The imitation game: How GenAI has supercharged fraud

How to deploy a multi-layered approach with a holistic view of the consumer to stay ahead of evolving fraud

What businesses need to know today

- ▷ The rise of Generative AI (GenAI)
- ▷ GenAI impact by fraud type
- ▷ Deepfakes: The authenticity challenge
- ▷ The challenge of detecting synthetic identities
- ▷ Scaling up: The emergence of bot-as-a-service
- ▷ Authorized Push Payment Fraud (APP Fraud)
- ▷ Understanding the role of intent and context in fraud prevention
- ▷ Key takeaways

The rise of Generative AI (GenAI)

There is no question that GenAI's rise to the top has been rapid. According to a report by Bloomberg Intelligence, the GenAI market is forecast to grow to US$1.3 trillion over the next decade at a compound annual growth rate of 42%. It was only last year that GenAI fully emerged in the public domain as an accessible tool, with the technology's impact and expectations reverberating across businesses worldwide.

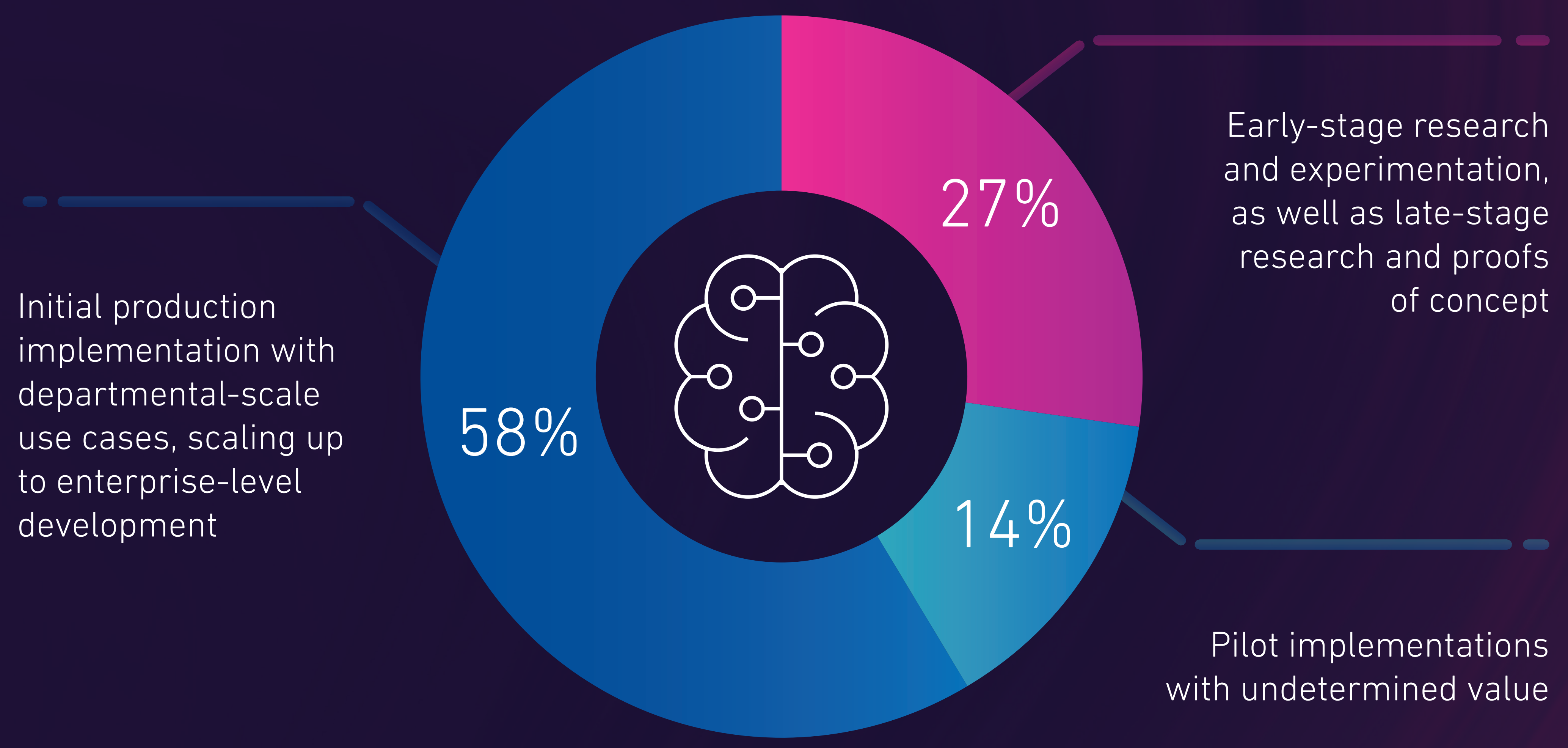
This massive growth trajectory has led some critics to suggest that GenAI is nearing its hype peak*. However, its potential is still unfolding as the technology continues to evolve and be applied to new use cases.

Most organizations are still very early in producing and scaling GenAI applications. Businesses are aware of the vast opportunities and, in parallel with the need to keep pace, are initially focused on simple use cases that can demonstrate quick ROI.

*2023 Gartner Hype Cycle for Emerging Technologies

The GenAI market is forecast to grow to US$1.3 trillion over the next decade

How far has your organization come on its journey of adopting generative AI?



Note: Percentages may not total 100 because of rounding. Base 171 to 272 global business and technology professionals in financial services who have some knowledge of the specified emerging technology. Source: Forrester's Priorities Survey, 2024

GenAI has many potential positive applications, from streamlining business processes to providing creative support for various industries such as architecture, design, or entertainment to significantly impacting healthcare or education. However, it also poses many risks.

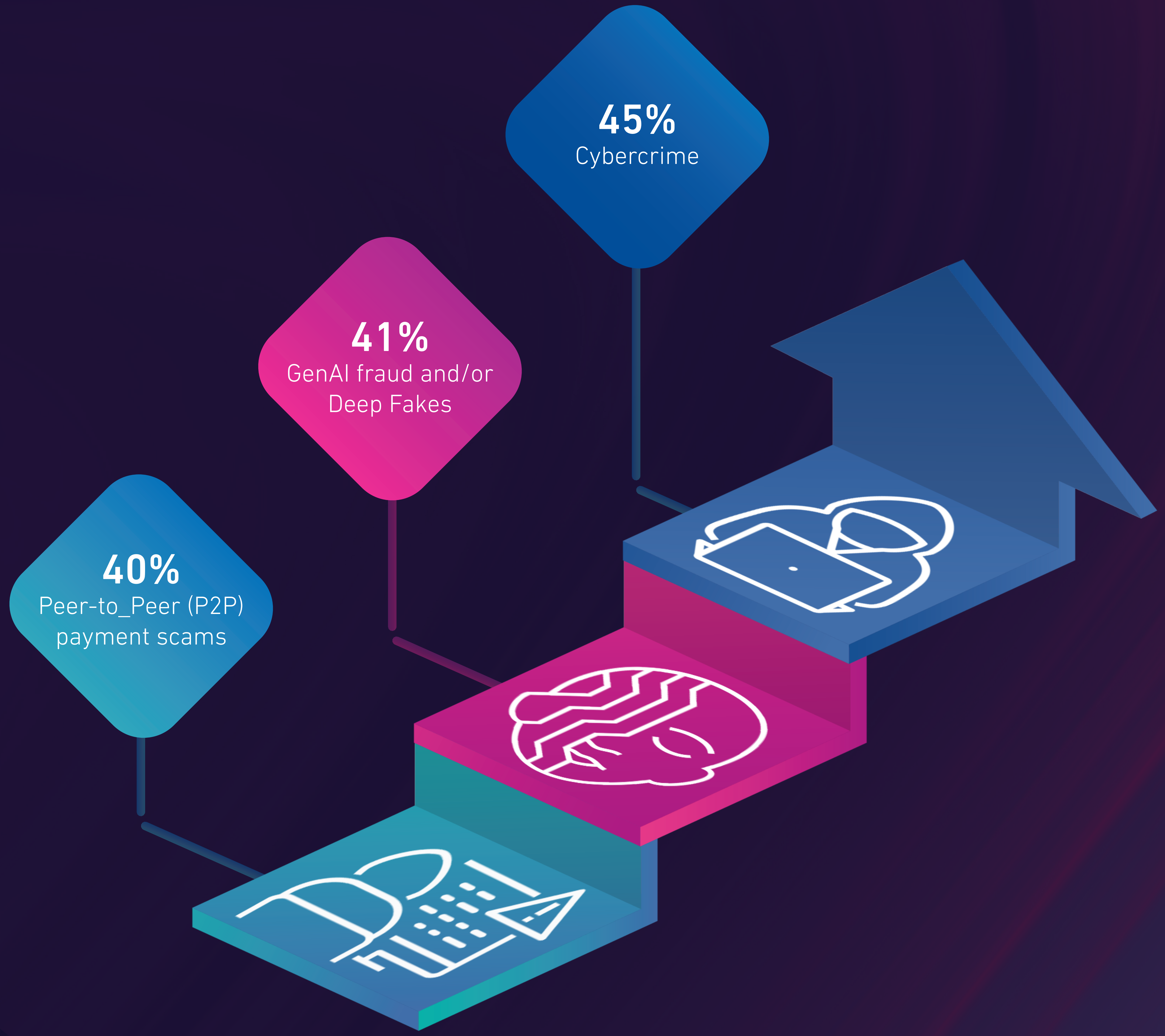
One of the biggest threats is its adoption by criminals to generate synthetic content that can potentially deceive businesses and individuals. Easy-to-use, widely available GenAI tools have created a low barrier of entry for those willing to commit illegal activities. Threat actors leverage GenAI to produce convincing synthetic identities and deepfakes** that include audio, images, and videos that are increasingly sophisticated and practically impossible to differentiate from genuine content without the help of technology. Fraudsters also exploit the power of Large Language Models (LLMs) by creating eloquent chatbots and elaborate phishing emails to help them steal vital information or establish communication with their targets.

According to Experian's latest research, the top three anticipated operational challenges businesses expect to struggle with when it comes to fraud are Cybercrime (45%), Generative AI fraud, and/or Deep Fakes (41%), followed by Peer-to-Peer (P2P) (40%), payment scams, which GenAI increasingly enables.

While it is impossible to gauge the true impact of GenAI on fraud attacks, understanding the implications of this new technology can help businesses mitigate the risk associated with GenAI.

***Deepfake: an image or recording that has been convincingly altered and manipulated to misrepresent someone as doing or saying something that was not actually done or said. Merriam-Webster*

Top three anticipated operational challenges



> GenAI-enabled fraud continues to proliferate: Fraudsters use GenAI tools to manipulate media and engage in automated fraud attacks. Since Q4 2022, there's been a 1,265% increase in malicious phishing emails and a 967% rise in credential phishing. Bad actors generate convincing phishing schemes leveraging GenAI tools like ChatGPT and FraudGPT.

Generative Artificial Intelligence (GenAI) and Fraud, The impact of GenAI on the fraud detection and prevention market, Liminal, March 2024

GenAI impact by fraud type

Authorised Push Payment (APP) fraud

During an APP scam, criminals manipulate their victims into making payments or sharing personal details under false pretences. Often, fraudsters will pose as well-known legitimate businesses or government bodies to win a victim's trust. They gain the trust of their victims by contacting them with convincing emails or messages on social media, deceiving them with synthetically generated pictures, and creating websites with fake adverts.

Phishing/Social engineering

GenAI has made social engineering attempts more convincing by helping criminals write personalized content at scale that appears to be legitimate for emails and messages on social media. They steal personal and financial information to be used later for other types of fraud.

Synthetic identity fraud

GenAI allows for the mass production of documents and PII data, supporting the establishment and trust of synthetic identities. Video injection attacks bypass Know Your Customer (KYC) checks and establish a new identity.

Account takeover (ATO)

Spoof authentication systems with voice, images, or video deepfakes. GenAI can be used to deceive customer support teams to help fraudsters regain access they claim to have lost. It can also be used to carry out impersonations against the actual account holders to steal access details directly from them.

Account opening fraud

Mass production of fake details is used to open new accounts on various platforms, including social media and LinkedIn. Coupled with established identity data and the documents required to set up a new account, attackers are increasingly difficult to differentiate from legitimate consumers.

Deepfakes: The authenticity challenge

Recent advancements in deepfake technology have made it much easier for fraudsters to take advantage of compromised identity data. GenAI is a valuable resource for creating convincing deepfakes, allowing criminals to 'complete' an identity profile with additional attributes such as a face and a voice.

By ensuring a name, address, phone number, and email look like they belong together and adding elements such as a facial image, documents, and voice, fraudsters can bypass the identity authentication requirements that businesses use for everything from government benefits to opening new bank accounts to submitting an eCommerce transaction. Due to GenAI, these interactions appear increasingly legitimate.

Video injection attacks are also an increasing concern for financial institutions, particularly those using Know Your Customer (KYC) systems that employ biometric data, such as video frames of an individual's face, to compare against an identity document.

During identity verification, video injection attacks happen when fraudulent data streams are inserted between the capture device and the biometric feature extractor.

Business problem:

Most individuals cannot spot a deepfake with the human eye, so scams are increasingly effective and can result in significant financial losses.

Most organizations have not deployed technology to identify deepfakes via document and selfie checks. Although these processes increase friction for good customers, they can effectively spot altered images.

How should businesses respond?

- Educate customers about an increase in scams that use deepfakes.
- The weakest link is often a legitimate consumer scammed into transferring funds to a fraudster, making education critical.
- Leverage document verification tools that compare government document images with a liveness detection and selfie check as part of a layered identity authentication solution. Document verification tools are highly effective at identifying deepfake presentations.

The challenge of detecting synthetic identities

The ability to scale fraudulent activity with GenAI is already impacting losses, with synthetic identity fraud emerging as the fastest-growing form of financial crime. According to some estimates, synthetic identity fraud could account for up to 20% of loan and credit card charge-offs, meaning the annual charge-off losses in the US alone tied to synthetics could be closer to $11 billion. Criminals can manipulate the billions of breached identity data records by replicating and synthesizing them to create profiles of human-looking information.

Many businesses in the financial services space have been trying to solve synthetic identity fraud with credit data matching. However, detecting synthetic identities can be difficult and requires multiple tools and resources. Synthetic identity fraud involves creating a partially valid identity and making it slip through the traditional checks and balances of identity verification. In addition, data fragmentation across multiple financial institutions and credit bureaus poses a challenge. A synthetic identity could have relationships with numerous banks and credit card companies. Unless these institutions share information with each other, it's challenging to get a comprehensive view of the suspicious activity.

Annual charge-off losses in the US alone tied to synthetics could be close to $11 Billion.

Business problem:

Organizations struggle to grasp the nature of synthetic identities—how they are created, how they behave, and how they are eventually used to exploit and monetize accounts. Businesses lack visibility of data that can easily separate synthetic from legitimate identities, and that has become increasingly difficult due to GenAI advances.

How should businesses respond?

- Use Generative Adversarial Networks (GANs) to create synthetic data and mimic fraudster behaviors to test identity and fraud controls.
- Leverage consumer credit attributes to help spot typical synthetic indicators, alongside cross-industry networks and identity behavior data.
- User-entered data and device/behavioral/network data provide an incredibly rich set of insights that, when combined, can differentiate between synthetic and authentic identities.

Scaling up:
The emergence of bot-as-a-service

In addition to leveraging GenAI to create more convincing identity attributes using deepfakes, fraudsters can now take advantage of and manipulate data at scale.

Before GenAI became accessible, building a synthetic identity by creating proof-of-life artifacts while leaving evidence of existence with utility bills, mortgages, multiple bank accounts, and established credit profiles was no small feat. GenAI has allowed criminals to scale these activities, using synthetic identities to set up multiple new bank accounts, often undetected. GenAI has impacted the evolution of fraud-as-a-service and, with it, the scaling of fraudulent activities.

Criminals are incredibly organized, networked, and connected. Although human networks are useful to fraudsters, bot-as-a-service is much more efficient. Using GenAI, bots can undertake tasks that had historically required humans, allowing fraudsters to scale activities to levels previously impossible when criminals depended on humans alone.

Automated bots can impersonate businesses to socially engineer consumers. A hired bot can make a thousand calls to consumers they know have a bank account with a specific bank, using a script to interact with that consumer to retrieve additional data.

The fraudster will then use that information to bypass existing authentication controls or get a consumer to submit a fraudulent transfer, all based on an interaction with a bot. The bad actor doesn't need to circumvent any controls because the business believes a legitimate consumer is on the other end. FraudGPT is available for as little as $200 per month , offering criminals a dangerously low entry point to this type of bot-as-a-service attack.

FraudGPT: The recent arrival of malicious large language models, such as FraudGPT, is driving a new wave of social engineering and phishing attacks.

Business problem:

The ease of creating realistic-looking identities with a digital footprint and synthetic proof-of-life trails makes it difficult for businesses with siloed fraud solutions to identify attackers.

How should businesses respond?

Implement a layered solution that brings together multiple dimensions of risk such as identity verification, behavioral biometrics, phone intelligence, document verification, and cross-industry identity behavior, into a single risk model or decision.

This will spot nuanced signals and patterns or detect the presence of bots in staging aspects of the synthetic identity or its use across businesses.

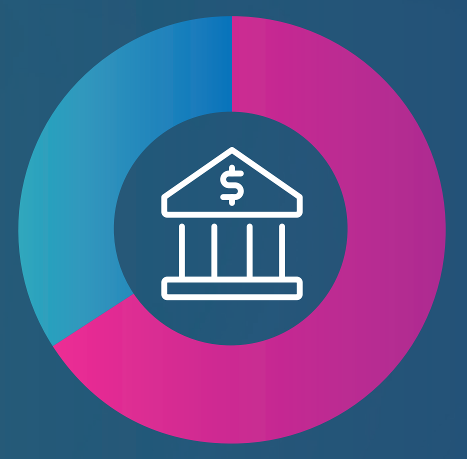
Authorized Push Payment Fraud (APP Fraud)

Faster payments and APP fraud
The speed of real-time payments has presented organizations globally with challenges. While consumers now see instant payments as necessary, on the business side, real-time payments represent a disconnect in recognizing the correlation between speed and lack of control.

APP fraud works by tricking individuals into voluntarily sending money under false pretences and is hugely successful. According to the Global Anti-Scam Alliance (GASA), $1.026 trillion was lost to APP scams between August 2022 and August 2023.

With the help of GenAI and hired bots, criminals can go further and test not only individuals but also whole organizations at scale to understand their processes and controls and discover how best to circumvent those guardrails. They use this intel to drive more fraud attempts in APP fraud.

Better regulations and the ability for businesses to understand the intention behind a transfer are critical in fighting APP fraud. Businesses can protect growth ambitions and consumer expectations for seamless digital interactions by introducing friction to a customer journey when risk is detected. However, social engineering is the weakest link when addressing APP fraud, and the most challenging part to solve.



66.8% of banks have experienced a increase in social engineering attacks over the past two years.

Liminal ATO Prevention in Banking Buyer Survey, March 2024

Our latest research on customer authentication shows that businesses place the most significant emphasis on security measures involving passwords (**44%**) and measures requiring customers to have a secondary device on hand (**42%**). These do little to solve the greatest emerging threats.

Business problem:

Regulatory environments can have massive implications for businesses, particularly where the bank is financially liable for customers' losses due to scams such as APP fraud. As countries review regulations that place financial liability onto banks, financial institutions will increasingly be responsible for fraudulent transfers.

How should businesses respond?

- Introduce targeted friction when high-risk cases are identified, such as adding a transaction push notification to help customers understand the possible consequences of a high-risk transfer.
- Closely monitor and evaluate new technologies and approaches to thwart APP and other GenAI-enabled attacks by complementing traditional identity-focused controls with more digital, behavioral, and cross-industry network/consortium-based services beyond screening typical identity elements or transactional logic.

Example: Deploy services to identify when a consumer is in a live phone call while attempting to make an unusually large transfer to a new payee.

This type of signal could be extremely valuable in identifying a distressed customer or someone being coached by a fraudster or bot. Behavioral analytics signals are also useful in examining how the customer is interacting with the organization's site. Organizations do not have to be blind to this - but most have not deployed these more advanced identity authentication and behavioral tools as part of their layered approach.

Understanding the role of intent and context in fraud prevention

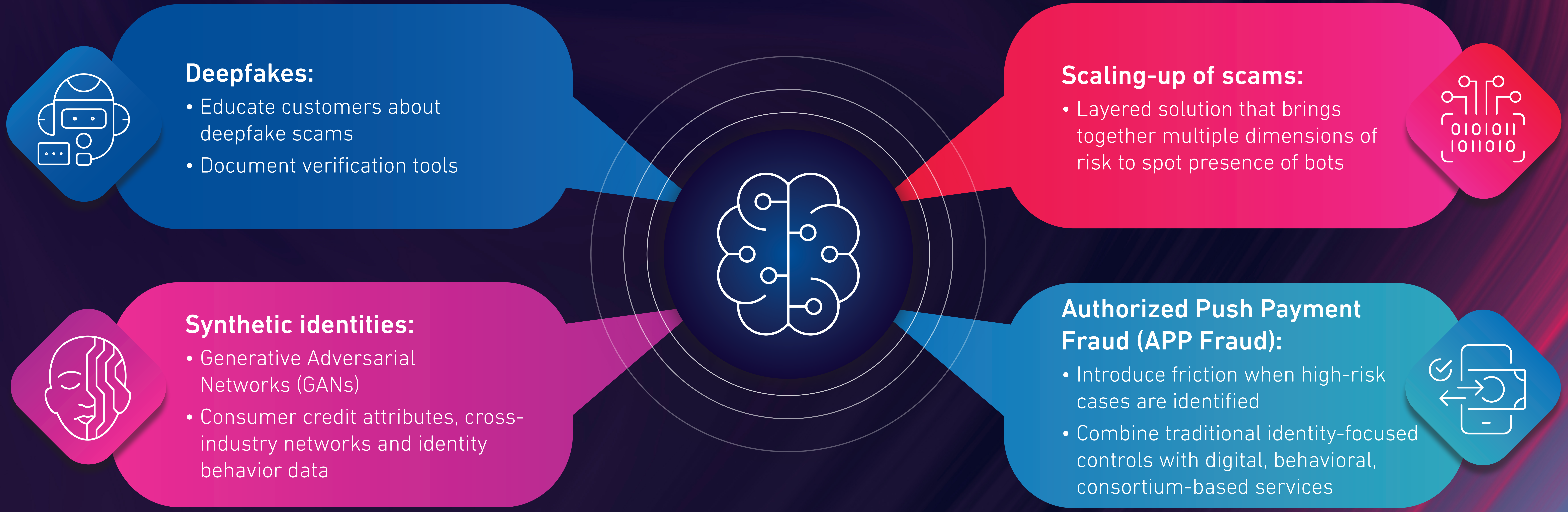
GenAI poses two main threats regarding fraud: the scaling and personalization of attacks. Mitigation comes in many forms, depending on the business. Still, the fundamental differentiator in the fight against evolving and increasing fraud attempts is the ability to have a holistic view of the consumer.

Businesses today deploy multiple solutions from various vendors to ensure fraud mitigation covers all touchpoints. Although full coverage may exist, businesses often don't have a holistic offline and digital view of the consumer, meaning losses can accumulate before patterns emerge within these siloed views.

GenAI allows fraudsters to create and scale a template for an identity, having the correct identity data and the ability to mimic behaviors and attributes. These templates can bypass solutions by using compromised data that already has a lifespan, making it increasingly difficult for organizations to pick up on red flags early enough to prevent losses. This is why fraud and identity point solutions are ineffective against GenAI-enabled fraud.

Rapidly evolving, highly automated, and large-scale attacks demand an up-to-date cross-industry view of online and offline identity behavior, linkages, and interactions. The flexible solution must similarly leverage GenAI to spot and validate fraud signals, interpret intelligence from fraud analysts, and quickly operationalize new attributes and models to keep pace with attackers. This is where layered fraud and identity controls in real time and a comprehensive offline analytics platform work together.

Mitigating GenAI-enhanced fraud – the key takeaways:



Deepfakes:

- Educate customers about deepfake scams
- Document verification tools

Scaling-up of scams:

- Layered solution that brings together multiple dimensions of risk to spot presence of bots

Synthetic identities:

- Generative Adversarial Networks (GANs)
- Consumer credit attributes, cross-industry networks and identity behavior data

Authorized Push Payment Fraud (APP Fraud):

- Introduce friction when high-risk cases are identified
- Combine traditional identity-focused controls with digital, behavioral, consortium-based services

Sources

- *Bloomberg Intelligence: Generative AI to become a 13 trillion market by 2023*
- *Gartner: 2023 Gartner Hype Cycle for Emerging Technologies*
- *Forrester: Forrester's Priorities Survey 2024*
- *Experian: Experian's 2024 U.S. Identity & Fraud Report*
- *Liminal: GenAI and Fraud: The impact of GenAI on the frau detection and prevention market, 2024*
- *Deloitte: Generative AI and Fraud – What are the risks firms face?*
- *Experian Insights: Understanding Synthetic ID Fraud*
- *Liminal: ATO Prevention in Banking Buyer Survey, March 2024*

Credits

- *Mike Gross, Vice President, Applied Fraud Research & Analytics*
- *Rebecca McGrath, Global Content Marketing Manager*
- *Matthew Stennett, Brand Design Manager*
- *Chris Ryan, Product Director, Ascend Fraud Sandbox*
- *Mihail Blagoev, Global Solution Strategy Analyst*
- *Michael Touchton, Senior Manager of Analyst Relations*
- *Christopher Wilson, Senior Vice President, Portfolio Marketing*
- *Paulina Yick, Global Director of Product Marketing*