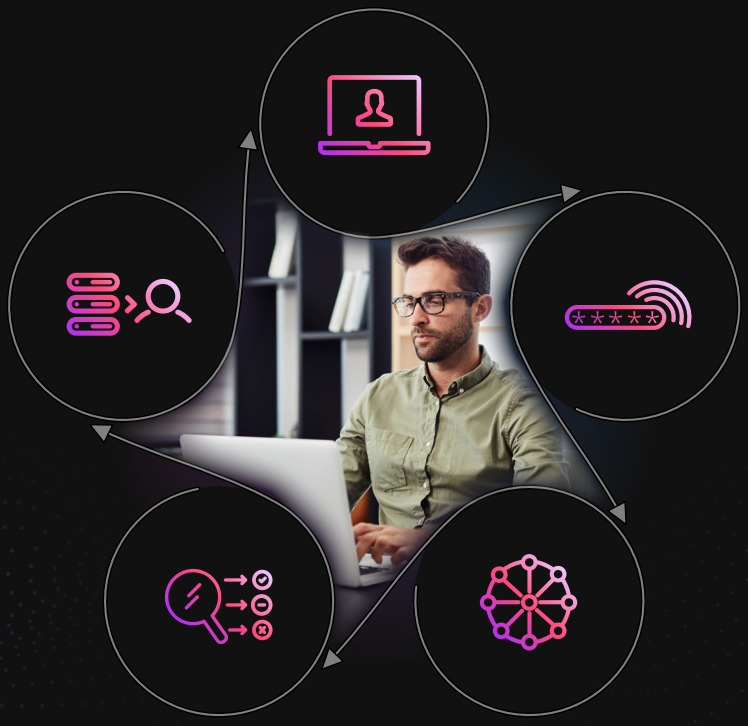
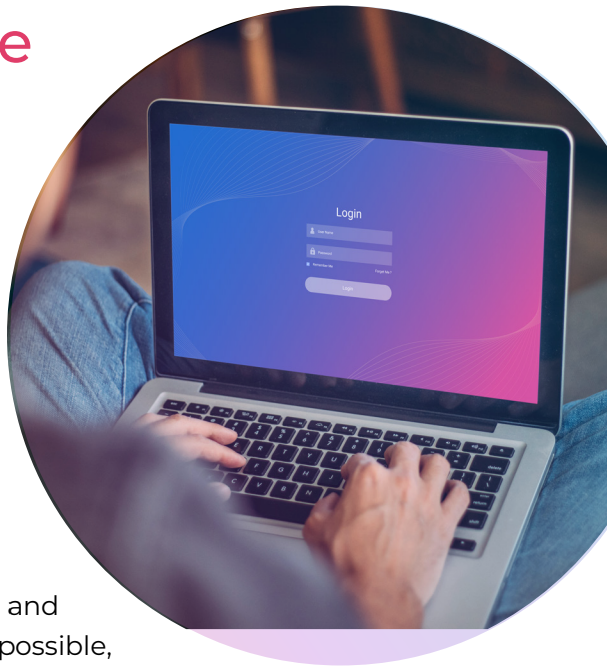
eBook

Stopping fake users at the door



TeleSign

Fake users are much more than a mere annoyance.



These bad actors commit costly fraud with constantly evolving tactics, sometimes even before they enter your ecosystem. When they invade your platform, they can quickly damage marketplaces and brands and cause legitimate customers to flee.

Today, most ecosystems are littered with fake accounts set up to steal confidential information, post fake product reviews, spam legitimate customers, along with other problematic actions that detract from the value of your products and services. As digital marketplaces grow and companies strive to onboard as many new customers as possible, fake account registration is an ever-increasing, expensive nuisance to the integrity of your network, marketplace, and platform. Even powerful brands are not immune; in fact, they are often the most prominent targets. In Q4 of 2021 alone, Facebook removed 1.3 billion fake accounts.

Creating havoc across industries

Many people think of fake users as disgruntled individuals who make their way onto a platform to create general mischief, such as bad-mouthing a product without the fear of reprisal or impersonating another user to damage their reputation. However, fake accounts are often created using highly sophisticated techniques by determined and skilled fraudsters.

New account registration fraud is growing rapidly, as bad actors discover and refine their tactics. Tens of thousands of fake accounts are created each month across industries, from banking and ecommerce sites to gaming and social media platforms. Bad actors use fraud tactics to create fake accounts and receive lucrative payoffs.

Though fake users are most active and visible on ecommerce sites, they target industries and platforms across the digital landscape using a variety of tactics.

Posting fake product reviews

In the world of e-commerce, fake reviews are commonplace. Companies pay fraudsters to push up a product or damage a competitor on a marketplace with this tactic. Doing so undermines the site's integrity while degrading customer confidence in the brand.

Spamming and phishing

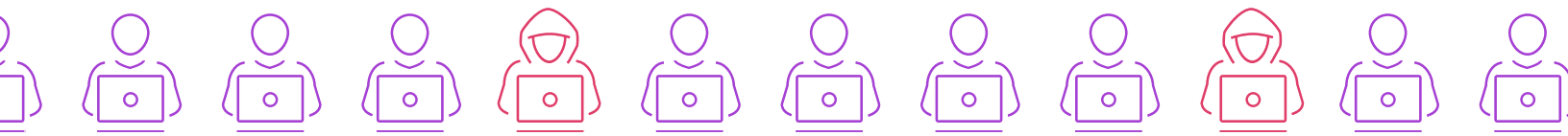
With spam and phishing attempts, fraudsters use fake accounts to sell their products or steal confidential information. Primarily impacting ecommerce and media platforms, up to 50% of new accounts on these platforms are created solely to send spam and phishing messages.

Abusing promotions

Sign-up promos can be lucrative for fraudsters, as they use fake accounts to collect on promotions repeatedly. Even if the loss is small, it can increase when other bad actors replicate the fraud tactic. In fact - one fraudster recently took Uber for a ride for $50,000 via promo abuse. Bad actors are increasingly using advanced phishing/vishing techniques and low-cost bots to automate the process, making it easier for them to create fake accounts and conduct their fraud schemes.

Selling accounts

In the gaming industry, fraudsters have created a black market for banned users or fraudsters looking to buy new accounts. This type of fraud is lucrative and difficult to defend against, as new users who appear to be legitimate can buy accounts that they then sell to bad actors.



Defrauding legitimate customers

Fake users also create accounts solely to defraud legitimate customers on the platform. Though it can happen anywhere, crypto platforms are the most common target for this type of fraud due to the difficulty tracking the transactions and the potentially lucrative payoffs.

Conducting International Revenue Share Fraud (IRSF)

With IRSF, the bad actors may not even want to enter the platform. As most web apps and websites are now communication-enabled, they send out SMS messages and voice calls as part of their onboarding workflow or other business processes. Fraudsters collect thousands of phone numbers to register with these websites, either through the onboarding process when they receive a six-digit pin through the 2FA process or via marketing messages. They then drive SMS messages and phone traffic to their own numbers and share the resulting revenue with shady phone carriers. Essentially, this intricate tactic uses the onboarding process to perpetrate revenue-skimming, often for hundreds of thousands of dollars.

Stopping fake users before they start

To successfully limit fake users and the damage they create, you need to stop fraud at the source: Onboarding. Unless bad actors are discovered during onboarding, it is difficult and costly to stop them once they enter your platform and set up shop. Left unchecked, your ecosystem could soon be full of fake accounts.

Using historical data provided in the 2FA process combined with other fraud detection solutions allows businesses to identify fake users. Most users are legitimate, so you want to limit aggressive onboarding protections that add too much friction across the board – saving those hurdles for high-risk new users. If you are too heavy-handed, it could cost your business far more than fraud when good customers leave.

Risk scoring to build trust

Onboarding is tricky. You want to provide a frictionless, easy experience for good customers while stopping fake users before they cause damage. The best defense against fake users is catching them before they create havoc: This starts with onboarding. Onboarding should begin with a risk score. Safe, low-risk customers should have an easy, streamlined onboarding process. Higher risk or high-risk users require more verification or should be blocked altogether. As a bonus to this approach, as you put additional verification tools in place as part of a layered fraud-prevention process, fraudsters will notice and look elsewhere for easier targets.

With the near-ubiquitous use of 2FA as a foundational component of a layered security stack, most major brands are using the provided phone numbers to build intelligence-based fraud risk scores. Risk scoring and digital identity simultaneously look at thousands of factors to help companies understand if the device, location, behavior, and thousands of other signals match the user attempting to create an account.

By using risk scoring — a nearly instantaneous, invisible verification method— companies can strike the right balance between security and customer experience as they work to limit fake accounts.

TeleSign solutions

TeleSign Score is a risk assessment solution that uses machine learning to analyze phone number data and deliver a reputation score. Score assesses the riskiness of users through phone number intelligence and recommends whether to “allow”, “flag”, or “block” them based on their risk score. When Score recommends allowing an interaction, the optional next step is to send a one-time passcode that the user then provides to verify their identity or transactional activity. When Score recommends flagging an interaction, the optional next step is to manually review the registration or transaction.

TeleSign reviews thousands of data points associated with a phone number to deliver a risk score. What types of data points would negatively impact a user’s score? Things like a VoIP phone number, a burner phone, or a phone number that has recently changed devices (SIM Swap) can each raise a flag and increase the risk score. Score helps you answer critical security and business questions, such as:

- Is this a fraudulent user trying to sign up?
- Is this promo code being abused?
- Is this an international revenue share fraud attack?

This process works seamlessly when businesses trust TeleSign to deliver risk scoring, verification, and authentication as a complete solution. Score is natively integrated into TeleSign’s Verification API and requires minimal developer resources to get started.

Onboarding is an opportunity to establish a trusted relationship with real customers and keep fake users out. Onboarding can be the beginning of an ongoing bond, one that enables customers on your platform to safely sign on and conduct business free of fear and knowing their identity and transactions will not be compromised.

Ready to deliver a trusted experience?

Get started