ENTRUST CYBERSECURITY INSTITUTE PRESENTS

2025 Identity Fraud Report

EXECUTIVE SUMMARY

November 2024

ENTRUST

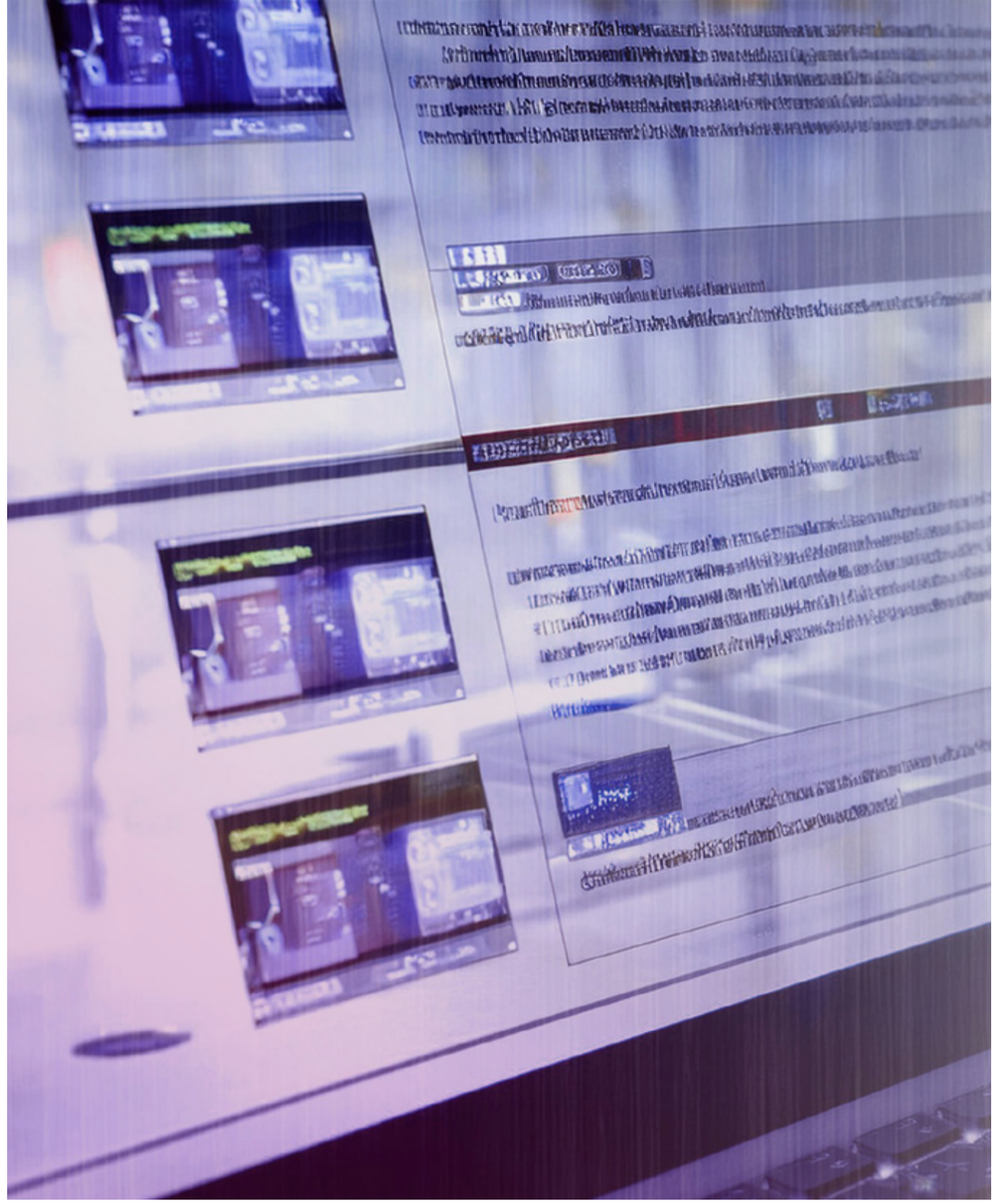
onfido
an Entrust Company

Table of Contents

Generative AI, Deepfakes, and “as a Service” – the New Face of Identity Fraud

Basic but highly scalable fraud tactics that are relatively easy to discern are quickly giving way to AI-generated deepfakes and synthetic identities that are both hyper-realistic and super scalable. At the same time, cybercriminals and fraudsters are enabling each other by sharing access to known vulnerabilities and threat tactics often via an as-a-service delivery model. With that lens, the Entrust Cybersecurity Institute is pleased to highlight the results of the 2025 Identity Fraud Report.

For this report, we analyzed tens of millions of identity verifications across 30+ industries in 195 countries for the one-year period of September 1, 2023 - August 31, 2024.



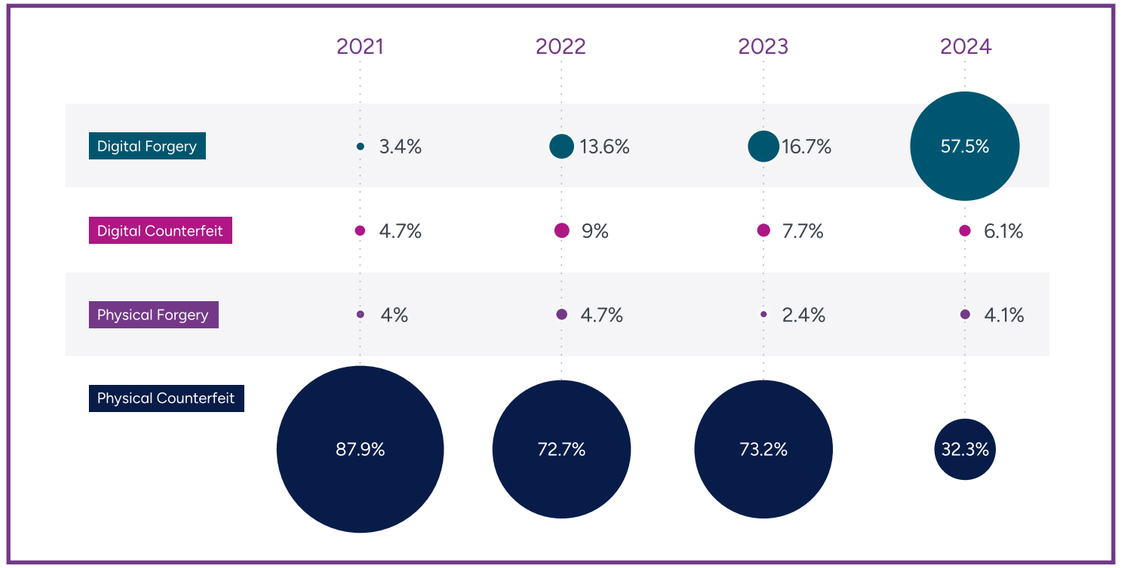
Generative AI Enables Cybercriminals

Generative AI, also known as GenAI, employs machine learning to create new, credible content including text, imagery, audio, and video. Many organizations already use GenAI tools like Microsoft Copilot as an office productivity booster. However, cybercriminals are increasingly using GenAI tools for their own gain.

Indeed, today's bad actors have access to a cybercrime treasure chest with GenAI tools that create very convincing phishing emails and hyper-realistic deepfakes, along with websites that specialize in creating credible fake documents. Fraudsters employed GenAI to create more digital forgeries than physical counterfeits for the first time ever in 2024, with digital forgeries now accounting for 57.46% of all document fraud. This represents a 244% year-over-year increase, and a 1,600% increase since 2021!

Digital forgery has become new document fraud of choice

Just four years ago, physical counterfeit was by far the most common form of document fraud. Not anymore. In 2024, digital forgery became the fraudsters' method of choice.



Digital Forgery

Physical Counterfeit

Did You Know?

In 2024, deepfake attempts are occurring at a rate of one every five minutes.

Deepfakes Emerge as New Face of Biometric Fraud

Deepfakes, often created with face-swapping apps or the use of GenAI, first became a widespread attack vector in 2023, increasing a staggering 3,000% in just one year and spiking to another all-time high in January 2024.

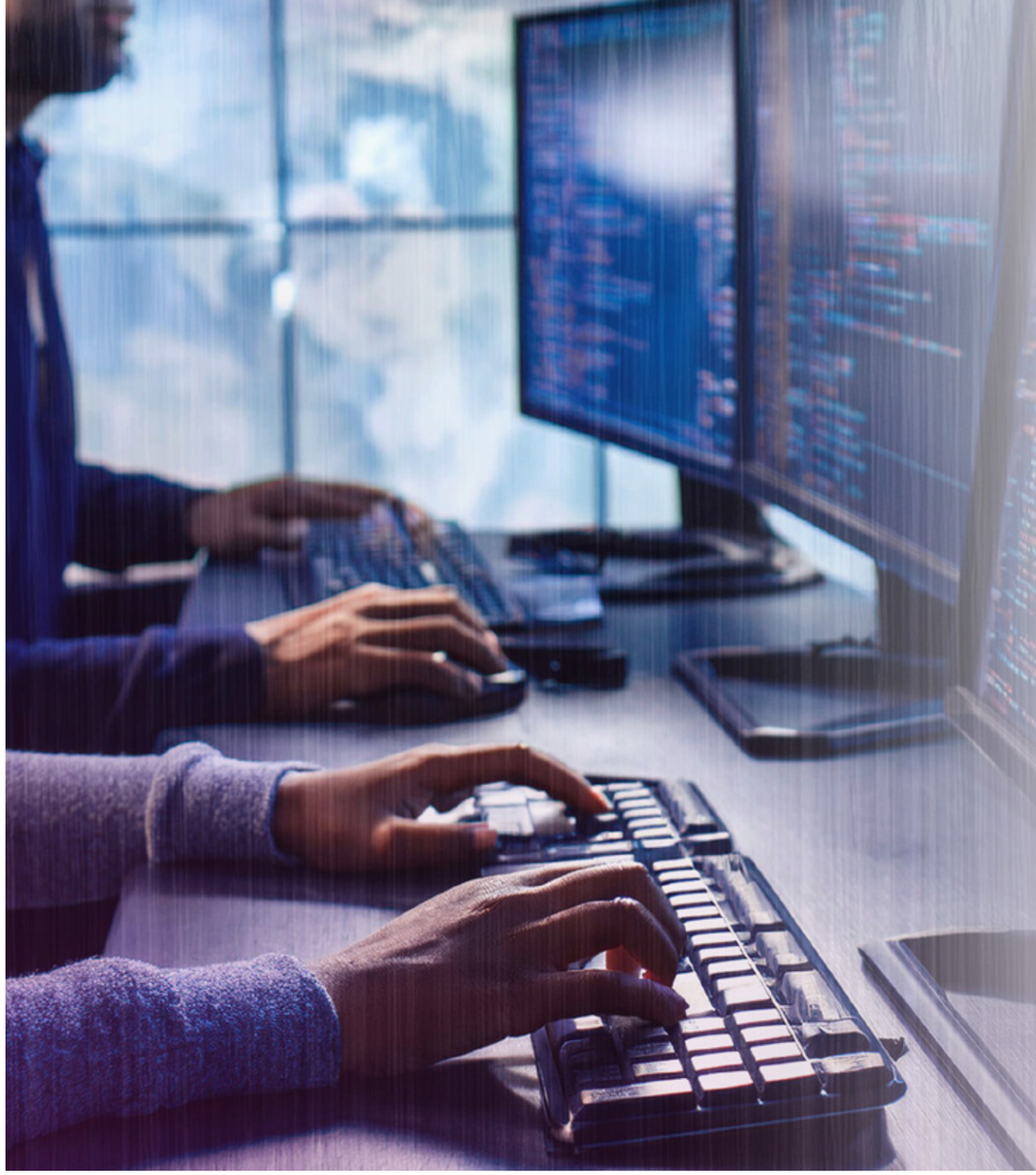
Deepfakes represent a particularly pernicious threat to fraud prevention and detection strategies that rely on biometric checks like a static photo (selfie) or a video element (video/motion) to confirm a person's identity. A deepfake is a digital manipulation of this photo or video where a person's face is altered to appear as someone else.

With AI-generated fakes becoming increasingly hyper-realistic, deepfaked photos (like a manipulated social media profile pic) now account for most selfie biometric fraud, and deepfaked videos also account for most video biometric fraud attempts at 40%. It's estimated that there is now, on average, one new deepfake attempt every five minutes!

Cybercriminals and Fraudsters Embrace “as a Service”

From fraud to ransomware to phishing and beyond, cybercriminals are embracing as-a-service models to up their own game – and that of others – by sharing known vulnerabilities and threat tactics over the internet.

Plus, with fraud-as-a-service (FaaS), ransomware-as-a-service (RaaS), and phishing-as-a-service (PhaaS), savvier bad actors are profiting from what they know by sharing and selling their knowledge on the dark web. This is enabling more amateur cybercriminals with the tools they need to commit fraud, increasing both the overall number of attacks and the volume of sophisticated attacks.



Cryptocurrency – a Prime Target for Fraudsters

When it comes to customer onboarding, cryptocurrency platforms have the highest rate of fraudulent attempts compared to any other industry. With a suspected fraud rate of 9.5%, it's nearly double that of the next two hardest-hit sectors – lending and traditional banking.

Fraudulent attempts in the crypto industry are also up nearly 50% this year, going from 6.4% in 2023 to 9.5% in 2024. It's likely that this level of fraudulent activity is due to the price of crypto hitting another all-time high in 2024.

Top 3 industries targeted most by fraudsters

Industry	Suspected Fraud Rate
1. Cryptocurrency	9.5%
2. Lending	5.4%
3. Traditional banks	5.3%

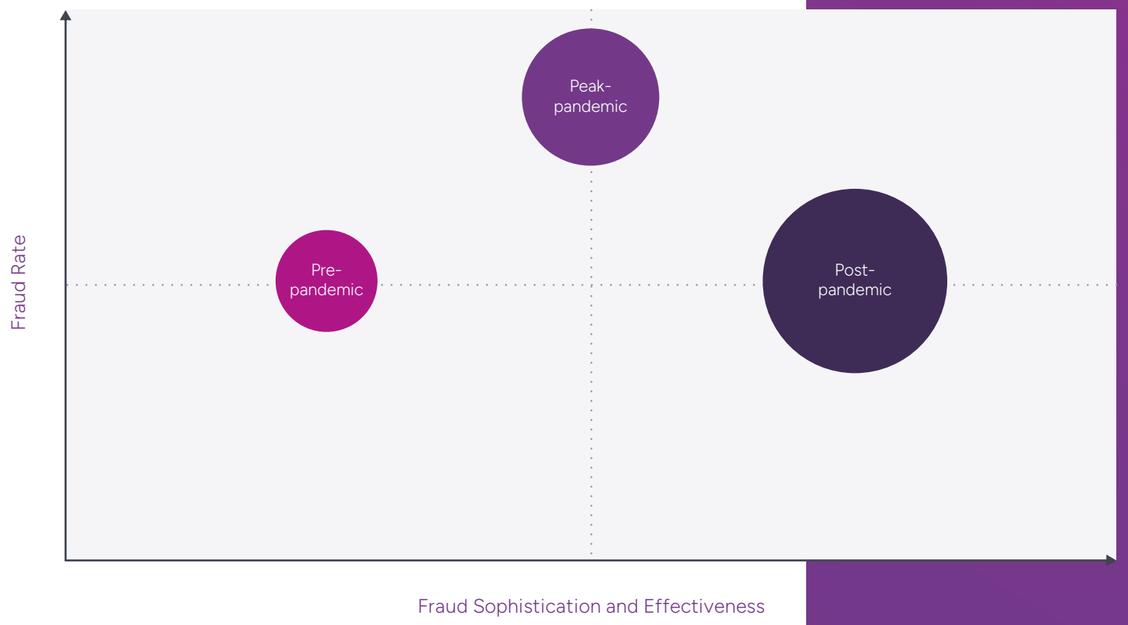
Evolution of Fraud Pre-, Peak-, and Post-Pandemic

Whether it's how we work, buy groceries, receive medical care, or interact with our government, it seems the last five years can be grouped into pre-, peak-, and post-pandemic.

Five years ago, most document fraud was performed on a physical identity document rather than the digital forgeries we see today.

During the pandemic, there was a marked uptick in fraud as more and more businesses moved operations online, in some cases overnight. While fraud volumes were at an all-time high during this period, it was before GenAI went mainstream and tactics were much less sophisticated.

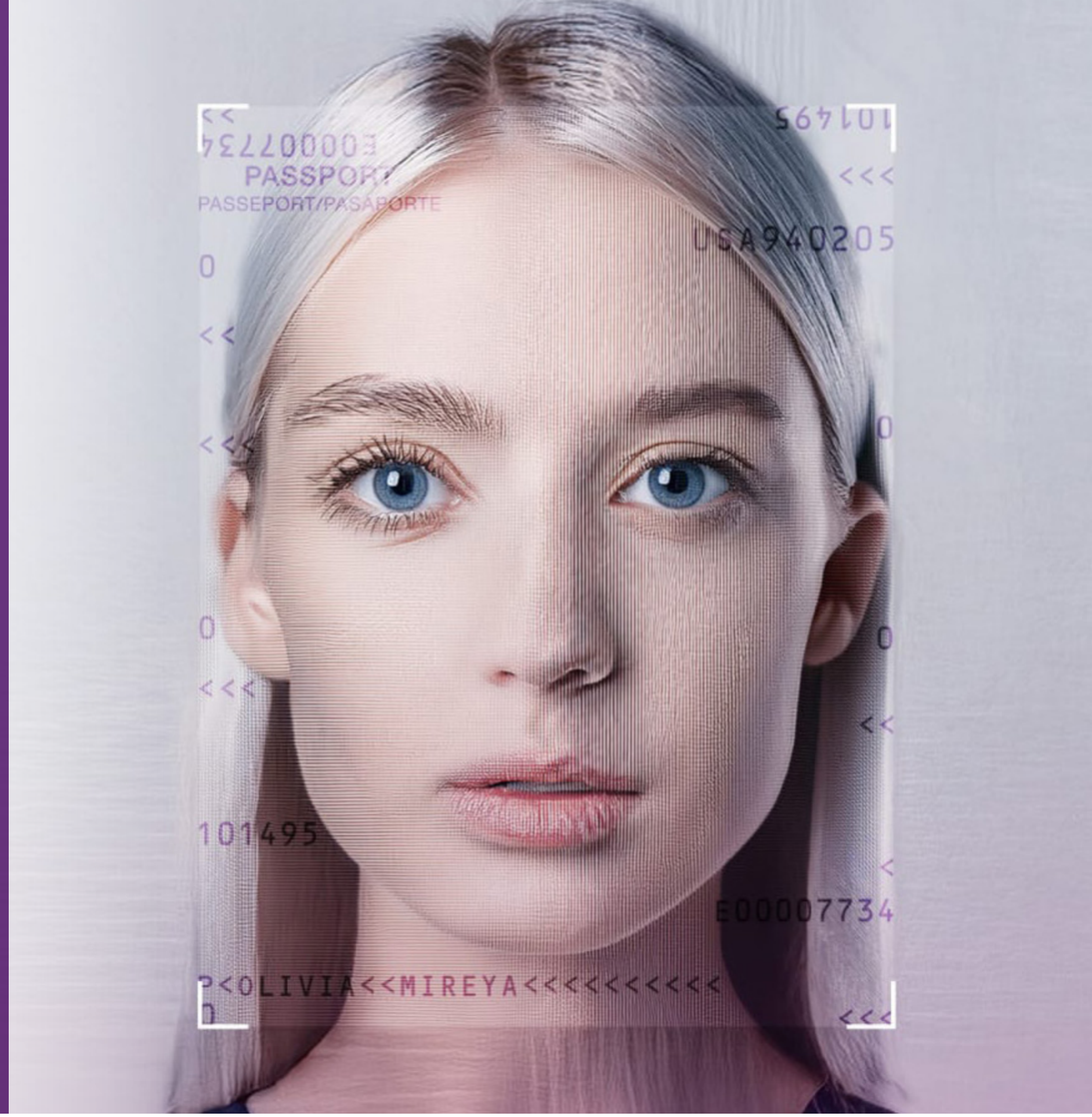
Fast forward to today and fraud rates have fallen back to pre-pandemic levels. However, GenAI has increased the sophistication, scale, and ultimately the effectiveness of attacks.



Get the Full Report

Want more insights into the current state of identity fraud? Download the full 2025 Identity Fraud Report for a deeper dive into the statistics.

Download full report



entrust.com | Toll-Free: 888.690.2424 | International: +1.952.933.1223 | sales@entrust.com

ENTRUST
SECURING A WORLD IN MOTION