Fingerprint


# The many faces of **new account fraud** & *what you can do about it*

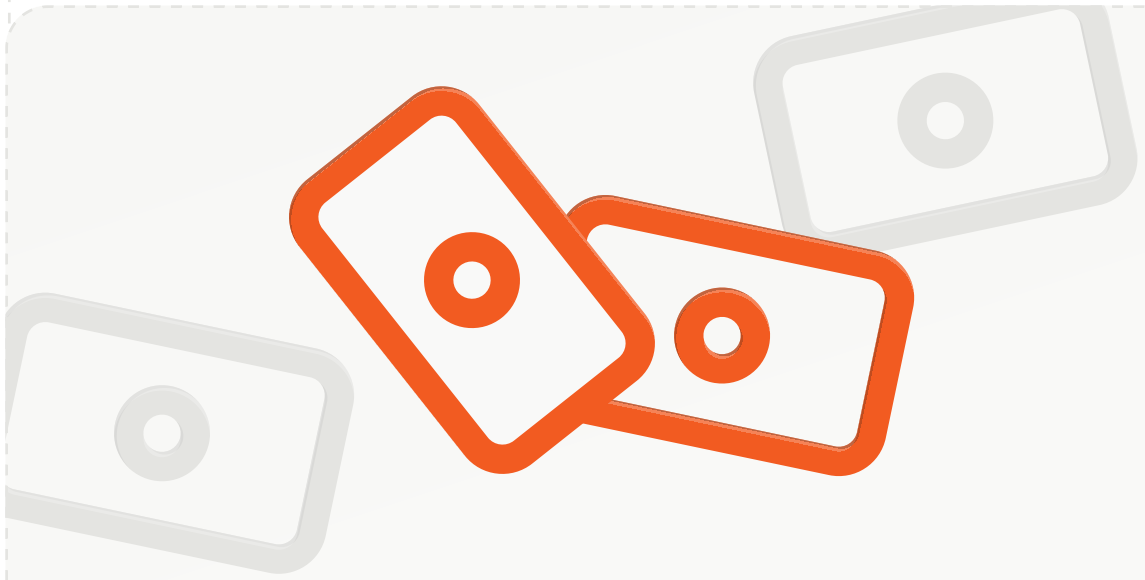
# Table of contents

## Introduction

New account fraud is a costly headache that distorts customer acquisition metrics. Unfortunately, it's increasingly common. According to TransUnion, one out of seven new account creations is an attack. In terms of financial losses, Javelin Strategy & Research estimated that new account fraud caused $5.3 billion in losses in 2023, a 35% increase from the previous year.

It affects a broad cross-section of organizations: At community colleges in California, teachers and administrators struggle to stem the tide of financial-aid-stealing bots enrolling fake students in online classes. Scammers use new accounts to create unique fake profiles on dating websites to swindle legitimate users. Fraudsters open new accounts to repeatedly claim first-time user promotions on gaming and food delivery apps.

With generative AI and app cloning tools making it easier than ever to scale malicious activities, it’s crucial to get a handle on how new account fraud works and how to prevent it.



**$5.3 billion**

was lost due to **new account fraud** in 2023

## What is new account fraud & what are the effects?

New account fraud is the act of creating an account (or multiple accounts) under false pretenses to deceive the site operator or fellow users. The goal of new account fraud is most often to gain access to financial benefits, bonuses, or services that the fraudster isn't supposed to get. Fraudsters also abuse accounts to break the rules, such as spreading spam, posting fake product reviews, or circumventing a ban for violating the terms of service.

It's not always just one person making one fake account to get another coupon code. It's often repeat behavior, carried out by sophisticated actors using bots, device farms, or emulators to create and cycle through hundreds or thousands of accounts.

**The impacts for online businesses and other organizations can be enormous:**

- **Lost revenue.** Companies lose money when bad actors repeatedly claim promos, file fraudulent chargebacks (aka first-party fraud), or take out credit they don't plan to repay.
- **Distorted growth metrics.** Large numbers of fraudulent new accounts can make it difficult for a business to determine customer acquisition costs (CAC) accurately. Meanwhile, large volumes of fake accounts can make marketing campaigns appear more successful than they really are.
- **Downstream issues.** Unchecked new account fraud can lead to problems like high chargeback rates, account takeover attacks, identity theft, or spam flooding your platform.
- **Loss of trust in the platform.** Sites with a high proportion of bot accounts and predatory users may suffer a diminished reputation in the marketplace.

For fraudsters, the appeal is a relatively low-risk, high-reward way to get access they shouldn't have. It's also often less complicated and detectable than launching an account takeover attack.

**$3.1 billion**

Estimated lender exposure to credit obtained with synthetic identities in 2023,

– TRANSUNION'S 2024 STATE OF OMNICHANNEL FRAUD REPORT.

## New account fraud is on the rise

Ease of access compared to other forms of fraud is one of the reasons new account fraud has become more popular in recent years. Compared to an account takeover attack, applying for a new account through an online portal is relatively simple.

“In lieu of using traditional tactics to gain access to and ultimately compromise existing accounts, fraudsters are increasingly choosing to create new accounts that they can control themselves,” said Steve Yin, senior vice president and global head of fraud solutions at TransUnion, in remarks to betting industry news site SBC Americas.

One specific kind of new account fraud has even prompted warnings from experts: synthetic identity fraud, a.k.a. Frankenstein fraud. The practice involves taking authentic data from different individuals — for instance, a Social Security number from one, an address from another, and a checking account number from a third — and recombining it to invent a fake person with details that appear real to automated fraud detection programs. In some cases, fraudsters may open credit cards with a synthetic identity and even pay off small amounts to establish good credit and make the identities seem more legitimate.

TransUnion found in its 2024 State of OmniChannel Fraud Report that synthetic identity fraud is the fastest-growing form of digital fraud. They estimated lender exposure to credit obtained with synthetic identities at $3.1 billion in 2023.

And that’s just one kind of new account fraud.

With this background, let’s take a more detailed look at different types of new account fraud, how they work, and what you can do about them. There’s overlap in these categories, but each section discusses a distinct aspect of how bad actors are using new account fraud.

## Multi-accounting fraud

As a term, multi-accounting fraud can sometimes be used interchangeably with new account fraud. In this section, we use the term to refer to when someone creates and uses numerous accounts, often in parallel, to get around limits on single users or to use stolen identities and credentials at scale. Some examples of multi-accounting fraud include:

- A fraudster who opens multiple accounts on an e-commerce site to quickly validate large numbers of stolen credit card numbers, a practice known as card testing.
- An online gambler who creates multiple profiles to manipulate odds or collude for an unfair advantage. A player with multiple accounts can take up several seats at a table to stack odds for or against other players, or place opposing bets for the same event to guarantee a win.
- An identity thief who uses stolen personal data, often purchased on the dark web, to apply for new credit cards or bank accounts and obtain credit without intention to repay.

This last kind of fraud is particularly perilous for banks and fintech. These attacks are not only costly in terms of lost revenue but can also pose Know Your Customer (KYC) and anti-money laundering (AML) compliance risks. In 2024, for example, Toronto Police broke up a 12-person Canadian fraud ring that used 680 synthetic identities to open hundreds of bank accounts and lines of credit, which were used to make online purchases and transfer money.

According to U.S. Federal Reserve payments fraud expert Mike Timoney, opening multiple new accounts gives malicious actors plenty of opportunities to commit various types of crimes. “It gives [fraudsters] access to the banking system,” Timoney said in an interview. “It gives them access to places where they can move money through.” The thousands of data breaches that occur every year also provide a steady stream of stolen personal data for fraudsters to mine.

### How to fix multi-accounting fraud

No single approach can fully tackle multi-accounting fraud, but several best practices can help:

- **Multi-factor authentication (MFA).** Add layers of verification to make it more cumbersome for fraudsters to create multiple accounts, especially on a large scale. Examples include emailing magic links, sending OTPs (one-time passwords), or using authenticator applications.
- **Machine learning.** Analyze user behavior to identify patterns indicative of fraudulent activity, such as rapid completion of signup forms, sequential username creation, and use of privacy tools like VPNs."
- **Device intelligence.** Use device and browser fingerprinting to identify when someone is using a single device to open multiple accounts. Some device intelligence platforms can also provide signals that indicate when fraudsters are using bots or emulator farms to automate sign-ups.

These strategies apply across all types of new account fraud. Behavioral analysis and device intelligence carry the advantage of happening in the background, not adding more friction to the process of opening a new account for legitimate users.

## Promo & bonus abuse

What is promo or bonus abuse? It's when fraudsters sign up for new accounts to repeatedly claim promotions, welcome credits, or referral bonuses meant to be offered only once. The business loses not only money but also accurate data about how well their marketing campaigns are working to attract new customers. It's also the most common form of digital fraud that online retailers and gambling companies face.

Promo and bonus abuse can be as simple as a single customer creating new email addresses to open several additional accounts, or a sophisticated, large-scale operation.

For example, in 2023, a UK man was convicted of fraud for opening more than 1,000 new player accounts on Bet365 as part of a matched betting scheme that netted over $300,000. The con involved signing up for new accounts to claim the gambling company's offer to match a first bet up to a certain amount. The player placed equal and opposite bets so he didn't lose his own money, and then he kept the matched amount that was part of the sign-up.

## Refund abuse

In the retail world, serial returners can repeatedly open new accounts to hide patterns of refund abuse. This type includes both customers who abuse generous policies by frequently using and returning legitimate merchandise (known as wardrobing) and those who commit refund fraud through false chargebacks or by returning stolen merchandise. Retailers including ASOS, Zara, and Wayfair have recently implemented policies to charge customers identified as repeat returners a fee for returned items to discourage the practice. Other companies seek to ban repeat offenders outright, although this can be tricky without the means to identify when multiple accounts belong to the same customer.

### How to fix refund & promo abuse

Retailers have to walk a delicate line. In a survey of 600 e-commerce companies by returns management platform Loop Systems, more than half of the respondents said their top challenge in curbing refund abuse and fraud is preserving a good customer experience for legitimate buyers. Online gambling companies similarly face heavy competitive pressure to continue offering bonuses and incentives to keep players coming to their sites.

As with multi-accounting, preventing and stopping promo and refund abuse requires solutions that don't penalize good customers. Anomaly detection and behavioral analysis programs can help spot risky transactions, and device and browser fingerprinting can help detect when one or more suspicious accounts are tied to a single device. Once you've anonymously identified devices associated with bad behavior, you can block or restrict them, getting ahead of fraudsters who simply try opening a new account if the previous one is restricted or blocked.

These strategies apply across all types of new account fraud. Behavioral analysis and device intelligence carry the advantage of happening in the background, not adding more friction to the process of opening a new account for legitimate users.

## Automated bot sign-ups

To create fake new accounts at scale, fraudsters typically deploy bots to automate the process. Sophisticated bots can quickly open large numbers of accounts that the fraudster controls to conduct many attacks quickly to maximize damage. Bots can carry out the types of fraud mentioned previously, as well as many other kinds of bad behavior:

- **Review fraud.** Bots open new accounts and use them to post fake reviews for products or services with the goal of convincing legitimate customers to make a purchase. They also might leave negative reviews for a competitor.
- **Spam messaging.** Bot accounts on social media sites can spread spam through private messages and as comments on posts.
- **Creating fake followers.** Almost half of social media influencers have paid to add bot accounts to boost follower numbers and earn more brand sponsorships.
- **SMS pumping fraud.** Fraudsters use bots to generate high volumes of account sign-ups that trigger one-time passwords (OTP) sent via SMS to premium numbers that are part of a particular mobile network. These numbers garner excessive SMS charges, paid for by the business sending the OTPs, and the fraudster that controls these numbers splits the proceeds with the network
- **Misinformation.** Bad actors open fake social media accounts in bulk to push disinformation and conspiracy theories.
- **Poker botting.** Players can pay for access to sophisticated online poker-playing bots that help them win more than they would otherwise.

According to a 2025 report from security provider Thales, bots now account for just over half of all Internet traffic. Bad bots alone account for just over a third of web traffic, and the problem is likely to grow worse as generative AI tools make it easier for less sophisticated fraudsters.

Social media platform Reddit recently announced additional measures to stem the tide of bot sign-ups on the site. The announcement follows the revelation that a group of Swiss university researchers secretly used AI agents with different personas to see how effective the bots were at changing unwitting human users' minds. "To keep Reddit human and to meet evolving regulatory requirements, we are going to need a little more information," said Reddit CEO Steve Huffman when explaining the new measures, which will involve third-party verification services but preserve anonymity. "Specifically, we will need to know whether you are a human, and in some locations, if you are an adult."

## How to detect bots

Fraudsters are constantly evolving new ways for bots to evade detection, but a combination of these bot detection techniques can help spot them:

- **IP blocklists.** Good bot detection solutions offer regularly updated databases of known bot IPs, data center ranges, and malicious proxies you can use to block traffic from those sources.
- **Machine learning.** Train models on large datasets of known human and bot interactions to spot patterns. These discovered patterns can then help identify bot behaviors in real time.
- **Behavioral analysis.** Analyze behavior on individual pages, such as mouse movements, scrolling cadences, and time spent on each page, to look for evidence of non-human behavior.
- **Honeypots.** Trap bots with hidden fields on form submissions that are not visible to human users browsing in a graphical interface but are visible to bots. The field is left blank if a human fills out the form, but bots fill out the field when they scan the site's HTML code. This action flags their submissions for blocking.
- **Device intelligence.** A comprehensive device intelligence platform analyzes hundreds of browser and device characteristics, which can help flag suspicious activity and devices that could indicate bots impersonating genuine users.

Putting together a multi-layered bot detection strategy is crucial, given that bots can carry out all the kinds of new account fraud discussed here. Detecting them is the first step in preventing them from accessing your site to begin with, and can help stop many fraud attacks before they start. It's likewise helpful for making sure banned users can't come back.

**30%**

of all internet traffic
is made up of **bad bots.**

## Ban evasion

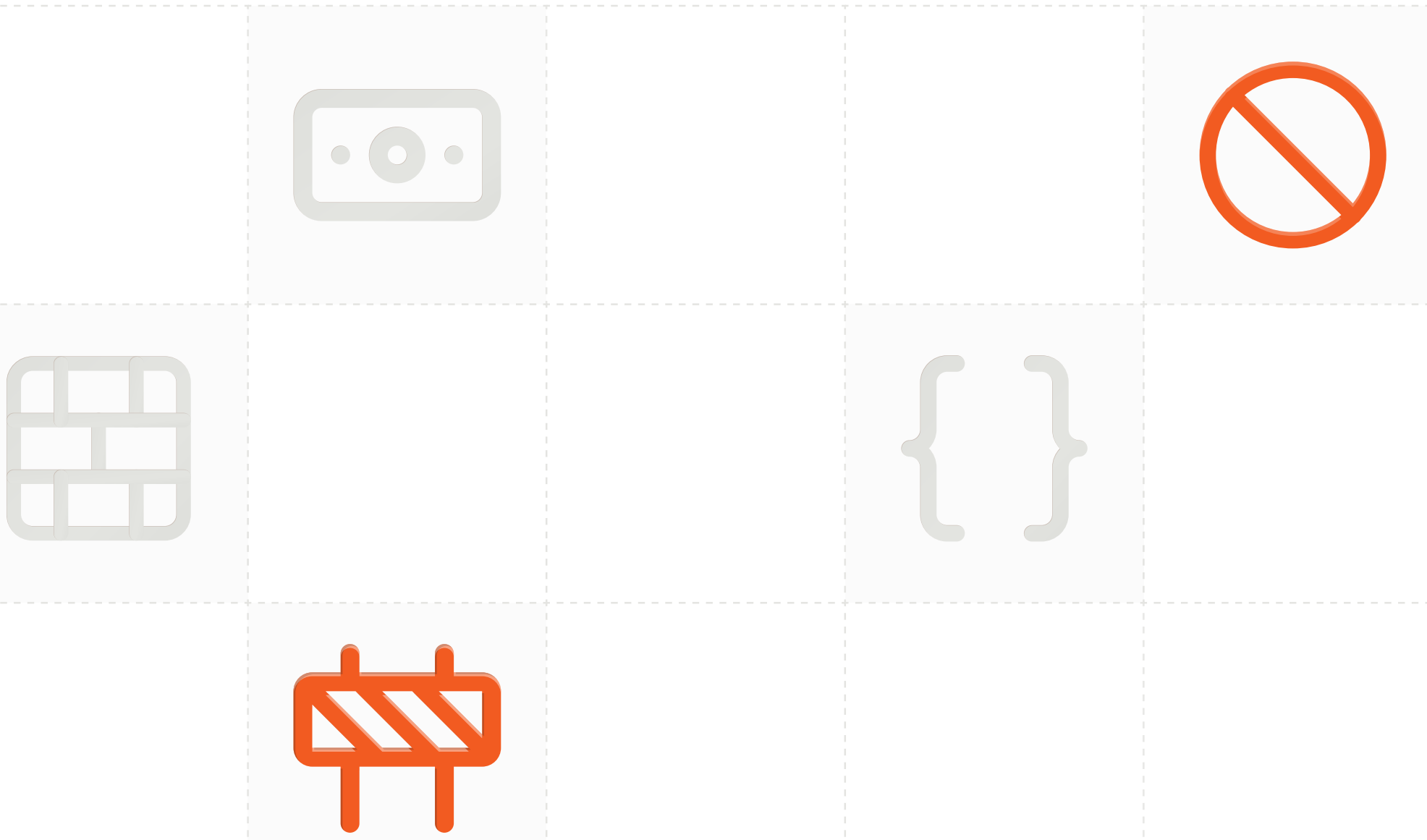
On top of the previously discussed aspects of new account fraud, there is also the problem of preventing scammers and trolls from turning around and opening more accounts after they are caught and blocked.

Stopping ban evaders is particularly important for sites where users interact with each other, such as social media or dating sites. Bad actors who use their accounts to harass others, send out spam, falsely influence discussions, or run social engineering scams are usually persistent and will simply sign up for new accounts if you don't have a way to prevent those users from perpetrating further harm.

On Tinder, Bumble, and Hinge, scammers use AI image generation tools to create photos for fake dating profiles, which they use to dupe hopeful potential romantic partners into investing in phony cryptocurrency schemes, for example. Over time, unchecked fake accounts damage the trust users have in the platform and may cause legal headaches for the site as well.

### How to detect ban evaders

Detecting repeat offenders often requires a mix of approaches, similar to bot detection. Sites can use cookies, IP addresses, and browser and device fingerprinting to spot devices that continue opening accounts after a ban. As with other types of new account fraud, using a mix of approaches is always helpful. However, most of these techniques have advantages and drawbacks in terms of how well they work and their effect on legitimate customers. The next section looks at how they compare.



## Which tools are best at preventing new account fraud?

There are two common problems with many of the tools used to prevent new account fraud: fraudsters and bots can circumvent them fairly easily, or they add considerable friction for legitimate customers. Some examples include:

- **MFA.** While sign-ups that require additional email, SMS, or biometric verification steps are very successful at making it harder for bots to open new accounts, especially at scale, MFA adds significant frustration for good users that may cause them to give up on creating an account.
- **Cookies.** While browser cookies help identify returning fraudsters when they open new accounts, cookies are easily erased or blocked.
- **CAPTCHA.** Once a standard tool for millions of websites, researchers have shown that bots can now reliably bypass all types of them 100% of the time. They also add considerable annoyance for regular users who are tired of clicking squares with bicycles in them.
- **IP address blocking.** If a returning visitor shows up with an IP address already flagged for suspicious behavior, you can automatically restrict access. However, fraudsters can easily change IP addresses with VPNs, and there's a risk of false positives.

In contrast, machine learning anomaly detection programs and device intelligence can operate in the background and are harder to get around. Device intelligence relies on browser and device signals that don't change frequently, so you can trace multiple fake accounts to the single device that opened them all. When you know which devices are behind bad behavior, it's easier to block fraudsters and bots from visiting your site in the first place.

KEY TAKEAWAYS

## Fingerprint's industry-leading device ID accuracy

At Fingerprint, our focus is on providing you with the highest-accuracy device identification. We identified more than four billion unique devices in 2024, and we use more than a hundred signals for industry-leading accuracy rates. We assign each device or browser that visits your site a unique Visitor ID that can remain stable for months or even years. It persists even when users visit using incognito mode, clear cookies, or use a VPN.

Our Bot Detection Smart Signal detected over 416 million bad bots in 2024. It works by collecting large amounts of browser data that bots leak to reliably distinguish genuine users from headless browsers and automation tools. The signal result indicates whether the visitor is a good bot (like a search or AI crawler), a bad bot (potential fraudster), or not a bot (human). Companies can use this data to quickly take appropriate action, such as blocking a visitor's IP, withholding content, or asking for human verification.

To learn more about Fingerprint, visit our product demo playground or get in contact with us today.

**About Fingerprint**

Fingerprint, the world's most accurate device intelligence platform, enables companies to prevent fraud and improve user experiences. Fingerprint processes 100+ signals from the browser, device, and network to generate a stable and persistent unique visitor identifier that can be used to understand visitor behavior. Fingerprint is ISO 27001 certified, and SOC 2 Type II, GDPR, and CCPA compliant. Fingerprint is trusted by over 6,000 companies worldwide, including 16% of the top 500 websites, to help catch sophisticated fraudsters and personalize experiences for trusted users.