud continues to increase. To stay up-to-date, research industry news, cybersecurity reports, and governmental regulations related to generative AI. Efforts of this kind will also help you stay compliant as regulators adapt the rules to the changing conditions of fraud.

- **Take proactive action:** Don't hesitate to shore up your defenses. Once you become aware of an emergent threat—take action. Voice spoofing, adversarial attacks, altered content, and AI-powered phishing are current AI-generated fraud trends that you can address. Protect your business now, not after a fraud attack.

- **Continuously improve:** Fraudsters continue to evolve in sophistication and ability. Good defense demands vigilance. That means conducting regular audits. Or bring in specialists to search for weakpoints. Develop processes that can match the ever-changing exploits of criminals. Even better, use the adaptive capabilities of AI to help support customized fraud models.

- **Deploy use cases of generative AI:** Just as AI enhances the capabilities of fraudsters, you can also use the tool as a defensive weapon There are already code scanners for AI models. AI can conduct continuous authentication to improve verification, ranging from voice, facial, and user behavior recognition. Generative AI can conduct dynamic access controls. You can train your systems with synthetic fraud scenarios so that your fraud tools better detect incoming fraud threats. The opportunities are vast: identify use cases and integrate AI into your fraud detection systems.

- **Scale:** Once deployed, automate your GAI-enabled fraud prevention. AI excels in managing large volumes of data. That simplifies scaling and will help protect your business as you grow.

## Using AI To Protect Your Business

For many, preparing for generative AI can seem like an insurmountable task. With zero training, the technical nature of any AI tool can appear foreign and complex. Generative AI uses machine learning models that require expertise to implement. Such tools also demand large volumes of input data and depend upon well-built data systems.

Plus, there are regulatory concerns. And you must integrate these tools into existing business systems, a task that often includes compatibility problems. Applying AI to fraud prevention can be a challenging task.

What can a non-enterprise company do to address such challenges? Four basic strategies can help simplify AI adoption:

- **Use pre-built solutions:** Pre-trained models come with simple interfaces and easy integration capabilities. This makes it simple to leverage the benefits of AI with less hassle.

- **Hire expert partners:** Experienced professionals offer the insights and guidance needed for an effective integration process.

- **Start small:** Deploy AI in simple use cases. It is an ideal way to determine the feasibility with a shorter timetable and return on investment.

- **Iterate and improve:** With several viable use cases, slowly scale according to need. That gives you time to test new applications without too much risk exposure.

## How does FraudLabs Pro help you to protect your business?

At Hexasoft, we are aware of these AI adoption challenges. That's why we offer specialized guidance regarding your digital transformation. We guide you through the entire process of integrating AI-powered fraud defenses.

More specifically, we leverage FraudLabs Pro. With its advanced algorithms, FraudLabs Pro provides unparalleled security via the following features:

- **Comprehensive fraud validation:** Fraudlabs Pro includes several validation services that can detect malicious fraud with high levels of accuracy.

  For example, incoming orders must pass blacklist, credit card, user account, and device validations. Machine learning compares data patterns against defined algorithms, leading to better fraud predictions. Validations are custom-built, occur in real-time, and integrate with all leading e-commerce platforms. Machine learning also regularly engages in data analysis of all transaction data to identify and predict fraudulent behavior.

- **Global merchant network: Fraudlabs** Pro connects with other merchants, that way you can access the benefits of data sharing. Gain the collective knowledge of a worldwide network to better identify and adapt to emerging threats.

- **Accurate IP geolocation detection powered by IP2Location:** Fraudlabs Pro provides IP and proxy detection to gather non-intrusive geolocation information. The tools extract relevant data so AI can learn patterns related to IP and proxy server usage. Suspicious IP addresses are blocked or require additional verification.

  For example, imagine an American customer making a surprise order from an IP address in Europe. That deviation from the expected location can prompt a fraud alert. The tool gives you a complete understanding of where your traffic is coming from.

- **Email verification powered by MailboxValidator:** Fraudlabs Pro uses Mailboxvalidator to verify the legitimacy of all emails. It can detect fake addresses and accounts by requesting authentication of ownership. That limits the avenues fraudsters can use to enact their schemes—especially social engineered scams generated by AI.

## Conclusion:

The rise of generative AI presents unprecedented opportunities—for both fraudsters and honest businesses. Looking to the future, generative AI features stand to add up to $4.4 trillion to the global economy annually. And experts estimate that gen AI will perform at a median level of human performance by the end of this decade. The benefits and drawbacks of AI will almost certainly characterize the fraud economy in the upcoming years.

Already, we are feeling those effects. Fraudsters have used AI to bypass traditional protections, creating novel scams from deepfake voice authentication to synthetic identity generation. Smart tools offer alarming ease and efficiency when it comes to perpetrating fraud.

In turn, merchants and enterprises are taking proactive steps to protect themselves. For example, Mastercard uses new AI-based transaction decisioning technology to improve fraud detection rates by 20% (and in some instances by 300%). Data sharing has helped turn the industry toward community-based defenses. And simple uses like AI-built fraud scenarios or dynamic access controls are now common defense strategies.

In short, generative AI offers early adopters a competitive edge. Those who integrate AI within their fraud defenses will have a clear advantage, especially in the face of AI-powered attacks. AI adoption and usage will only grow—organizations prepared for the pitfalls of GAI-enabled fraud will limit the negative fallout. With smart fraud prevention, Merchants can stay one step ahead of fraudsters and protect their businesses from the ever-changing landscape of generative AI-enabled scams.

*“If everyone is moving forward together, success takes care of itself”*

**Henry Ford**

# About MFJ

Merchant Fraud Journal is an independent and unbiased publication dedicated to empowering online sellers to greatly reduce the impact of eCommerce fraud on their businesses. Its core mission is to break the silos surrounding merchants' internal fraud prevention processes by bringing together industry professionals to share their knowledge with one another.

Unfortunately, the business process knowledge needed for online sellers to greatly reduce the impact of eCommerce fraud is scarcely available right now. There is no single forum and resource where merchants, payment professionals, and other industry professionals could go to get educated on the myriad of challenges they face.

We seek to fill that gap by being a resource that collects insight from industry thought leaders and fraud prevention tool experts on topics such as chargebacks, false positive declines, account takeover fraud, friendly fraud, data breaches and more. Our goal is to help honest businesses quickly understand their security options and take action, so they can get back to focusing on their core business activities.

# About FraudLabs Pro

FraudLabs Pro is a leading fraud prevention solution provider that helps online businesses to detect and prevent fraudulent transactions. Our mission is to empower businesses with advanced fraud detection tools to minimize financial losses and chargebacks. With our cutting-edge technology and comprehensive suite of fraud detection tools, we enable businesses to protect their revenue, reputation, and customers.

FraudLabs Pro offers key features like:

Fraud Scoring: Analyzes various elements (data points) like IP geolocation, email address, proxy information, credit card information, transaction history, and many more, to calculate and assign a risk score to each transaction.
Customizable Validation Rules: Enables businesses to set up their own fraud validation rules to target specific fraudulent activities.
Global Merchant Network: Leverages a vast network of merchants to share fraud data and patterns, enhancing overall detection and prevention.
FraudLabs Pro also offers a free Micro plan, allowing businesses to start protecting themselves from fraudulent activities without any initial investment.

For additional information about FraudLabs Pro,
please visit www.fraudlabspro.com

FRAUDLABS PRO

**Contact Merchant Fraud Journal**
Editor In Chief - Bradley Chalupski
Bradley@merchantfraudjouranl.com

**Contact FraudLabs Pro**
www.fraudlabspro.com
support@fraudlabspro.com

Merchant
Fraud
Journal

290 Caldari Road,
Concord, Ontario L4K 4J4
Canada
--

hello@merchantfraudjournal.com

www.merchantfraudjournal.com

1-(888) 225-2909