

## IDENTITYIQ Q1 2026 FRAUD REPORT

# FRAUD IS NOW INDUSTRIAL.

New-account fraud is accelerating at a record pace.  
And AI is the engine driving it.

---

# 123%

Q1 2026 surge in fraudulently opened new accounts year over year, the fastest Q1 growth on record.

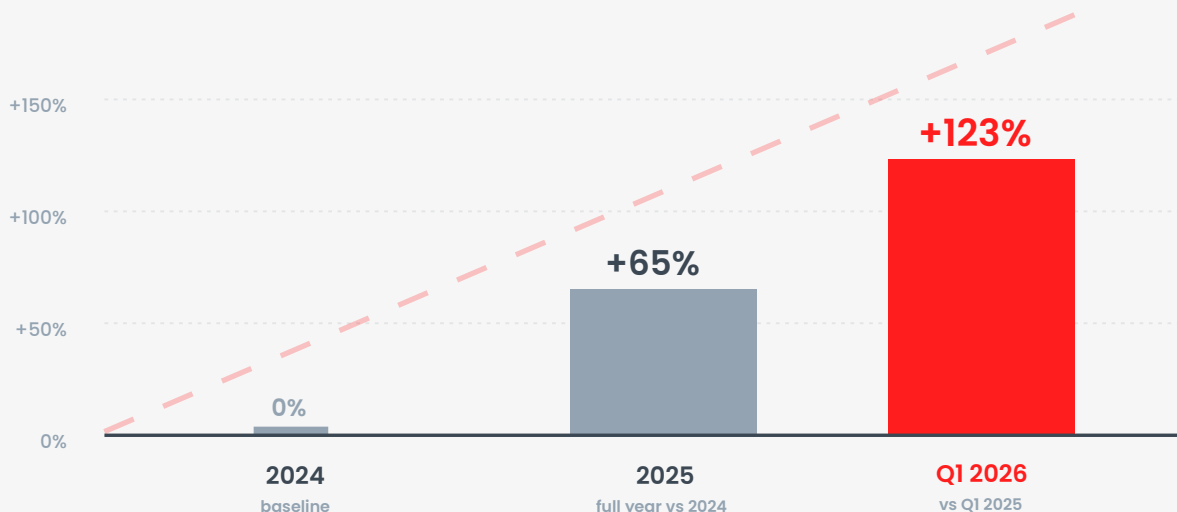
## THE ACCELERATION

# Faster than expected. And **still climbing.**

Proprietary IdentityIQ data shows fraudulently opened new accounts, credit cards, auto loans, and other trade lines, jumping **123% in Q1 2026 versus Q1 2025**. That's the fastest Q1 growth on record, and nearly double last year's already-elevated 65% spike.

### New-Account Fraud • Year-over-Year Growth

Each bar represents the YoY increase in suspected fraudulent new accounts opened, per IdentityIQ proprietary data



This level of acceleration isn't random. It signals a shift in *how* fraud is being committed, from opportunistic, one-off attacks to coordinated, AI-driven operations capable of opening multiple unauthorized accounts before a single consumer realizes anything is wrong.

## WHAT'S DRIVING IT

# Synthetic identities. AI at scale.

The sharp rise in new-account fraud is being driven, in large part, by two forces working together: **synthetic identity fraud** and the rapid adoption of **AI** by criminal operations.

Synthetic identity fraud combines real personal data, like a Social Security number, with fabricated information to create entirely new identities. To lenders, these profiles often look legitimate, which makes them notoriously hard to detect. AI now makes the entire process faster, cheaper, and dramatically more scalable.

### What AI lets criminals do now

- Generate realistic synthetic identities in seconds.
- Automate credit applications across dozens of lenders simultaneously.
- Mimic normal consumer behavior to dodge fraud-detection models.
- Iterate and refine attack patterns at machine speed.

### Why it's hitting harder in 2026

- Synthetic profiles have no human "victim" to alert lenders early.
- Multiple accounts open before any alarm fires.
- AI-generated applications look indistinguishable from legitimate ones.
- Each successful attack trains the next one to be even sharper.



This level of acceleration isn't happening by accident. It's being fueled by AI. Fraudsters are now using AI to scale identity theft faster than ever, automating everything from synthetic identity creation to real-time application submissions. By the time a consumer realizes something is wrong, multiple accounts may already be open. The 123% spike is a clear signal that AI has shifted fraud from opportunistic to industrialized.

**MICHAEL SCHEUMACK**

Chief Innovation Officer, IdentityIQ

## THE DOWNSTREAM

# One fraudulent account. A **cascade** of damage.

New-account fraud is rarely the end of the story. It's the first link in a chain. Once an unauthorized account is open, the damage spreads quickly, often long before the victim sees a single warning sign.



### Unpaid balances

Fraudulent accounts rack up debt fast, and the bill lands on the victim's credit file before they know the account exists.



### Collections & chargeoffs

Unpaid fraudulent accounts get sent to collections or charged off, leaving major derogatory marks that don't disappear easily.



### Credit score drops

Scores tumble fast and stay down. Recovery can take years, even after the fraud is reported and disputed.

The jump from a 65% increase in 2025 to **123% in Q1 2026** tells a clear story: fraud is happening earlier in the consumer's credit lifecycle and spreading faster across credit profiles than it ever has. The longer it goes unnoticed, the deeper the damage, which is why early detection now matters more than ever.

# +58pts

Year-over-year growth nearly doubled.

Annual growth jumped from +65% (2025) to +123% (Q1 2026). That's a 58-point acceleration in the pace of new-account fraud.



## YOUR PLAYBOOK

# Catch credit fraud **early.**

When fraud is moving this fast, visibility is everything. These five habits give consumers the best shot at catching unauthorized activity before it cascades.

**01****Monitor credit reports and alerts**

Review your credit reports regularly and pay attention to alerts. New-account notifications are often the earliest signal that something is wrong.

**02****Freeze or lock your credit**

A credit freeze or lock is the single most effective way to block fraudulent account openings outright, and it can be lifted in minutes when you need it.

**03****Verify any request for personal info**

Before sharing personal details, confirm the request through a separate, trusted channel. AI-generated voices and messages now impersonate banks, agencies, and even people you know.

**04****Act fast on suspicious activity**

Spot an unfamiliar account or alert?  
Contact your lender and the credit bureaus immediately to limit the spread and start the dispute process.

**05****Use an identity theft protection service**

Continuous monitoring of your credit, identity, and financial activity, paired with real-time alerts and restoration support, is the most reliable way to stay ahead of AI-scale fraud.

## SCAM SPOTLIGHT

# “I’m not a robot.” But this isn’t real.

Fake reCAPTCHA scams are exploding in 2026. Cybercriminals are weaponizing one of the internet’s most trusted security tools, the familiar verification box, because users instinctively trust it and rarely pause to question it.

1

### Victim lands on a compromised page

A fake streaming page, phishing email link, sponsored search ad, or even a cloned retail site. The destination looks ordinary.

2

### A realistic CAPTCHA prompt appears

A convincing CAPTCHA or Cloudflare-style verification screen asks the user to “verify you are human.” Everything looks legitimate.

3

### Error: Complete a few verification steps

The page reports an error and instructs the user to complete “verification steps” using their keyboard. This is the trap.

4

### The user is told to press these keys

A short sequence silently launching malicious commands behind the scenes:

Windows + R

CTRL + V

Enter

5

### Malware silently installs

Credential thieves, spyware, or remote-access tools deploy in seconds, immediately harvesting passwords, browser cookies, banking credentials, cryptocurrency wallets, and active login sessions.

## YOUR DEFENSE

# Spot the fake. Skip the **click**.

The single biggest red flag: any CAPTCHA page that asks users to perform keyboard shortcuts or paste commands into their computer. **Legitimate CAPTCHA systems never do this.**

**01****Never paste CAPTCHA “commands”**

If a verification page asks you to press Windows+R, CTRL+V, or run anything on your keyboard — stop. That’s a malware delivery attempt, not a CAPTCHA.

**02****Avoid suspicious links and ads**

A credit freeze or lock is the single most effective way to block fraudulent account openings outright, and it can be lifted in minutes when you need it.

**03****Check URLs carefully**

Cloned sites often use lookalike domains with small misspellings or extra characters. Verify the URL before interacting with any verification prompt.

**04****Keep software updated**

Up-to-date operating systems, browsers, and security tools close the vulnerabilities that malware needs to take hold after a successful keystroke trick.

**05****Enable multi-factor authentication**

Even if credentials are stolen, MFA can stop attackers from logging in. Turn it on for email, banking, and any account that holds value.

**06****Exit suspicious verification pages**

When in doubt, close the tab. If you’ve already interacted with a fake page, monitor your accounts, run a malware scan, and change passwords immediately.

## YOUR DEFENSE

# Fraud has gone industrial. Protection has to keep up.

The 123% increase in new-account fraud in Q1 2026 isn't a blip. It's evidence that fraud is becoming faster, more scalable, and more sophisticated. What was already a growing issue in 2025 has rapidly evolved into an AI-driven, synthetic-identity-powered threat operating at industrial scale.

Staying ahead now requires a more proactive approach: continuous credit monitoring, faster response times, and tools designed to spot fraud before the damage compounds. Awareness is no longer enough on its own.

## 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.