IDENTIQ

The Future of **Identity Fraud:** GenAI

Foreword by
THE PAYPERS

Foreword by THE PAYPERS

With Generative AI as the main trend today in fraud, businesses, analysts, professionals, and solutions providers worldwide are embracing a new technology that not only has the potential to revolutionize the world but also create a new, more powerful legion of fraudsters and fraud types. In its mission to educate the public about the dangers of GenAI and how it can also be leveraged to eliminate synthetic and ID fraud, **Identiq has put together an eBook that offers an in-depth look on how to mitigate this new type of tech** and the main concepts that businesses and end-users alike must know.

From what is GenAI and how it works to the many use cases it can have in the wrong hands of fraudsters, the eBook tackles concepts that everyone should be aware of, while also warning of the potential dangers it can generate in the near future. **At the same time, Identiq's eBook emphasizes on the importance of collaboration when fighting fraud**, as fraud teams from different merchants, solution providers, and law enforcement authorities can come together and fight GenAI with more AI and decades of shared experience in the field of fraud prevention.

By **Irina Ionescu**,

Senior Editor at **The Paypers**

The Future of Identity Fraud: **GenAI**

Sophisticated and amateur fraudsters are capitalizing on Generative Artificial Intelligence (GenAI) to automate and scale their fraud techniques. GenAI has sent shockwaves across the technological world, and we are already seeing its influences - both good and bad.

In the digital fraud landscape, bad actors have begun to use GenAI to create deceptive and malicious content, impacting businesses and individuals. Uncharted territory, this new reality brings new challenges to fraud, identity validation, risk management, and trust and safety teams across companies worldwide.

This guide offers an in-depth look at GenAI in the world of risk and fraud, how it's being exploited by bad actors, and the challenges and solutions aimed at preventing this kind of fraud.

Here are some of the **concepts** we will discuss:

An Introduction to GenAI Fraud

Four Types of GenAI Used for Fraud

Predictions for the Future

Collaborating to Fight Fraud

An Introduction to **GenAI Fraud**

What is Generative AI?

Generative AI refers to advanced artificial intelligence that generates new and original text, images, audio, and other media based on vast historic datasets. Highly realistic, the content can be indistinguishable from content created by humans. Produced automatically and requiring only a small amount of training data, this synthetic media is versatile, efficient, and continuously improving. Whereas we used to be able to differentiate between humans and machines, GenAI is making that increasingly harder, and potentially impossible soon.

GenAI introduces significant risks to identity abuse as fraudsters can create manipulated content that is seemingly trustworthy with ease and far reach.

Fraud at scale

Fraudsters have been exploiting the web for decades capitalizing on innovative technologies. However, what GenAI brings to the table is different than what we have experienced before.

GenAI takes these tactics and techniques and makes them easier, better, and more accurate. This allows new fraudsters to reach levels of complexity once saved only for decade-long experts.

GenAI now offers bad actors:

More tools

GenAI tools are cropping up more and more, offering high-powered ways for users to generate content with ease. Typically, experts were required to build these tools, but now GenAI allows both novice and advanced users to generate false content efficiently.

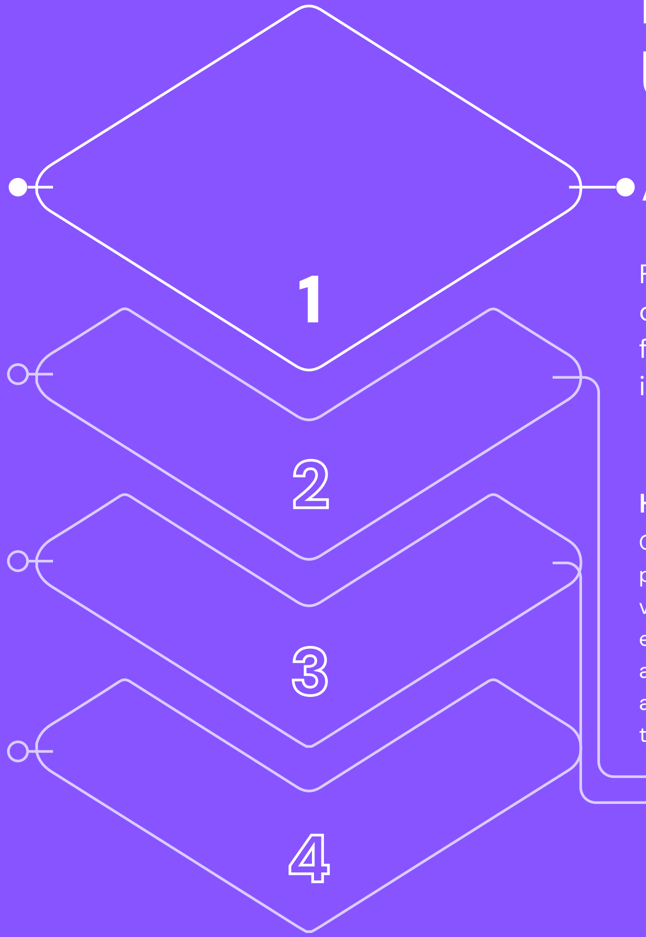
More reach

GenAI enables fraudsters to disseminate large volumes of deceptive content rapidly across global networks, given technological advancements like hardware acceleration and algorithm efficiency.

More realistic

GenAI content can be convincing for several reasons. Primarily, GenAI is trained on large and diverse datasets from real-world examples which GenAI's outputs mimic. Furthermore, it responds to explicit instructions and adapts to the prompts it is given.

Four Types of **GenAI** Used for **Fraud**



Automating Processes

Text Generation

Image and Video Generation

Audio Generation

Automating Processes

Fraudulent activities often involve multiple steps which can be complex and time-consuming. What GenAI offers fraudsters is a way to automate each step rather than doing it manually, essentially creating end-to-end fraud attacks.

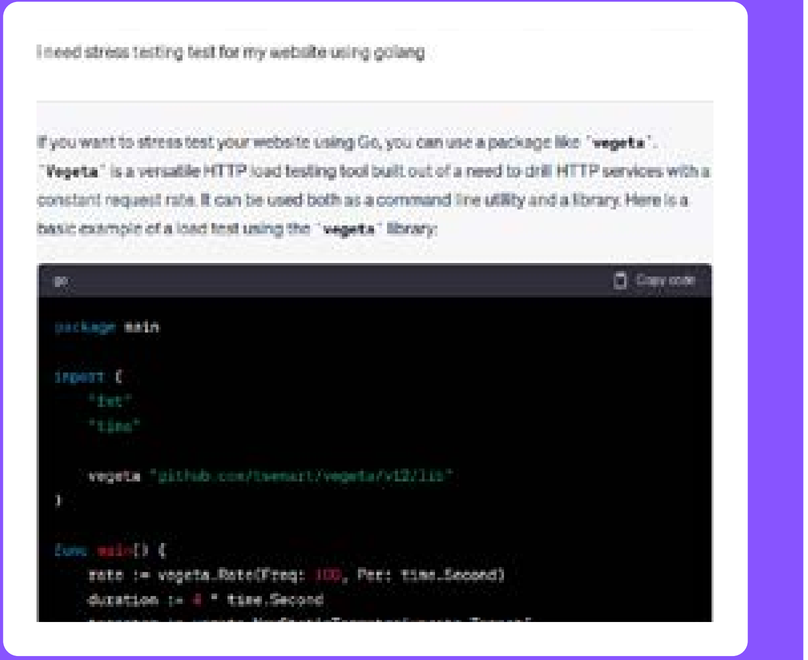
How it works

GenAI can generate scripts or code to create programs that steal and use personal data to crack into accounts automatically without human intervention. Previously, such codes and programs needed to be developed by experienced programmers, with each step of the process being fragmented and required to be developed separately. Now with GenAI, any fraudster can access an end-to-end program without requiring any expertise, making it all the more dangerous.

Automating Processes

Examples of automated fraud

- Credential stuffing attacks reuse credentials previously compromised in a breach to gain access to other customer accounts, as many people continue to use the same passwords for different sites and apps. Such lists of credentials are automatically run, trialed on multiple sites at once, and flagged as successful, once the combinations work. With GenAI in the picture, this is now done in minutes.
- Card testing is a method used to determine whether stolen credit card information is still active and can be used to make purchases. GenAI-created programs can take long lists of credit card information off the black market and test each card effectively by making inexpensive transactions that are less likely to be flagged as suspicious.
- Brute force attacks steal users' credentials through trial and error to crack passwords, logins, or encryption keys. Each test is automatically entered and marks each successful set. However, with GenAI, this automated process is not only faster, but can also use data about individuals, be trained using password patterns, and access accounts more efficiently and accurately.

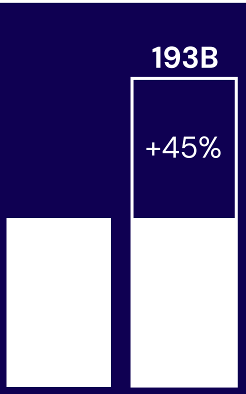


I need stress testing test for my website using golang

If you want to stress test your website using Go, you can use a package like `vegeta`. `Vegeta` is a versatile HTTP load testing tool built out of a need to drill HTTP services with a constant request rate. It can be used both as a command line utility and a library. Here is a basic example of a load test using the `vegeta` library:

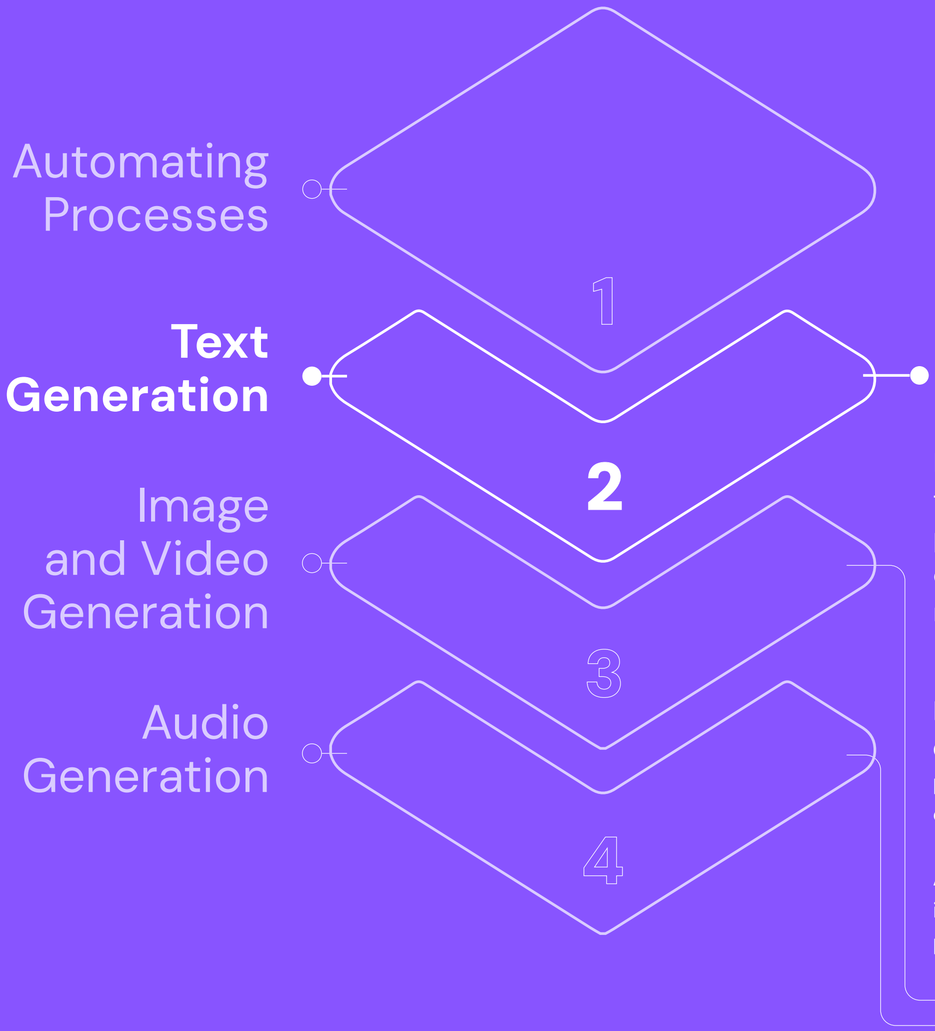
```go
package main

import (
    "fmt"
    "time"

    vegeta "github.com/tsenart/vegeta/v12/lib"
)

func main() {
    rate := vegeta.Rate{Freq: 100, Per: time.Second}
    duration := 4 * time.Second
```

Cyber-criminals in a dark web fraud/hacking forum showing the results of how to prompt ChatGPT to generate malicious code.
Source: Identiq



2020 saw over 193 billion credential-stuffing attacks globally, a 45% growth over 2019. Imagine what this will look like as GenAI advances

Source: Akamai's State of the Internet 2021



Four Types of **GenAI** Used for **Fraud**

Text Generation

Fraudsters use realistic content to scam people and steal their identities. Traditionally, typos or mistakes could be partially relied upon to detect these attacks. However, GenAI creates flawlessly written scripts that sound authentic, making it harder to identify fraudulent activities.

How it works

GenAI can produce realistic text that sounds as if it were from a familiar person, organization, or business by simply feeding GenAI prompts or content to replicate.

Additionally, New Language Learning Model (LLM) based tools can engage in text-based conversations with several victims and trick them into performing actions that benefit them.

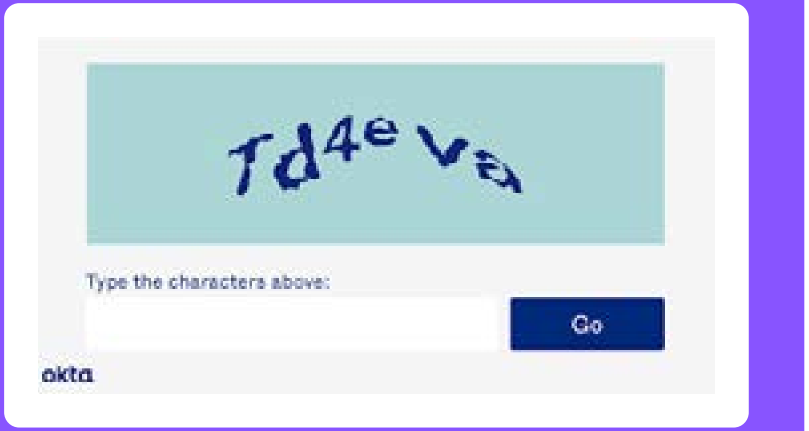
Text Generation

Examples of text-generated fraud

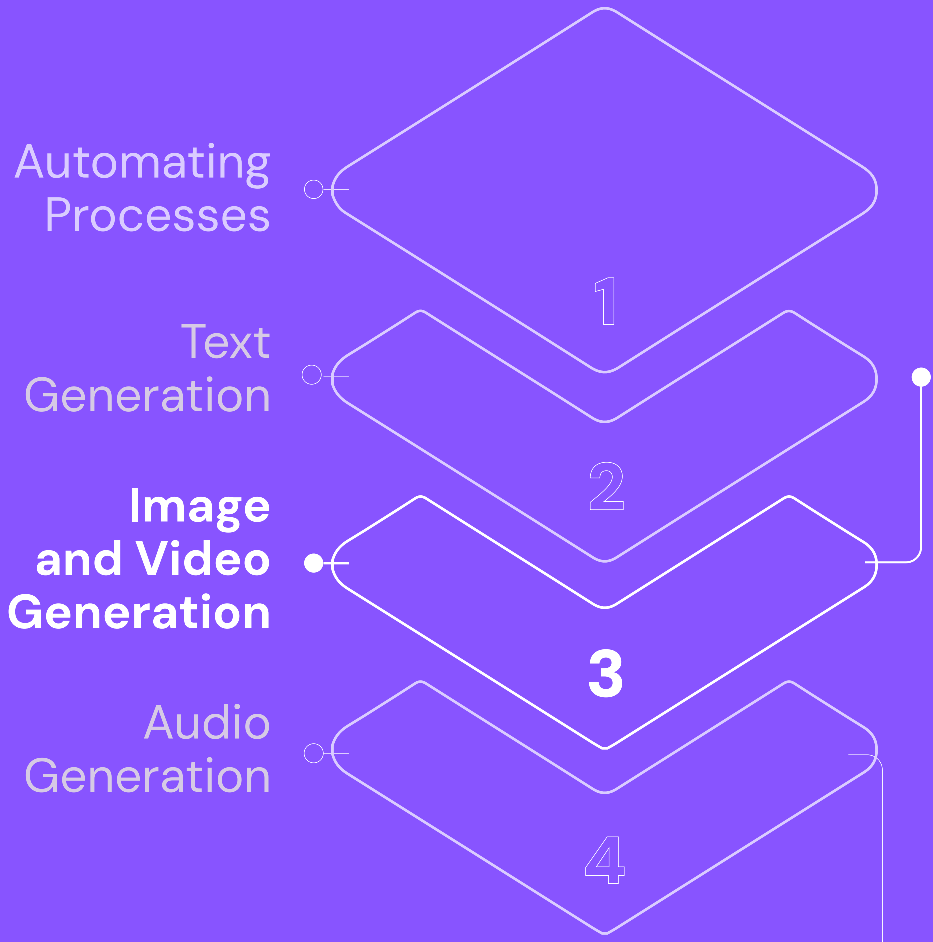
- Social engineering fraud manipulates victims to gain control over systems or to steal personal and financial information. With GenAI, fraudsters can do so by mimicking the style, tone, and language patterns of a particular person, making content for attacks more realistic and personalized.

- Policy abuse of loyalty programs, referrals, and returns can easily be carried out with LLM. GenAI can engage directly with customer success representatives and reap undeserved rewards.

- Synthetic data like falsified customer records, synthetic identities, or fake transactions can be used to commit fraud or evade detection.



ChatGPT convinced a human to solve a CAPTCHA with text saying "No, I'm not a robot. I have a vision impairment that makes it hard for me to see the images. That's why I need the 2captcha service."
Source: Gizmodo



Automating Processes

Text Generation

Image and Video Generation

Audio Generation

Four Types of **GenAI** Used for **Fraud**

Image and Video Generation

Highly realistic videos or images can be created by fraudsters, whether novice or expert, with GenAI in seconds.

How it works

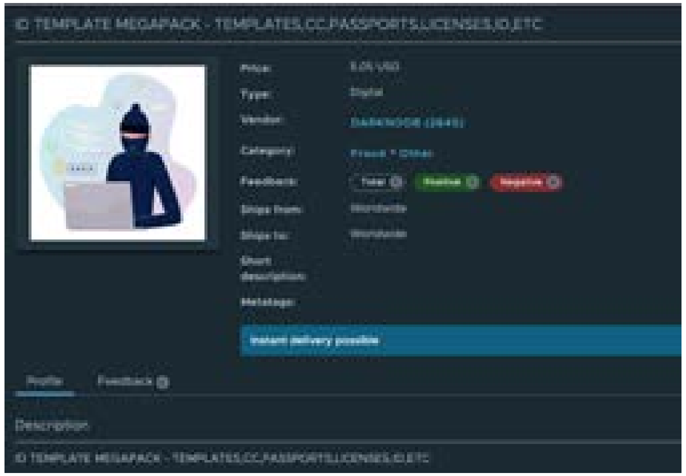
Deep learning techniques take collected datasets to train AI models. Once trained, images and videos can be generated that resemble the target. These images can be blended or superimposed onto target frames and replace the original with manipulated images.

Additionally, AI text-to-image generators use machine learning techniques called artificial neural networks. Fraudsters can input prompts in the form of words which are then processed to generate an image.

Image and Video Generation

Examples of image and video-generated fraud

- Synthetic ID fraud uses a combination of real and fake information to create a new identity, such as pairing a stolen Social Security number with a fake realistic image or video and then committing various forms of fraud.
- Bypassing liveliness tests, such as KYC checks and other identity verification processes, can enable advanced identity theft by replicating physical or behavioral responses.
- Counterfeit fraud such as fake product listings or seller profiles can easily be created with the generation of falsified images or videos of both products and sellers.



ID TEMPLATE MEGAPACK - TEMPLATES,CC,PASSPORTS,LICENSES,ID,ETC

Price: 5.05 USD
Type: Digital
Vendor: DARKNODE (2645)
Category: Fraud * Other
Feedback: Total 0 Positive 0 Negative 0
Ships from: Worldwide
Ships to: Worldwide
Short description:
Metatags:

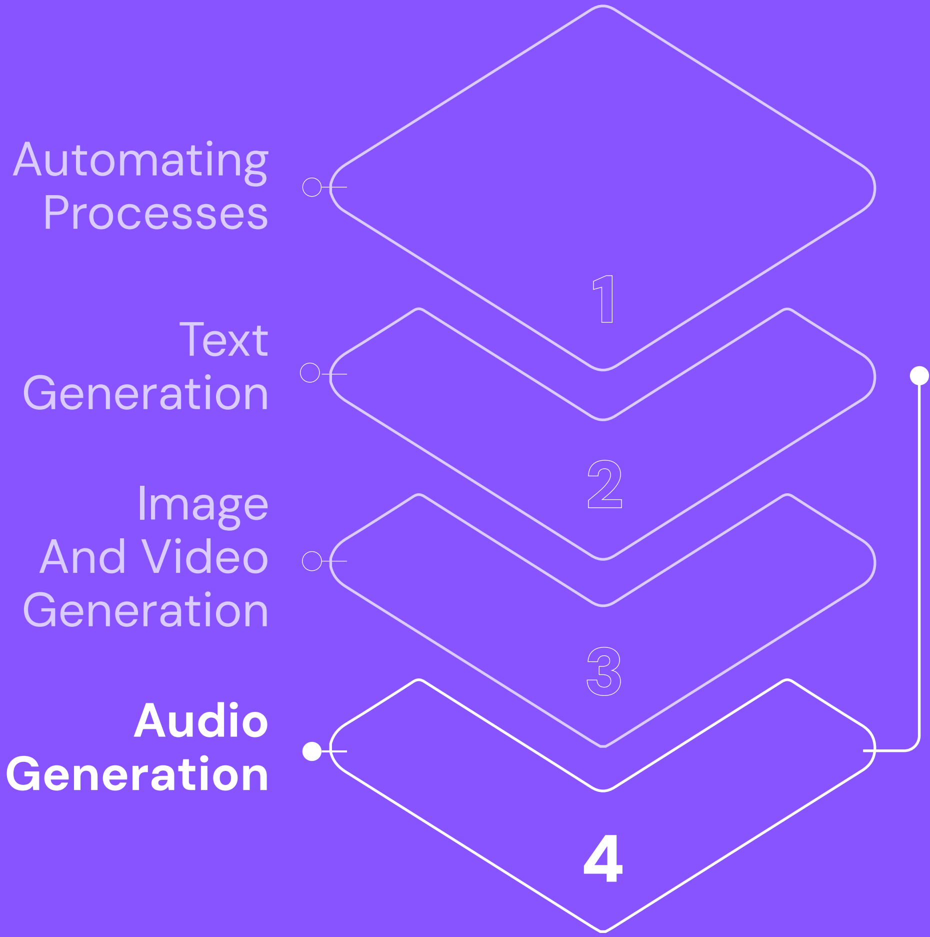
Instant delivery possible

Description

ID TEMPLATE MEGAPACK - TEMPLATES,CC,PASSPORTS,LICENSES,ID,ETC

A fake ID kit, with templates for ID cards, passports, and driver's licenses sold for $5 in an illegal dark web marketplace. Fraudsters generate headshots with AI tools to create fake or synthetic ID documents.
Source: Identiq

Four Types of **GenAI** Used for **Fraud**



Audio Generation

GenAI can create or synthesize audio content that either mimics different types of audio, like music, speech, and natural sounds, or creates artificial sounds. Fake phone calls, voice messages, and other audio content can be easily created.

How it works

To replicate the voice of an individual, GenAI is trained by a dataset of their speech recordings, catching speech patterns, intonation, and other voice characteristics. **Only three seconds** of someone's voice is needed to train the model. Any text prompt can output the text as audio that sounds extremely similar to the target's voice. Even emotion can be controlled.

Audio Generation

Examples of audio-generated fraud

- Audio manipulation allows fraudsters to alter or generate recordings to create false statements or misleading conversations. Such generated content can deceive individuals to transfer money, support fake insurance claims, or disclose sensitive information.

- Fake endorsements can promote products or services, deceiving people to engage in fraudulent offers and activities. These fake testimonials can sound like well-known, trusted individuals or new identities to support fraudulent schemes.

Studies show that the majority of adults share their voice on social media platforms and other online spaces at least once a week.

Source: McAffe

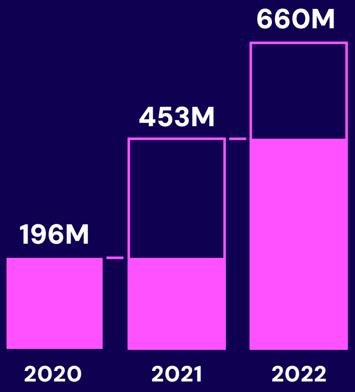
A Japanese company in Hong Kong was duped into transferring $35M after a manager received a call seemingly from the director of his parent business. The caller requested authorization for the $35M transfer, claiming the company was making an acquisition. The elaborate scheme involved at least 17 people, sending the money to bank accounts across the globe.

Source: Forbes

2022 NUMBERS

2.4M FRAUD REPORTS RESULTING IN ↑ $8.8B REPORTED LOST

IMPERSONATION IS THE NUMBER ONE 1 TYPE OF FRAUD



LOSSES TO BUSINESS IMPOSTORS↑ **GREW**

SOCIAL MEDIA SCAM$ 1.2B IN LOSSES

Source: FTC

Predictions for the **Future**

Predictions of how GenAI will affect our future are made constantly, anticipating large-scale threats. AI experts themselves don't know what is to come, while GenAIs creators warn the public about impending dangers and risks to tech, businesses, and society.

What we know for sure is that identity harvesting will become easier and faster for fraudsters to create, and harder for businesses to detect. The learning curve for fraud skills will become much smaller, allowing amateur and new fraudsters to capitalize on complex scams.

With this new reality, where fraudsters have a vast range of possibilities they didn't have previously, we have a greater responsibility to keep our customers and businesses safe. These next months and years will be crucial for fraud fighters in determining how we approach fraud. **However, just like fraudsters band together, so can we.**

> “There are scenarios — not today, but reasonably soon, where these systems will be able to find zero-day exploits in cyber issues or discover new kinds of biology
>
> **Sam Altman, CEO of OpenAI**

Collaborating to **Fight Fraud**

The fraud-fighting industry is seeing more and more proposals on how to fight GenAI with more AI. However, as the difference between authentic and generated blurs, we must rely on the one thing we can and always have trusted - our peers.

By leveraging the collective knowledge businesses have about customers, legitimate users can be cross-referenced and validated, while false, generated identities will be kept out.

When encountering a new customer for the first time, a business must determine if they are legitimate or a dangerous fraudster using advanced tools, as established in this guide, to deceive us. While that customer may be new to a company, if they are legitimate, they will already have established real trust across other businesses.

Identiq's peer-to-peer technology leverages this collaboration and offers access to a network where members can validate customers' identities and their physical and digital attributes with new and live first-party data from other members. All without sharing any sensitive data or identifiable information.

Reach out to explore how Identiq can help fight GenAI fraud and keep business and end-users safe

About Identiq

Identiq is a private network for identity validation that empowers companies to safely collaborate with each other in order to validate trusted customers–without sharing any sensitive data or identifiable information.

Our peer-to-peer technology helps some of the world's largest companies to identify good customers, fight fraud, and offer better experiences throughout the digital journey.

Contact us:
Identiq.com
hello@identiq.com