IDENTITYIQ

IDENTITYIQ FRAUD REPORT

2025 FRAUD REPORT.

The surge in credit-based fraud, the rise of AI-driven scams, and what to expect in 2026.

65%

surge in alerts tied to suspected fraudulent new accounts — year over year.

THE HEADLINES

2025, at a glance.

Three numbers tell the story of how fraud changed this year, and why the damage is lasting longer than ever.

^65%

New-account fraud alerts

IdentityIQ member alerts tied to suspected fraudulent new credit accounts jumped 65% in 2025 versus 2024, the clearest signal that criminals are opening credit lines in victims' names at an accelerating pace.

^39%

Major derogatory events

Charge-offs, collections, bankruptcies, and foreclosures climbed sharply, the downstream damage when fraud is not caught in time. Fraud is no longer a single event; it's a financial wound that keeps bleeding.

^32%

Derogatory Tradelines

Late payments, defaults, and collection statuses on individual accounts are up nearly a third, pulling credit scores down and stretching recovery timelines into years rather than months.

THE NEW REALITY

Fraud is faster. And it hits harder.

According to proprietary IdentityIQ data, alerts to members tied to suspected fraudulent new accounts climbed **65% in 2025 versus 2024**. That spike is more than a statistic. It's the sound of identity fraud accelerating across millions of consumer credit profiles in real time.

A major driver is artificial intelligence. AI is making fraud more convincing, harder to detect, and dramatically easier to scale. Criminals are no longer just stealing identities, they're weaponizing them on the spot. With AI tools they automate applications, fabricate synthetic identities, and mimic legitimate behavior at scale. New credit lines open, balances rise, and damage compounds long before the victim sees the first sign.

And the impact doesn't stop with the initial account. IdentityIQ data shows a sharp increase in serious credit damage, like collections, defaults, charge-offs, and derogatory tradelines, much of it the direct downstream effect of fraud caught too late.

What begins as a single unauthorized account can quickly cascade into missed payments, collections, and long-term credit damage that takes years to repair. With AI amplifying both speed and scale, today's fraud is more coordinated, more persistent, and more financially destructive than at any point in recent memory.

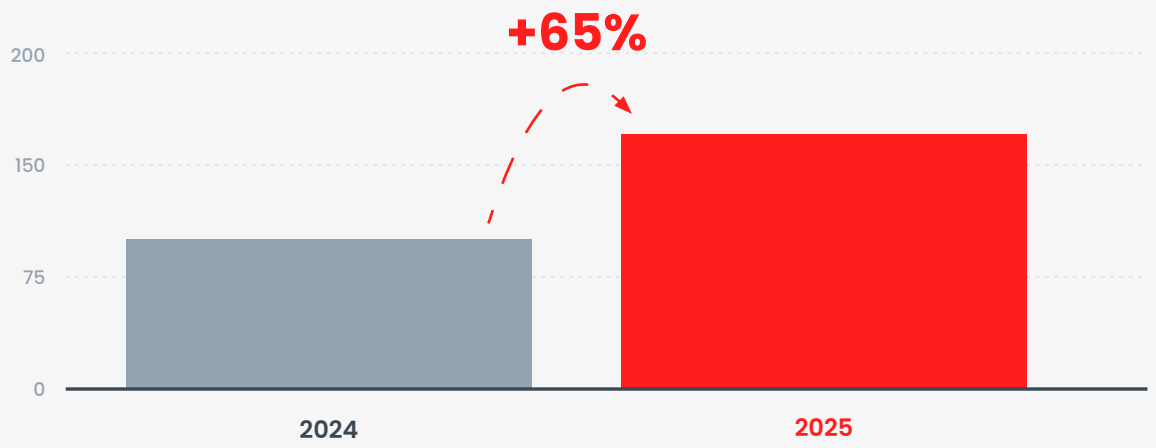
> A 65% spike in possible fraudulent new account alerts shows identity fraud is accelerating rapidly. Protecting your identity and monitoring your credit early are critical to limiting the damage.
>
> **MICHAEL SCHEUMACK**
> Chief Innovation Officer, IdentityIQ

TREND 01 • UNAUTHORIZED OPENINGS

Credit accounts are being opened — without permission.

New-Account Fraud Alerts

IdentityIQ member alerts triggered when a new credit line appears on a profile.



New-account alerts fire when a credit card, auto loan, or other tradeline appears on a consumer's credit profile. Some of these are normal life events, but a surge of this magnitude is a flashing warning sign that credit is being opened without consumers' knowledge or consent.

Fraudulent accounts opened in victims' names

- Criminals use stolen personal information to apply for credit cards, loans, and financing.
- Accounts often go undetected until balances go unpaid and damage shows up on credit reports.

Synthetic identity theft

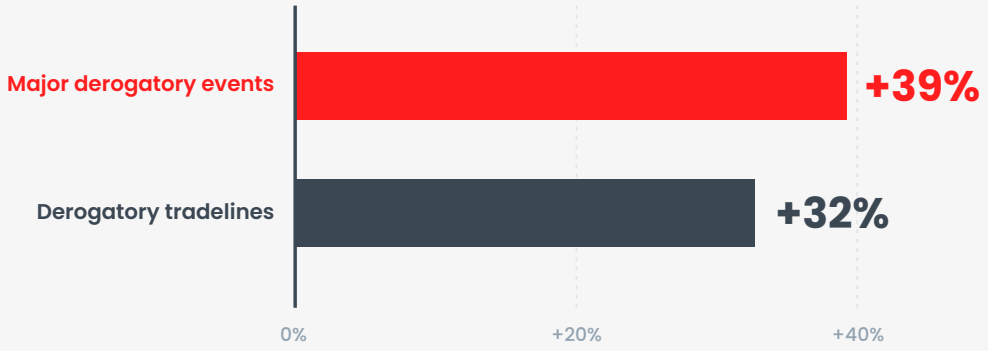
- Fraudsters combine real data (like a Social Security number) with fabricated details to invent entirely new identities.
- Synthetic profiles appear legitimate to lenders and are used to open multiple credit lines at once.

TREND 02 • LONG-TERM DAMAGE

Fraud isn't a one-time hit. It's a lasting wound.

Downstream Credit Damage · Year-over-Year Change

Both indicators measure what happens after fraud is missed. And both are climbing together.



A **major derogatory event** is a serious negative mark on a credit report, like a charge-off, account in collections, bankruptcy, or foreclosure. A **derogatory tradeline** is an individual account with negative activity, like late payments, defaults, or collections.

These two indicators rise together when fraud isn't caught in time. The pattern is familiar and predictable:

The fraud cascade

- Fraudulent account opens and is used.
- Balances go unpaid; late payments accrue.
- Accounts go to collections or are charged off.
- Credit scores drop sharply; recovery takes years.

Why it keeps growing

- More cases now go undetected for longer.
- AI lets criminals run more scams in parallel.
- Synthetic identities don't have an obvious "victim" to alert lenders early.
- Unpaid balances pile up before alarms fire.

YOUR PLAYBOOK

Stop credit-based fraud before it spreads.

As fraud increasingly centers on unauthorized credit activity, early detection and proactive monitoring are non-negotiable. These seven moves can stop fraud before it escalates.

01

Monitor your credit

Review credit reports and alerts regularly. New-account alerts can flag unauthorized openings before damage builds.

02

Freeze or lock your credit

Restricting access to your credit file is one of the most effective ways to block fraudulent account openings outright.

03

Verify before you share

Only share personal data through trusted, confirmed sources. Scammers now use AI-generated voices and messages to impersonate institutions and even people you know.

04

Beware of urgency

Pressure to act immediately is one of the loudest fraud signals. Pause, verify, then act — never the other way around.

05

Act fast on suspicious activity

Spot an unfamiliar account or alert? Contact your lender and the credit bureaus immediately to stop the spread and limit damage.

06

Protect your personal data

Limit what you share online. Use strong, unique passwords paired with multi-factor authentication on every account that matters.

07

Use an identity theft protection service

Enroll in continuous monitoring of your credit, personal information, and financial activity, paired with real-time alerts and recovery support, to catch fraud before it compounds.

THE NEXT EVOLUTION

AI is rewriting the fraud playbook.

AI is changing the fraud landscape at record speed, giving criminals tools to run scams that are more convincing, more personalized, and easier to scale than ever before.

22,000+

complaints tied to AI-enabled fraud

Source: FBI · 2025 · first year formally tracked

~$900M

in U.S. losses from AI-driven scams

Source: FBI · 2025

The Federal Trade Commission has reported billions in total fraud losses in recent years, with impersonation and phishing, now turbocharged by AI, among the fastest-growing scam categories.

Deepfakes & impersonation

- AI-generated audio and video impersonate family members or executives demanding urgent money transfers.
- Banks, government agencies, and trusted brands are spoofed convincingly.
- Fake celebrity and expert endorsements push fraudulent investment schemes.

Smarter, sharper phishing

- Highly personalized emails crafted from public online activity. No more typos or red flags.
- Real writing styles copied to mimic people you actually know.
- Believable fake websites generated in seconds, hosted in minutes.

YOUR AI DEFENSE

Don’t trust your eyes. Verify everything.

AI scams are engineered to look and sound real. As tactics get sharper, four habits protect you most.

01

Create a family verification code

Deepfake voices and faces are getting eerily convincing. Agree on a private code phrase that only trusted people know and use it to confirm identity during any urgent or unusual request involving money or sensitive info.

02

Verify before you trust

A call, message, or video looking real isn’t proof. If something feels urgent or unusual, verify through a separate, trusted channel using contact info you already had, not what was given to you in the message.

03

Slow down urgent requests

AI scams manufacture pressure to act now. Pause before responding to anything involving money, credentials, or personal data. Urgency is one of the strongest indicators of fraud.

04

Limit what AI can learn about you

Fraudsters use publicly available data to personalize attacks. Shrink your digital footprint, review privacy settings across platforms, and think twice before posting personal details, locations, or routines.

THE BOTTOM LINE

Awareness and caution are the strongest lines of defense.

Fraud is evolving from isolated incidents into complex, long-term financial threats. The sharp rise in unauthorized credit activity and derogatory credit events highlights a new reality. Today's fraud is more strategic, more scalable, and more damaging than ever before.

At the same time, AI is accelerating this evolution, arming scammers with tools that make scams more convincing and harder to detect. Consumers must take a proactive approach by monitoring their identity and credit, verifying communications, and staying informed about emerging threats.

ABOUT

IdentityIQ

IdentityIQ®, offered by IDIQ®, is a leading provider of identity theft protection, credit monitoring, and financial wellness solutions, serving more than **6 million members** nationwide. Combining advanced monitoring technology, real-time fraud alerts, rent and utility payment reporting, and U.S.-based identity restoration services, IdentityIQ helps consumers protect what matters most and build a stronger financial future.

Recognized by Best Company, TechBullion, and the Inc. 5000 list of America's fastest-growing private companies, IdentityIQ continues to deliver innovative protection designed for today's evolving financial and identity threats.