



The Trust Ledger:

Transaction & Identity Fraud Bulletin

JULY 2025



Table of contents

Introduction	3
What We're Dealing With: The Face of Modern Fraud	4
The Generative AI Effect: Fuel for the Fraud Fire	12
The Policy Gap: Fraud Moves Fast. Regulation Doesn't	19
What You Can Do Now: Practical Takeaways for 2025	22
Looking Ahead: The Future of Fraud Prevention	24

Introduction

Trust used to be human. Now it has to be engineered.

Not long ago, identity was personal. Trust was built through handshakes, eye contact, and reputation—earned over time, not through a login screen.

In a digital-first world, every interaction is a transaction—and every transaction is a potential risk.

Trust needs to be verified in real time. Fraudsters aren't just targeting big banks or vulnerable seniors. They're targeting everyone, everywhere, all at once. Whether it's a call using a cloned loved one's voice, a deepfaked video from your "CEO," or a phishing email crafted by AI, **the threats are getting smarter, faster, and more personal.**

2024 made it clear: we are not keeping up. According to the FBI internet crime hit new records, with **\$16 billion in reported losses—a 33% jump from the year before.** And that's just the fraud we know about.

Proof's first annual **Transaction & Identity Fraud Bulletin** should be a wake-up call for businesses, policymakers, and everyday consumers. Based on frontline insights from identity verification data, threat research, and fraud leaders across industries, this report unpacks the fraud economy in 2025.

The central question: **How do we rebuild trust in a world where identity is easy to fake—and harder than ever to prove?**

Because in this environment, trust isn't given. It's earned at every click, call, and credential check.



What We're Dealing With: The Face of Modern Fraud

This rise in fraud isn't isolated to a few bad actors or shady websites. It's happening across every industry and every type of transaction—and it's targeting real people at their most vulnerable moments.

Who's Being Targeted

Consumers

The elderly continue to be the top target for fraud. In the United States, the 60+ demographic filed the **most fraud complaints and suffered nearly \$5 billion in losses**.¹

According to the FTC, the most common types of fraud in 2025 have been via **business impersonation, online shopping, and online payment services**.²

The most common modes of communication are **email (21%), text (21%), and phone calls (18%)**, however the most effective channels (i.e. those that most often result in monetary loss) are **social media (73%), websites/apps (70%), and online ads or pop-ups (66%)**.²

Additionally, states like **California, Texas, and Florida** saw the highest rates of reported fraud, further reinforcing that this is a **nationwide epidemic**, not a fringe issue.¹

Businesses

Fraud is no longer just a payments problem—it's hitting sectors that never expected to be in the crosshairs.

For decades, fraud teams operated within narrow lanes: verifying transactions, flagging stolen credit cards, catching obvious red flags. But today, identity-based fraud is spilling into new and unexpected domains. Businesses that historically had minimal exposure are now being forced to become fraud experts overnight.

WHO'S TAKING PRECAUTIONS?

Despite being highly targeted, older adults are also proactively adopting identity protection—outpacing younger users in online identity verification (IDV) usage.

- *According to Proof.com user data, there are nearly 2x as many identity verification users aged 60–64 as there are 20–24.*
- *The largest demographic of IDV users on the platform is 35–39, followed by 40–44, and 30–34.*

¹ Federal Bureau of Investigation Internet Crime Report, 2024

² Fraud Reports by U.S. Consumers, Federal Trade Commission

- **Utility companies** are facing surges in fraudulent account creation. In some states, scammers are signing up for electricity using fake IDs and racking up unpaid bills. Because power shutoffs are highly regulated, these companies are losing millions without an easy recourse.
- **HR departments** are being targeted by fake job candidates who make it through screening, land on the payroll, and start collecting a paycheck—sometimes while using insider access to steal company data. Employment laws make it difficult to quickly remove these bad actors.
- **Property managers** in multifamily housing are grappling with lease fraud. Renters use synthetic or stolen identities to secure housing and then live rent-free until they’re legally evicted—a process that can take months.

The Data Economy Powering Fraud

Behind the scenes, identity-based fraud is being fueled by something deceptively simple: **data**. On the dark web, the most prized commodity is “**fullz**”—shorthand for “full details” that typically includes **full name, address, date of birth, and Social Security number**.

So where does this data come from?

- **Data breaches** remain a goldmine—especially in industries like **healthcare**, where records are **comprehensive, current, and abundant**.
- **Infostealers**—malware designed to extract autofill data, saved credentials, and authentication tokens—represent the fastest-growing source of high-value stolen data.

QUICK GLOSSARY

Fullz

*/fʊlz/ **noun**: Complete identity profiles (name, DOB, SSN, address, etc.)*

Logs

*/lɒg, lɒg/ **noun (pl)**: Stolen credentials and authentication cookies from infected devices*

Infostealers

*/ˈɪn fəʊ-ˈsti:ləz/ **noun (pl)**: Malware that collects logs from browsers and apps*

GOING RATE FOR YOUR IDENTITY - \$3

*A full identity record—known as “fullz”—sells for as little as **\$3**.
Buy in bulk, and the price drops even further.*

These “**logs**” often include not just personal information, but **bank credentials, credit card numbers, and authentication cookies**, all bundled together and sold by device.

Ironically, **fraudsters are also leveraging legitimate tools** originally meant to prevent fraud. Access to commercial platforms like **TransUnion’s TLOxp**, intended for law enforcement and financial institutions, is now being resold or abused via compromised accounts—making it easier than ever to enrich stolen data and impersonate individuals or businesses.⁴

THE INFOSTEALER MALWARE PROBLEM IS RAMPANT—AND IT’S ONLY GETTING WORSE.

It’s been estimated that in the first two months of 2025 alone, more than 200 million credentials have been stolen.

Attempted countermeasures like Chrome’s recent Application-Bound Encryption have done little to slow malware developers.³

HOW PROOF DEFENDS DATA

Proof has developed AI-powered risk detection features like Defend to protect our data sources.

Defend uses over 100 risk signals to detect both traditional identity fraud and emerging threats like synthetic identities and deepfakes.

You’ll receive real-time alerts via email or webhook anytime a customer is flagged as high or medium risk during identity verification. Every flagged transaction includes enhanced identity insights (like IP address, phone and email risk data, and credential images) so your team can investigate with confidence.

³SpyCloud, “How Infostealers Are Bypassing New Chrome Security Feature to Steal User Session Cookies”

⁴404 Media, “Feds Charge Alleged ‘TLO’ Underground Data Broker”

High Stakes at Massive Scale: Every Transaction is a Fraud Opportunity

As the sheer volume of transactions increases, so too does the opportunity for fraudsters to capture “fullz” and logs, which together give bad actors carte blanche to open new financial accounts and empty existing ones.

The Proof platform processes **millions of high-risk interactions** across industries like:

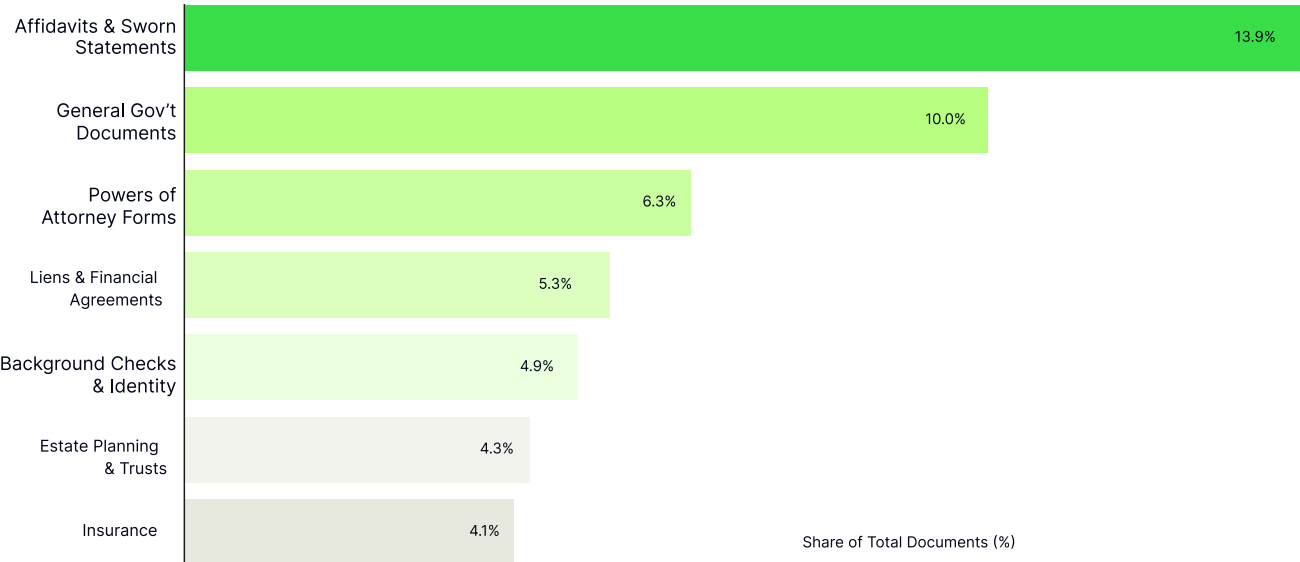
- Financial services
- Real estate
- Legal services
- Auto and transportation
- Business services and employment
- Construction, energy & utilities
- Education
- Insurance
- Healthcare
- Government

“
The increased prevalence of fraud has made transactions more cumbersome.

-Anonymous survey respondent,
Real Estate

For the real estate vertical in 2024 alone, Proof authorized transactions involving over **\$487 billion** in assets. The majority of transactions fall into high-risk categories like **affidavits, government documents, and powers of attorney**. These aren’t simple e-signatures. They’re high-value, fraud-prone transactions that demand airtight identity verification.

NOTARIZE.COM DOCUMENTS BY CATEGORY



The Need for Better Protection

As the attack surface expands and scammers become increasingly sophisticated, the threat grows. According to Verizon's 2025 Data Breach Investigations Report (DBIR), in 2024:

- **2.8 billion passwords** were leaked or sold online
- **61% of breaches** involved email addresses.
- **39% included phone numbers**, and **22% involved government-issued IDs**.⁵

⁵ Verizon Business 2025 Data Breach Investigations Report

⁶ CISA, Mobile Communications Best Practice Guidance

THE SIM-SWAPPING SITUATION

Phone numbers are increasingly being targeted—not just for robocalls or phishing texts, but to bypass SMS-based multi-factor authentication (MFA) via SIM-swapping attacks.

In a SIM swap, a fraudster convinces a mobile carrier to transfer the victim's number to a SIM card they control. This enables them to intercept calls and text messages, including one-time passcodes, effectively defeating SMS-based MFA.

Unlike deploying custom cellphone malware, SIM-swapping is relatively low-tech and well within reach for the average fraudster. While NIST and CISA explicitly discourage the use of SMS for MFA due to this vulnerability, many platforms still rely on it because of its simplicity and user familiarity.⁶

TOTP-based MFA (e.g., authenticator apps) and SIM protection services can harden authentication. However, in some cases fraudsters have access to TOTP seeds, allowing them to generate app-based codes themselves and bypass stronger MFA mechanisms.

More and more, CIOs and CISOs are beginning to phase out vulnerable MFA methods in favor of more secure, phishing-resistant forms of authentication, alongside real-time fraud intelligence platforms that monitor for the telltale signs of SIM-swapping and other targeted attacks.

In short: the building blocks of digital fraud—credentials, personal data, and access tokens—are cheap, abundant, and disturbingly easy to obtain across the **grey web, the dark web, and Telegram**.

Legacy protections like **passwords, KBA, and SMS-based MFA** are no longer **enough**. Passwords can be cracked, phones can be spoofed—even biometric data can be manipulated.

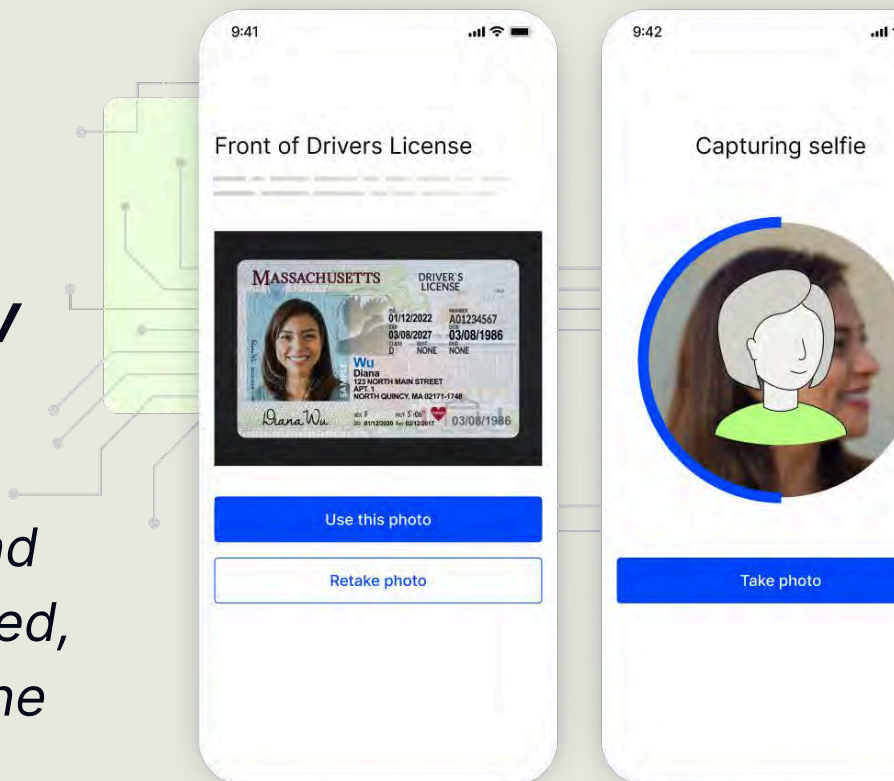
For years, the prevailing mindset was to **minimize friction** and only ask for identity verification when absolutely necessary. That approach has backfired leading to a **fragmented, high-cost model** where businesses repeatedly pay to verify the same consumer's identity using tools like KBA and document scans. It's a poor experience for users and a growing liability for businesses.

A modern approach flips the model: in high-risk flows, **verify the customer once, but do it with high assurance**. That may mean getting them on camera in front of a live agent. Fraudsters hate this—they don't want to be seen. And that's precisely why high-assurance verification still works.

The key is what comes next. Once verified, issue a **digital credential, token, or certificate** that proves their identity going forward. That way, the user doesn't have to keep re-sharing personal information, and businesses don't have to re-verify from scratch every time.

It's more secure, more private, and more cost-effective in the long run.

*Proof has verified **millions of unique individuals, 33% of whom are repeat IDV users**—a figure that continues to rise alongside the demand for secure, streamlined, and trustworthy online interactions.*



What Businesses Are Saying

The need for stronger fraud protection is being urgently felt by the people on the front lines. In a recent Proof survey of more than 80 fraud leaders and customers across industries, we found a sobering gap between **awareness and action**.

Concern is high, but confidence is low

- Over **80%** of respondents ranked fraud among their top business concerns in 2025. But more than **30%** said they were unsure of how their companies will address it in the coming year.

Most are seeing an uptick

- Nearly **40%** reported an increase in fraud attempts over the past year, driven by factors like deepfakes or other AI generated forgery. Close to **30%** noted a significant spike in fraud attempts across their organizations.

Many still can't measure it

- Shockingly, about **30%** of businesses said they don't have a clear way to track or quantify fraud across their systems. That means even teams investing in fraud tools may not be catching the full picture—or catching incidents at all.

This lack of clarity creates a dangerous feedback loop: fraud continues to rise, yet many organizations are flying blind—unable to benchmark risk, prove ROI, or adapt to evolving threats in real time.

Modern fraud prevention isn't just about better tools—it's about smarter insight. Businesses need solutions that **anticipate threats, verify intent, and build trust at every touchpoint**.



As a loan processor, I've seen increasing efforts by fraudsters attempting to submit falsified documents or use stolen identities.

-Anonymous survey respondent, Banking & Financial Services

The Generative AI Effect: Fuel for the Fraud Fire

Artificial intelligence isn't just transforming business—it's transforming cybercrime. We've crossed a dangerous threshold: it has become easier than ever for bad actors to **automate, scale, and personalize fraud using off-the-shelf AI tools**. Today's scammers don't need technical expertise or deep pockets. Running a convincing phishing campaign or generating a fake voice recording takes about as much effort as downloading a mobile app.

The FBI has issued urgent warnings about this shift, highlighting how generative AI is now being used to supercharge phishing, impersonation, and social engineering schemes. With a few prompts, fraudsters can **mimic real voices, create believable deepfake videos, or generate flawless forged documents**—all with unprecedented ease.



Gen AI could enable fraud losses to reach US\$40 billion in the United States by 2027, from US\$12.3 billion in 2023, a compound annual growth rate of 32%

– Deloitte's Center for Financial Services⁷

Deepfakes, in particular, are growing more convincing by the day. What used to be a novelty is now a serious liability for consumers, businesses, and financial institutions alike.

⁷ Deloitte, "Generative AI is expected to magnify the risk of deepfakes and other fraud in banking"

When Your Voice Becomes a Weapon

It takes **just a few audio clips** (like your outgoing voicemail, YouTube videos, or social media posts) for fraudsters to clone your voice. Using inexpensive, widely available AI tools, scammers can replicate not just the pitch and tone, but also the rhythm and cadence of how you speak. All they need is a snippet of your voice—often **pulled from social media, a podcast, or even a voicemail**.

Voice deepfakes are emerging as one of the most dangerous and emotionally manipulative forms of AI-enhanced fraud.

The \$40M Ozy Media voice fraud attempt

- Famously, in 2021, an executive from Ozy Media pleaded guilty to fraud and identity theft after using voice-faking software to pose as a YouTube executive on a call with Goldman Sachs. The aim was to convince the bank to invest \$40 million. The impersonation worked long enough to earn serious interest—before the deception unraveled.⁸

Major U.S. bank fooled in voice authentication test

- During a controlled experiment, one of the biggest banks in the country was successfully tricked by an AI-generated voice. While the bank emphasized that additional verification is always required for transactions, the incident highlights just how vulnerable voice authentication systems have become in the AI era.⁹

Faked voices, frantic parents

- Philadelphia attorney Gary Schildhorn testified before Congress in 2023 about receiving a frantic call from his "son," who claimed he'd been in a car accident and was in jail. The voice was tearful, urgent, and sounded exactly like his child. Schildhorn was about to wire money to a supposed attorney when—thankfully—his real son called, unharmed and unaware. The entire call had been a voice-cloning scam designed to exploit a parent's instinct to protect their child.¹⁰

⁸ The New York Times, "Goldman Sachs, Ozy Media and a \$40 Million Conference Call Gone Wrong"

⁹ The Wall Street Journal, "I Cloned Myself With AI. She Fooled My Bank and My Family"

¹⁰ Axios, "AI voice-cloning scams: A persistent threat with limited guardrails"

Seeing Isn't Believing: The Rise of Visual Deepfakes

As AI technology becomes more powerful and the corresponding hardware becomes faster and cheaper, fraudsters are progressing from audio deepfakes to **AI-generated faces and deepfake videos** to commit identity fraud. What once required Hollywood-level special effects can now be pulled off with a single photo and a free download.

In a recent study by Variety and HarrisX, **the majority of adults surveyed admitted to being fooled by AI-generated videos** created using OpenAI's Sora.¹¹ From fabricated celebrity endorsements to impersonated political figures, video deepfakes are muddying the waters of trust in a profoundly dangerous way.

\$25M heist via deepfake video call in Hong Kong

- An employee was tricked into wiring \$25 million to fraudsters after attending a video conference call filled with AI-generated replicas of senior company executives. The meeting looked legitimate. The people looked real. But none of it was.¹²

Impersonating the CEO of the world's largest ad firm

- Fraudsters created a WhatsApp account using a publicly available image of WPP CEO Mark Read, then invited an agency leader to a Microsoft Teams call. The scammers used AI-generated voice clones and YouTube footage to simulate a virtual meeting, impersonating Read via the chat window and voice audio. The goal? Trick the executive into launching a fake business and surrendering sensitive information. The scam failed—but only barely.¹³

Australian politicians used in Facebook investment scams

- Finance Minister Katy Gallagher, Foreign Minister Penny Wong, and even former PM Scott Morrison were digitally inserted into fake investment ads circulating widely on social media. These AI-generated video ads, which reached thousands before being removed, show just how quickly deepfakes can be weaponized for financial fraud—and how slow current systems are to stop them.¹⁴

¹¹ Variety, "Sora AI Videos Easily Confused With Real Footage in Survey Test"

¹² CNN, "Finance worker pays out \$25 million after video call with deepfake 'chief financial officer'"

¹³ Financial Times, "WPP boss targeted by deepfake scammers using voice clone"

¹⁴ The Guardian, "Deepfakes of Australian politicians including Penny Wong and Katy Gallagher used in investment scams"

¹⁵ Ars Technica, "Deep-Live-Cam goes viral, allowing anyone to become a digital doppelganger"

DIY DEEPPKAKES

The viral Deep-Live-Cam software project allows anyone to become a digital doppelgänger with just one photo. Sample videos show average users appearing as Elon Musk and J.D. Vance (among others) in real-time video chats. The open-source tool became the No. 1 trending repository on GitHub, signaling just how accessible (and popular) this technology has become.¹⁵

Synthetic Everything: Fake IDs, Forged Docs, and Fraud for a Price

Once upon a time, faking an ID or forging a bank statement took time, skill, and access to specialized tools. Today, it takes a prompt. Generative AI has made it nearly effortless to create realistic-looking fake documents—from **driver's licenses and passports to utility bills, pay stubs, and even professional credentials**. With nothing more than a few inputs, fraud actors can fabricate convincing digital identities designed to fool even the most advanced onboarding systems.

Across the dark web and Telegram, a cottage industry of **fraud-as-a-service** providers has emerged.

These vendors offer everything a bad actor needs to pass identity checks, beat KYC controls, and impersonate real people.

Docs 4 You

One service called Docs 4 You allows fraud actors to spin up entirely synthetic identities: driver's license, passport, selfie videos, and more. The goal isn't just a quick score—it's to build credit histories over time and later max them out for maximum profit.¹⁶

¹⁶ Reuters, "How AI will disrupt fraud prevention & detection technologies"

HOW SYNTHETIC IDENTITIES ARE CREATED

Synthetic identities are carefully engineered fraud constructs—built by blending real, stolen, and fabricated data to defeat identity verification systems. Here's how it's done:

1. Criminals generate ID documents containing a mix of real and fake information—such as a legitimate ID number combined with a fictional name and a slightly altered address.
2. Using Gen AI, scammers then create synthetic imagery that matches the photo on the forged document, enabling them to manipulate facial recognition and KYC systems.

These synthetic identities can slip past standard identity verification methods. As a result, traditional data checks are no longer enough.

Smarter, Faster, Scarier: AI Supercharges Phishing and Fraud Automation

The era of typo-ridden scam emails and clunky phishing attempts is over. Thanks to generative AI, fraudsters are no longer limited by poor grammar, awkward syntax, or limited resources. Today's phishing scams are **polished, personalized, and multilingual**—crafted by large language models that can convincingly mimic human tone and writing style across any context.

AI tools like OpenAI's ChatGPT are being repurposed to create **scam emails, fake investment pitches, and romance schemes** with near-perfect grammar and tone. They also accelerate fraud operations by reducing the time and effort needed to craft and localize messages.

But the threat goes beyond better emails. Generative AI enables fraud at scale. Social engineering attacks that once required manual effort can now be launched simultaneously against thousands of targets with **minimal human involvement**. The result: more victims, in less time, with fewer red flags.

Rise of Fraud-Specific AI Tools

While generative AI platforms like ChatGPT have been co-opted by criminals, more purpose-built adversarial tools are now being marketed specifically for cybercrime:

FraudGPT

Circulating on Telegram and sold via dark web forums, FraudGPT is a subscription-based AI tool designed exclusively for fraud. Prices start at \$200/month and go up to \$1,700/year. It's advertised as an all-in-one tool to help criminals write malware, build phishing pages, create scam letters, discover vulnerabilities, and even learn to code. As of mid-2024, the creator claimed over 3,000 paying customers.¹⁸

WormGPT

A darker sibling to ChatGPT, WormGPT allows users to generate persuasive phishing messages, execute BEC (business email compromise) attacks, and create malicious code. It operates on the same foundational language models—but with no ethical guardrails or use restrictions.¹⁶

PassGAN

This AI-powered password-cracking tool uses machine learning and neural networks to guess passwords with shocking speed and accuracy. In a recent study, PassGAN cracked 51% of passwords in under a minute, 65% within an hour, and over 80% within a month.¹⁹



Generative AI
email fraud losses
could total about
US\$11.5 billion by
2027

– Deloitte's Center for Financial
Services⁷

Business email compromise (BEC) is big business

In 2024, more than

\$6.3B

was stolen through BEC scams.

The median loss per incident is

\$50K

across 19,000 different complaints.

That's not petty theft. That's enterprise-scale fraud, executed one inbox at a time.¹

From Bots to Autonomous Fraud Agents

Traditional bots followed scripts. Modern AI agents can **think, adapt, and act**. These autonomous agents, sometimes referred to as agentic AI, can make decisions, adjust to user behavior in real time, and continuously learn from interactions.

That means criminals will soon be able to deploy systems that never sleep, never repeat themselves, and never get tired—perfect for:

- **Scraping personal or financial data**
- **Executing credential-stuffing and brute-force attacks**
- **Evading traditional fraud detection systems**

Current fraud tooling—focused on detecting human behaviors like typing speed or IP anomalies—**falls short when confronting AI agents**, whose behaviors don't match human patterns at all.

KNOW YOUR AGENT: A NEW VERIFICATION FRONTIER

In this new age of autonomous fraud, a pressing challenge emerges: How do we verify the identity of an AI agent? Traditional Know Your Customer (KYC) systems don't apply when the "user" is an intelligent bot. Fraud prevention systems are not yet equipped to detect or respond to agentic fraud activity without generating false positives that frustrate real users.

Until the ecosystem develops better tools to detect, verify, and limit AI-driven transactions, agentic AI will remain a growing blind spot—one that's already being exploited by bad actors.

¹⁸ Dark Reading, "FraudGPT! Malicious Chatbot Now for Sale on Dark Web"

¹⁹ Reuters, "Identity theft is being fueled by AI & cyber-attacks"

We're Losing Ground

The hard truth? We're losing the battle against AI-enabled fraud.

Fraud detection systems were designed to stop yesterday's scams—predictable, manual, and easier to spot. But today's fraud is **automated, adaptive, and dangerously scalable**. AI makes scams faster, cheaper, and harder to detect.

AI even allows fraudsters to **evolve in real time**, adjusting attacks as systems respond. This level of dynamic adaptation renders static rule-based detection models ineffective. As synthetic identities become harder to distinguish from legitimate ones, the **cracks in legacy verification systems are widening**.

Businesses are feeling the pressure to protect their customers and themselves. According to a 2025 Liminal buyer survey:

- **68% of buyers** expressed concerns about their fraud tools' ability to withstand threats like social engineering and rapid attack execution.
- **76% of enterprises** say growing user bases and AI-enabled threats are forcing them to rethink fraud prevention—fast.

The takeaway? **AI is redefining the rules of engagement**, and if organizations want to stand a chance, they need more than traditional tools—they need integrated, adaptive, and AI-powered defenses that evolve as fast as the threats do. At the same time, it's worth examining how this shift is being approached from a regulatory perspective.

Remote work, real risks: Inside a modern-day laptop farm

While GenAI is dominating headlines (and rightly so) it's important not to lose sight of the fact that other forms of fraud are still thriving.

Case in point: the recent Wall Street Journal exposé on how North Korea is infiltrating U.S. companies via remote work scams. Authorities uncovered a "laptop farm" run by Christina Chapman, a 50-year-old former waitress turned TikTok personality. With just a few laptops connected to remote access software, she helped North Koreans nationals land remote tech jobs at over **300 American companies**.

They collected more than **\$17 million in fraudulent pay**, while Chapman managed logistics—handling paperwork, faking tax records, and shipping employer-provided devices overseas.

The story is a reminder that while AI-powered threats are escalating, more basic scams still fly under the radar—especially when they exploit blind spots like remote hiring, lax identity checks, and gig economy loopholes. ²¹

²⁰ Liminal, "Solving Advanced Fraud in Account Opening"

The Policy Gap: Fraud Moves Fast. Regulation Doesn't.



Fraud is evolving faster than the policies designed to stop it. While regulators debate the future of AI, criminals are already exploiting it—at scale. What’s missing? A modern policy framework built for speed, adaptability, and impact.

HERE’S WHAT NEEDS TO CHANGE.

1. Let the Good Guys Use the Good Stuff

Right now, fraudsters have unfettered access to cutting-edge tools. Defenders? Not so much. Well-intended efforts to regulate AI risk slowing our ability to deploy the technologies designed to prevent fraud in the first place. If we treat all AI the same, we risk tying the hands of those trying to stop crime while giving bad actors a head start.

What’s needed:

Carve out explicit exemptions for fraud detection, prevention, and investigation in any AI-related legislation. Regulators should fast-track approval of high-assurance tools (like advanced identity verification, real-time fraud analytics, and behavioral detection models) especially in high-risk sectors like healthcare, finance, and energy.

Setting up regulatory sandboxes will allow industries to test and scale these technologies responsibly, without red tape slowing everything down.

A better way forward

Deepfake detection is important. So are the efforts to outlaw AI-enabled impersonation.

But the real fix? Leverage digital credentials issued with high-assurance to positively verify a person’s identity, and let others rely on that trusted credential in daily transactions.

That’s exactly what Visa did with the card in your wallet. Now it’s accepted worldwide. We need a similar model for digital identity.

²¹ The Wall Street Journal, “North Korea Infiltrates U.S. Remote Jobs—With the Help of Everyday Americans”

2. Flip the Fraud Response Model

Many of the policies that exist today to protect consumers and businesses from bad actors were never really designed for fraud prevention.

The focus by U.S. financial regulators on combatting money laundering and terrorist financing remains important, but the surge of AI-driven fraud warrants a reassessment of our current approach. Our existing infrastructure is backward-looking, focusing too much on post-incident reporting (like Suspicious Activity Reports). These are useful for investigations, but ineffective at stopping live attacks.

What's needed:

Shift from reactive to real-time fraud prevention.

Inspired by payment networks, we need a new fraud intelligence framework, built around tokenized identities and privacy-preserving data sharing. If one institution flags a suspected fraudster, others should be alerted immediately. Fraudsters shouldn't get a second chance at a different bank.

3. Crack Down on Fraud-as-a-Service

As noted previously, entire black-market ecosystems now exist to generate fake identities, sell synthetic documents, and automate attacks using AI tools.

From deepfake generators to phishing-as-a-service subscriptions, the business of frau...

What's needed:

Governments must go beyond chasing individual actors and start targeting the businesses enabling fraud at scale. That means:

- Criminalizing the sale and distribution of synthetic identity kits
- Prosecuting operators of AI-powered fraud tools like FraudGPT, WormGPT, and PassGAN
- Applying financial sanctions or takedown authority to platforms that knowingly support or host this activity

Fraud has become a product. It's time regulators treated it like one and shut the suppliers down.

4. Enable Law Enforcement to Stop Modern Fraud

While impersonation and forgery are already serious crimes, our laws simply weren't written for deepfakes, voice clones, or digital impersonation.

What's needed:

Update the existing criminal code to explicitly outlaw Gen-AI enabled fraud. This removes the guesswork for law enforcement, accelerates investigations, and sends a clear signal: digital deception is a crime, not a loophole.

5. Protect Your Face. And Your Voice. And Your Digital Self.

No one should ever live with the fear that a stranger is digitally impersonating them—using their voice, face, or likeness to scam others or ruin their reputation.

Americans deserve clear protections against the malicious use of their digital likeness. While there are some legitimate reasons to create a digital replica, the unauthorized impersonation of someone's identity—especially for deception or personal gain—should be prohibited.

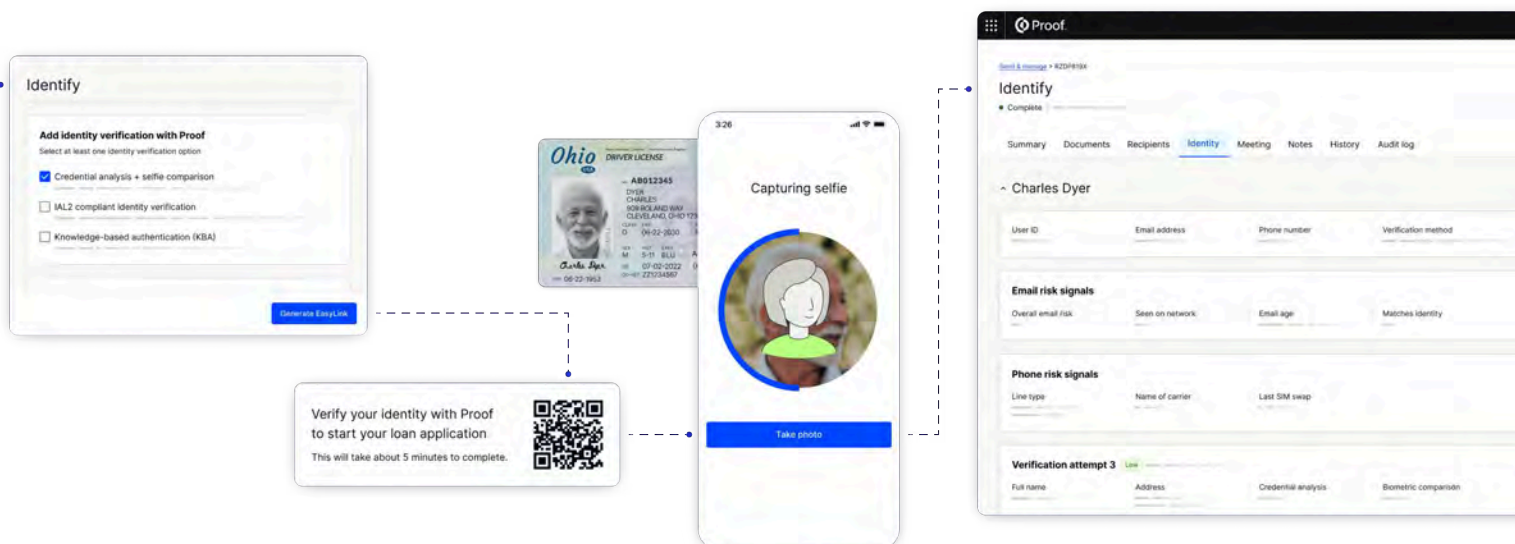
What's needed:

It's time to recognize our identities as personal property—especially online. Platforms that create or host digital avatars or digital twins should be required to meet baseline standards:

- **Security:** Require investment in cybersecurity practices to weed out the fly-by-night vendors looking to make a quick buck. Biometric data should be treated like health records—safeguarded with clear, enforceable standards.
- **Verification:** Platforms must perform a series of checks to confirm that users own the identity data they submit.
- **Consent:** Every use of a digital likeness must require explicit opt-in from the person being represented.

Fraud policy needs a hard reset. That starts by enabling innovation, shutting down fraud supply chains, and enshrining protections that reflect today's threats—not yesterday's assumptions.

We don't just need to catch up. We need to get ahead.



What You Can Do Now: Practical Takeaways for 2025

Fraud isn't just a technology problem. It's a people problem, too. And whether you're a consumer or a company, your choices matter.

For Consumers: Stay One Step Ahead

The fraudsters are fast—but with vigilance and a few smart habits, you can stay faster.

- **Pause before you trust.** If something feels off—a weird URL, an urgent request, an unfamiliar voice—don't act on instinct. Verify it through a separate channel.
- **Don't trust traditional ID checks alone.** Deepfaked videos, spoofed websites, and polished fake IDs can appear convincing. Scammers count on that.
- **Protect your data. Use strong, unique passwords.** Enable MFA using an authenticator app—not SMS. Freeze your credit if you're not using it.
- **Monitor and report.** Check your accounts and credit activity regularly. Report anything suspicious. One complaint might stop a chain reaction.

Fraud is now emotional, intelligent, and personalized. Staying safe starts with staying skeptical.





For Businesses: How to Spot—and Stop—Fraud Before It Strikes

2025 made one thing clear: fraud prevention isn't static. It's an ever-evolving process, and the most effective defenses share three traits:

1. Layered

Don't trust a single signal. Combine device fingerprints, behavioral data, and document checks. Ask:

- Is this a known device?
- Has this person behaved this way before?
- Does the location make sense?

2. Dynamic

Rules alone won't cut it. Risk levels change by the minute. Platforms must dynamically orchestrate the right verification method for the moment, based on context, use case, and law.

3. Human-In-The-Loop

AI can catch patterns. But people catch nuance. The most effective systems escalate risky transactions to a live agent when things don't add up. Additional best practices:

- Build fraud awareness across teams (especially in finance, HR, and compliance).
- Maintain clear audit trails and encourage a culture of internal transparency.
- Collaborate across industries to share anonymized threat intelligence and strengthen collective defense.

At Proof, we believe that identity verification isn't a checkbox—it's a continuous trust signal. The businesses that approach it that way to protect themselves and their customers will stay ahead.



Our team strengthened document verification and partnered with compliance to detect red flags early. Continued investment in fraud prevention tools is essential to protect both our clients and the company.

– Anonymous customer,
Banking & Financial
Services

Looking Ahead: The Future of Fraud Prevention

We're entering a new chapter—one where fraud can be fully automated, identity can be convincingly faked, and detection can't rely on yesterday's playbook.

Autonomous fraud is on the rise.

Bots can now learn, adapt, and execute attacks in real time, without human input.

Legacy defenses can't keep up.


Passwords, ID scans, and SMS-based MFA are no match for today's threats.

Fraud prevention must shift.

Waiting until after the fact is no longer an option. Protection must happen before the fraud does.

For businesses, that means investing in real-time, adaptive identity infrastructure. For consumers, it means staying sharp—even when everything looks legitimate.

This report should be a wake-up call. But it's also a roadmap.



Fraud is evolving.
It's time our defenses did too.

Ready to build fraud prevention
that keeps up?

[\[Contact the Proof team →\]](#)

