Generative AI and the future of scams

A game-changing shift for banks

The better the question.
The better the answer.
The better the world works.

feedzai

EY
Shape the future
with confidence

EXECUTIVE SUMMARY

In brief

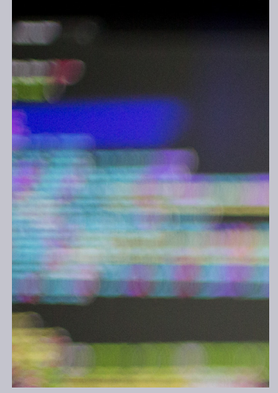
Generative AI (GenAI) is rapidly transforming the fraud landscape for banks. Traditional fraud defenses are proving insufficient as fraudsters leverage scams, including through the use of GenAI, to manipulate customers into authorizing fraudulent transactions. This article, written in collaboration between EY Canada and Feedzai, explores how AI and GenAI are game changers in the fight against scams and offers insights into how banks can innovate to stay ahead.

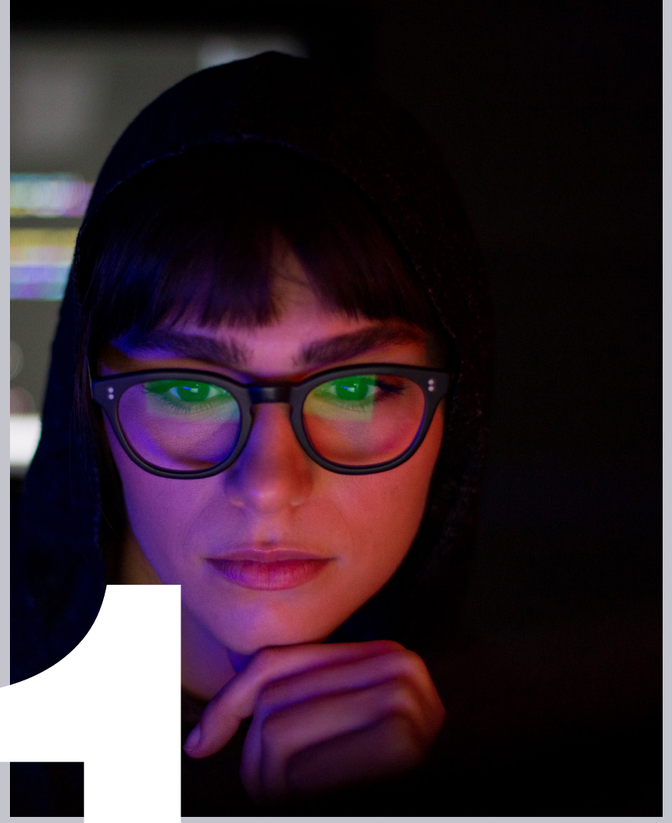
AI can shield against scams, but GenAI can be misused by fraudsters too.

Banks can retain customers and avoid negative outcomes by effectively managing scam fraud; UK leads with consumer protection regulations.

Banks should blend AI with expert judgment for thorough fraud prevention and customer safety.

Content





SECTION 01

Scams: a growing challenge for traditional fraud defenses

Scams have emerged as a major challenge for banks as fraudsters evolve tactics and take advantage of technological advancements. The days when banks could rely on traditional fraud defenses—such as rules-based detection systems and generic customer education—are rapidly fading. Criminals now bypass these defenses by directly targeting customers through scams like impersonation, romance, investment, and cryptocurrency fraud. This shift has led to a steep decline in fraud detection rates, with the majority of scams slipping through the cracks undetected.

Why have scams become such a challenge?

With scams that involve customers unknowingly authorizing fraudulent transactions, traditional fraud management solutions are often less effective. These scams, unlike typical fraud attempts, aren't easily flagged by fraud detection systems because the transactions appear to be authorized by legitimate account holders.

The impact is devastating, not only to the individuals being scammed but also to the banks involved. As scams increase in complexity and volume, financial institutions are finding it harder to keep up. These challenges require banks to rethink their fraud strategies and adapt to a more holistic approach that encompasses tailored customer education, real-time monitoring, and advanced AI solutions.

The impact of scams

Scams don't just harm customers; they pose a multi-dimensional threat to banks as well. The financial, emotional, and reputational impacts of these crimes are significant and often underestimated.

Emotional impact 01/03

Scammed customers often experience shame and embarrassment, which discourages them from reporting incidents. This low reporting rate leaves banks without critical data needed to understand and respond to evolving scam tactics.

Financial impact 02/03

Scams can have devastating financial consequences on customers when a decision is made to not reimburse them. In the cases where scams victims are being reimbursed, scams can have a significant impact on banks' fraud losses.

Reputational impact 03/03

The reputational damage from scams can be immense. If a bank is perceived as unsupportive or unresponsive when dealing with scam victims, they risk customer attrition, negative press, and even legal action. In a highly competitive market, this can have long-term effects on customer trust and loyalty.

How Fraudsters Are Leveraging GenAI and AI

The rapid adoption of GenAI is proving to be a game-changer for criminals. Fraudsters have become the fastest adopters of new technology, and they face none of the regulatory or privacy constraints that hinder legitimate businesses. With GenAI, fraudsters can scale their operations with unprecedented speed and precision, creating more sophisticated scams that bypass traditional security measures.

Here are several ways criminals are leveraging GenAI to challenge banks:

Lowering the barrier to entry

GenAI makes it easier for criminals to execute complex scams without needing advanced skills. They no longer need to spell or write well, or even speak the victim's language. GenAI tools can generate and send phishing messages in multiple languages, 24/7, making scams more scalable.

Mimicking voices

GenAI's ability to mimic voices is alarming. Scammers are using it for CEO fraud, where they can impersonate a company leader's voice on phone calls to authorize fraudulent payments. In another example, a woman in Arizona received a call where she heard what sounded like her daughter screaming for help—generated using just a few seconds of her daughter's voice from social media.

Deepfake videos

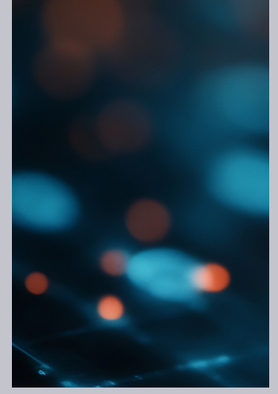
Criminals have begun using deepfake videos to deceive victims. A notable case involved a tech company employee who received a video call from someone who appeared to be their CFO, but it was a deepfake. Deepfakes have also been used to create disruptive content, such as a fake video of the Pentagon on fire, which caused market panic.

Scaling traditional crimes

GenAI can enhance traditional scams like phishing or email impersonation. Messages from impersonated relatives or C-suite executives have become more convincing, which leads to a higher success rate, even with low response rates.

Synthetic data & security attacks

With GenAI, criminals can create synthetic data that closely resembles legitimate transactions, making it much harder for traditional fraud detection systems to flag them. They can also launch sophisticated AI security attacks, such as injecting malicious input into a bank's model training data or using prompt injections to manipulate AI models.

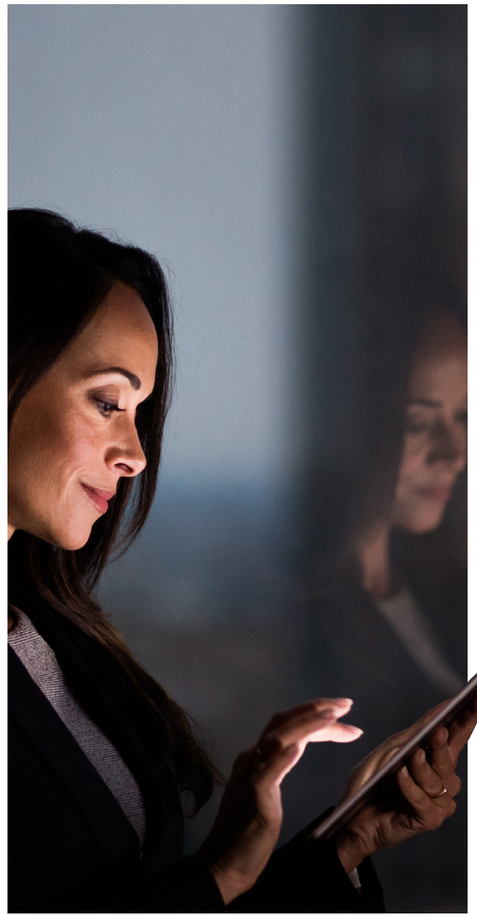


SECTION 02

Why AI and GenAI are game changers in the fight against scams

Artificial intelligence (AI) has played an important role in fraud risk management for decades, helping financial institutions improve detection and prevention strategies. However, the rise of increasingly sophisticated scams has exposed the limitations of traditional defenses such as authentication systems, rule-based decisioning, device profiling, and biometrics. While effective for some types of fraud, these methods are falling short when it comes to preventing scams. The question isn't whether banks should continue to evolve their approach—it's how quickly they can adopt the right innovations, including expanding the use of AI in fraud prevention, detection and response to keep pace with these new threats.

The time is now for banks to raise the bar on their ability to collaborate, prioritize the consumer relationship, and embrace new technologies like AI and GenAI. These technologies aren't just incremental improvements—they represent a fundamental shift in how we approach fraud risk management. Through innovation and collaboration, financial institutions can proactively prevent scams before they occur.



Traditional fraud risk management is no longer enough

While traditional fraud risk management methods have been effective in many cases, they struggle against scams that rely on social engineering and customer manipulation. While still important, these tactics are reactive and often unable to address the nuances of scams where customers unknowingly authorize fraudulent transactions.

Scams, particularly impersonation, investment, and romance scams, exploit the trust that exists between customers and their banks. To tackle these challenges, banks must shift from reactive fraud defenses to proactive fraud prevention, leveraging AI to stay ahead of evolving threats.

AI and GenAI: the future of scam prevention

AI and GenAI are the real game changers in scam prevention. By expanding the use of these technologies, banks can enhance their existing fraud defenses and pioneer new ways to protect their customers.

Collaboration is essential. Banks must collaborate, sharing insights and data to create more resilient defenses. Prioritizing the customer relationship is key, ensuring that fraud prevention strategies are centered around the consumer's experience and trust. Finally, AI and GenAI are innovative technologies that can take scam prevention to the next level.

Demystifying GenAI: key use cases

GenAI holds immense potential in the fight against scams. Here are some of the ways it can be applied:

Synthetic data generation 01/07

Fraud detection systems often struggle due to unbalanced datasets. GenAI excels at generating synthetic data, which is invaluable for augmenting datasets where there is a lack of high-quality data or labeled examples. This helps fraud models better recognize and flag fraudulent activity, even in low-frequency events like emerging scams.

Adversarial training 02/07

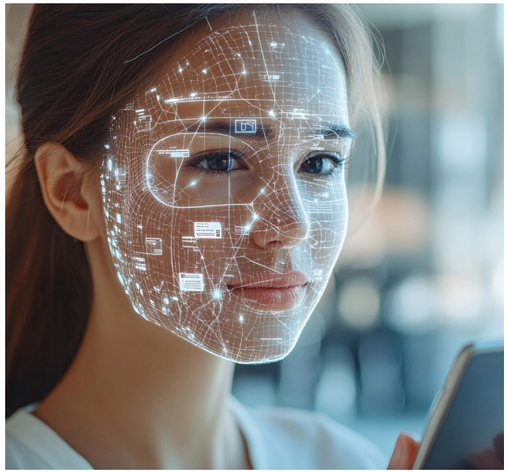
GenAI can simulate synthetic attacks, allowing fraud models to be stress-tested against potential future threats. This method not only strengthens the model's defenses but also reduce bias risk, which is critical in maintaining customer trust.

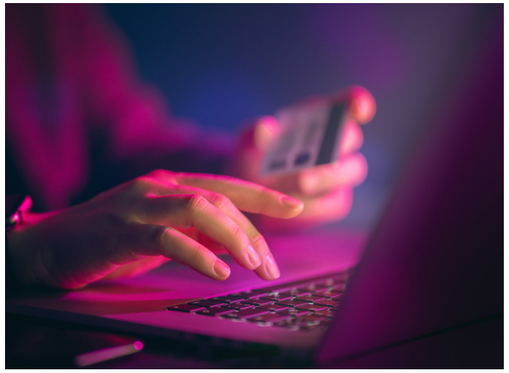
Anomaly detection and remediation 03/07

AI has proven effective in identifying anomalies within quantitative data, and GenAI further enhances these capabilities. It improves the performance and efficiency of fraud detection models, ultimately leading to better customer outcomes by reducing false positives and streamlining the remediation process.

Authentication 04/07

GenAI can generate advanced behavioral profiles for users, identifying subtle signs of suspicious activity, such as abnormal typing speed, navigation habits, or location inconsistencies. This allows banks to detect and prevent unauthorized access or account takeover attempts before they escalate while also ensuring that legitimate customers experience minimal friction during their interactions.





Threat modeling 05/07

GenAI can be used to create simulated fraud attacks or scam scenarios that banks might face in the future. By generating these complex, realistic threats, banks can proactively test their existing fraud defenses. This process, known as threat modeling, helps banks identify potential weaknesses in their systems before real criminals exploit them.

In short, GenAI allows banks to "practice" defending against new, emerging fraud techniques, helping them stay ahead of evolving threats and be better prepared for future fraud attempts.

Automating the investigation process 06/07

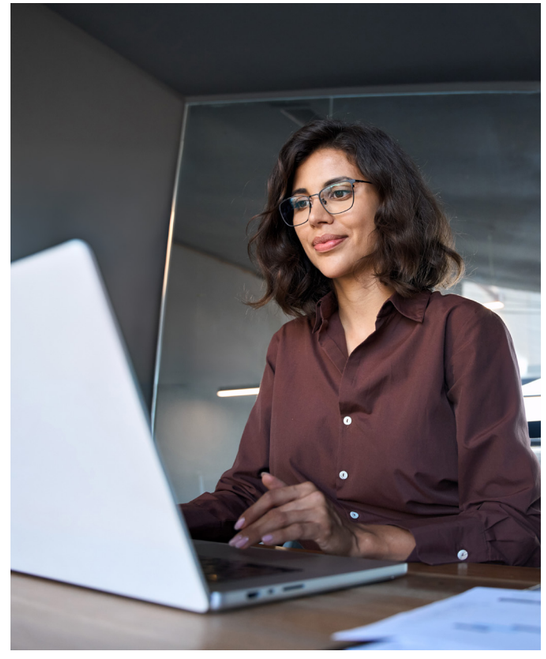
AI models can streamline the case management process in fraud investigations by automating time-consuming, repetitive tasks. For example, instead of investigators manually gathering data, analyzing it, or creating reports, AI can do these routine activities. This allows investigators to focus on more complex, high-priority cases where human judgment and expertise are needed, making the overall process faster and more efficient.

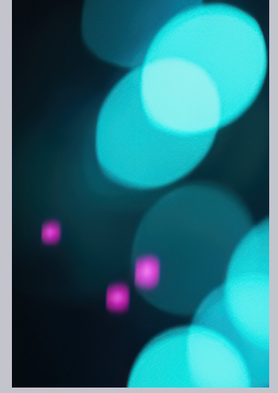
Model documentation 07/07

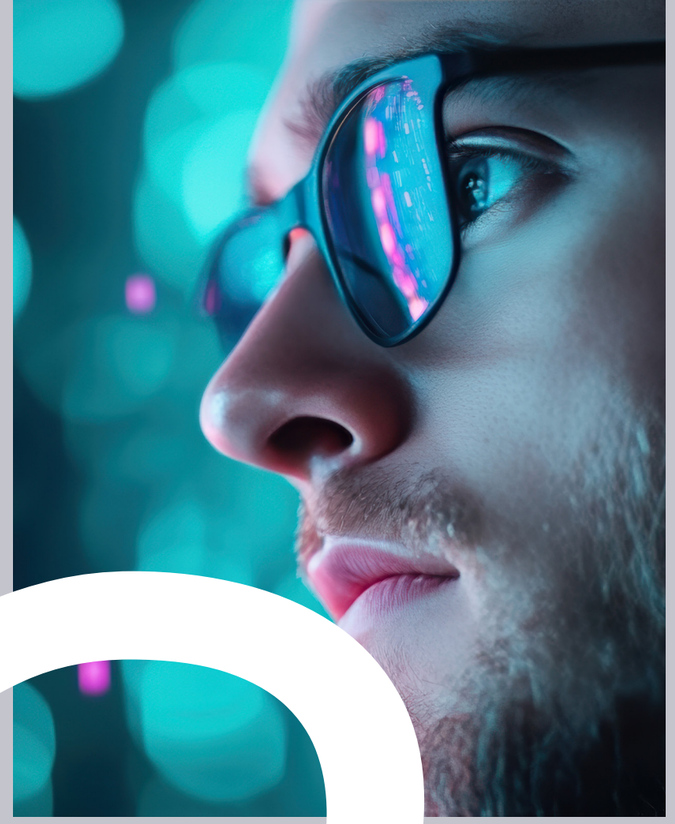
AI simplifies the model documentation process by automatically generating detailed records of how a model is built, tested, and operates. This documentation is essential for meeting regulatory requirements which mandates transparency and accountability in how financial institutions use AI models.

Typically, manually creating this documentation can take days or weeks, as it involves tracking various technical aspects of the model's development and performance. AI automates much of this work by logging data, modeling decisions, and processes, reducing what used to take a week to just a few hours. This automation frees up teams to focus on more strategic tasks while still ensuring regulatory compliance.

A top-tier bank has already implemented this technology, reducing what used to be a week's worth of work to just a few hours.







SECTION 03

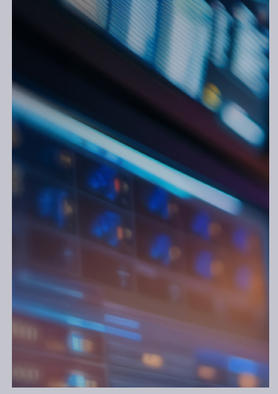
The path forward for banks in fraud prevention

As fraud tactics evolve, financial institutions must adapt by increasing their use of AI—not just GenAI—in fraud risk management across prevention, detection, and response. AI can provide powerful insights and automate tasks, but it must be integrated thoughtfully into a bank's strategy. It is key to prioritize innovative use cases and iterate based on lessons learned. By testing and refining AI applications, banks can continuously deliver tangible benefits while staying ahead of evolving threats.

However, humans remain central to this technological innovation. AI doesn't replace fraud professionals; it enhances their work, allowing them to focus on more complex, high-value tasks. As GenAI advances, both good and bad actors will continue to innovate. The challenge will be to find positive uses for GenAI while mitigating the risks.

Banks also need to rethink how they educate customers about scams. Customer communications should be clear and personalized, and front-line employees must be trained to handle potential scams with agility and understanding.

The dynamic nature of GenAI means that both its applications and the defenses against it will evolve rapidly. To stay ahead, banks must remain vigilant, constantly adapting to new advancements and threats. By taking a proactive, human-centered approach to AI, banks can create a safer future for both their customers and their institutions.



SECTION 04

Conclusion

Scams continue to present significant challenges to traditional fraud defenses worldwide, demanding innovative strategies across fraud prevention, detection, and response to mitigate risks effectively. Holding customers liable for scams risks customer attrition and negative press coverage and can also invite regulatory changes, as seen in the UK, where new rules are being implemented to better protect consumers.

While GenAI holds immense potential for improving efficiency, effectiveness, and user experience, its implementation requires continuous vigilance and adaptation to ensure its benefits are realized while minimizing associated risks.

Ultimately, there is no one-size-fits-all solution to fraud risk management, and that applies to AI and GenAI as well.

A holistic approach is essential—one that incorporates AI and GenAI but also considers broader elements like risk assessments, customer and employee fraud awareness, robust authentication, and a comprehensive fraud response. By taking this multifaceted approach, financial institutions will be better positioned to combat scams and protect their customers in the evolving fraud landscape.

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multi-disciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

4625365

ey.com/ca

Feedzai | More Trust, Less Crime.

At Feedzai, we're on a mission to make the world a safer place for commerce, one transaction at a time.

We analyze billions of data points per year, using AI-powered models to detect and prevent fraud in real time. Our RiskOps platform helps institutions achieve compliance, stop illicit activities, and uncover money laundering and organized crime. Think of us as the guardians of your entire financial ecosystem, from onboarding throughout your entire customer journey.

The world's leading financial institutions trust Feedzai to safeguard trillions of dollars of transactions, manage risk, and improve the customer experience.

Identity | Enterprise Fraud Management | Anti-Money Laundering

info@feedzai.com