WHITE PAPER SPONSORED CONTENT

telesign

A best practices approach to customer onboarding

Reduce friction and stop fraud

Organizations that adopt the right strategic and technology framework while onboarding improve customer experience while thwarting fake accounts and fraud.

Never before have companies had the ability to reach so far and wide to gain new customers. Thanks to the internet, a business' footprint knows no limits. Today, there are unprecedented opportunities to attract customers and boost revenues. Yet, onboarding customers is tricky and challenging. It's critical to balance ease of use with strong security. If it's too difficult to create an account, customers will flock elsewhere. On the other hand, a lack of security may spawn fake accounts, fraud, and other problems. These issues can lead to a lack of confidence among customers and, in turn, diminished revenues.

Consequently, streamlining processes while keeping fake users out is imperative. Asorganizations grow—including across borders and around the world—it's also crucial that their strategic framework and technology scale adequately. To create a scalable, frictionless onboarding experience, organizations should concentrate on identifying users, analyzing risk, and authenticating effectively.

A best practices approach to customer onboarding: reduce friction and stop fraud

Avoiding an identity crisis

When a new customer interacts with a business online, it sets the tone for how they view the company. For better or worse, the sign-up and account creation processes must be simple, straightforward, and painless.

If a person encounters too many obstacles—such as multiple verification requests, challenging captchas, or countless user inputs—there's a good chance they will give up and go elsewhere. In fact, it's estimated that up to 20% of sign-ups are abandoned. At the same time, making things too easy creates an entirely different set of problems. In 2020, 39 million consumers lost $43 billion to identity fraud. Even worse, new account fraud increased by 70% during 2021.

In addition, financial institutions, e-commerce companies, social media companies, and more find themselves coping with the cost and hassle of fake accounts. These fraudulent accounts are used for identity theft, fake product reviews, platform spam, promotion code abuse, and phishing attacks, as well as to gain access to other systems for potential ransomware attacks.

The bottom line: Strong security and anti-fraud detection are paramount in today's digital landscape. Although they're the foundation for trust and confidence, most businesses lack the right strategic framework and technology to address these issues on their own. They, therefore, fail to achieve the delicate balance between usability and protection. In the end, this leads to massive headaches—and real-world costs—for both the company and potential customers.

By the numbers

In 2021, fraudulent accounts increased by

70%

Fraud resulting from accounts that were less than a day old:

48%

Synthetic identity fraud losses grew to

US $20B

Internet traffic attributed to bots with malicious content:

25%

Consumers frustrated by long and complicated sign-up processes:

49%

Adults who expect to spend less than 5 minutes completing a new account sign-up:

59%

Potential customers who abandon shopping carts or registration pages when they encounter a complex sign-up process:

83%

A question of balance: Usability and strong security can coexist

A fundamental problem during onboarding is that adequate verification often doesn't exist when a person signs up for an account. In some cases, there is no verification process in place. This means that bad actors can easily create fake accounts at scale, including the use of other people's email addresses and credentials.

Yet, even when the best verification practices and solutions are deployed, gaps and loopholes still exist. For example:

- Fraudsters purchase fake emails, VoIP numbers, and SIM cards in bulk.
- Bots and scripts can generate millions of user accounts in seconds, increasing the risks of data breaches through synthetic identity fraud.
- Newer biometric strategies are not foolproof. Significant differences exist in IT infrastructures, global bandwidth capacities, and the sophistication levels of bad actors.

All of this creates windows of opportunity for thieves and fraudsters. Remarkably, 48% of all fraud occurs from accounts that are less than a day old, according to the "Safe, Secure & Simple Onboarding" report by TeleSign. By the time an organization recognizes that an account is not authentic, fraud and theft have already occurred.

The answer? Businesses require always-on, layered fraud prevention solutions. By classifying digital identity signals during onboarding, a business can challenge risky users while delivering a quick and easy onboarding experience to legitimate users. It's a win for everyone, stopping fraud before it starts.

This process achieves protection by using:

Dynamic risk scoring

Assess the risk of every new user to prevent new account fraud, platform spam, and promotional abuse. By assigning a risk score, an enterprise can detect risk, block fraud, keep fraudulent users off their platform, and make dynamic, risk-based decisions in milliseconds using tailored scoring methods. This risk assessment score can recommend the appropriate action, including allowing or blocking a user sign-up. Best-in-class solutions integrate with existing security frameworks.

Phone number intelligence

Curtail the creation of fake accounts with intelligence about the user integrated seamlessly into your verification workflows. Detect suspect devices like VoIP numbers and SIM farms to ensure that only legitimate users complete the onboarding workflow. Using phone number and subscriber attributes, organizations can monitor traffic for suspicious patterns and then compare a new account request with a global telecom fraud database.

Identity verification

Validate a user's identity without adding friction to the sign-up process. By simply collecting a phone number at sign-up, an organization can validate a person's identity using more than 5,000 machine learning and identity insights. This approach thwarts unauthorized account creation and protects users with one-time passcodes and multifactor authentication (MFA). It can block multi-account creation by verifying the device and the user.

When organizations use these controls, they can build a business framework that supports trust and confidence, benefitting both consumers and the business. Because this digital identity verification framework operates in real-time, it's possible to authenticate identities, evaluate risks, and validate accounts globally at the speed of digital business. Organizations are equipped to make fast and smart decisions intuitively.

A best practice verification model takes shape

When organizations adopt a more advanced approach to digital verification—through a solution like TeleSign—several important benefits accrue:

- They block fake users at the source through MFA, digital identity verification, and dynamic-based risk assessments.
- Social media, gaming, retail, food, travel, and other sites can block fake reviewers that harm the business's or platform's reputation. It's also possible to block bots and other accounts that spread false news and generate other problems.
- It's possible to scale digital identity protection globally. As a business expands to other countries, this eliminates some risks. With TeleSign, for example, it's possible to securely onboard and verify customers in more than 200 countries and 90 languages globally.
- Organizations avoid sign-up friction and abandonments that result from overly aggressive vetting. This framework builds trust and affinity with new customers from the start.
- Within this trust-first framework, customers encounter a safe, seamless experience from day one. Meanwhile, the business reduces risk of fraud.

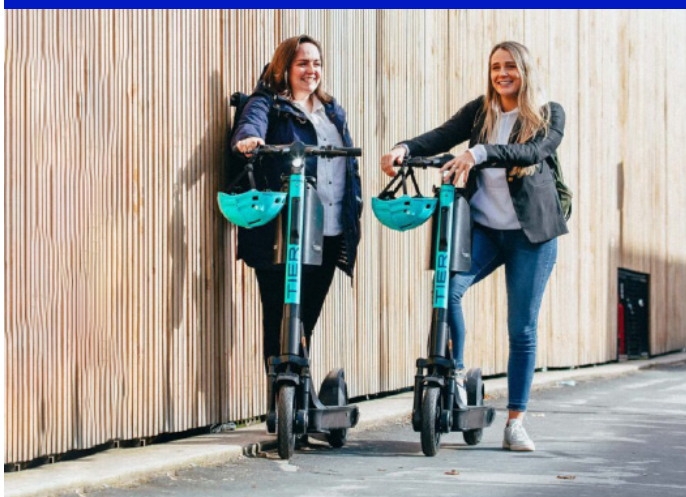
CUSTOMER SUCCESS:

TIER dials into gains using advanced verification

Churn can wreak havoc on a company's ability to earn a profit. When TIER, a Berlin-based micromobility provider, started to expand its rental scooters into additional countries and grow its user base, secure account creation was paramount.

TIER turned to TeleSign to develop a secure onboarding process. Today, with effective account verification and risk scoring in place, the company instantly flags suspicious accounts for manual review.

After putting the solution in place, TIER began blocking hundreds of fraudulent transactions per day. This has led to reduced credit card fraud and lower security costs. Equally important: Rather than constantly reacting to problems, staff devotes time and resources to strategic tasks that help the company innovate further.



- FinTech and financial services companies can crack down on synthetic identity fraud, which is a tactic that fraudsters use to apply for credit cards and loans with a mix of real and fabricated information.
- By harnessing billions of global identity signals—online, mobile, behavioral, geo, and more an organization can use a sophisticated risk-scoring model to embed trust into onboarding and throughout the customer journey.
- It isn't necessary to rethink or rebuild security infrastructure or data. That's because the verification data, typically collected during sign-ups, already exists within a business. If this isn't the case, the business can pull the required data from existing systems and databases, such as a mobile phone provider. A solution like TeleSign connects all the dots quickly and seamlessly.
- Telesign technology handles this task across a wide range of industries, including e-commerce, financial services, media and entertainment, and on-demand services such as ride sharing and food delivery. The solution can be tailored to fit virtually any business model and any industry.

Identity verification is a winning approach

As organizations wade deeper into digital business and online interactions become commonplace, strong customer verification isn't just desirable; it's mission critical.

With the right technology framework in place, it's possible to deliver a smooth signup experience while protecting the enterprise.

But the benefits don't stop there. Organizations can lower customer acquisition costs and ensure that conversion rates are legitimate.

Today, strong digital identity verification is at the center of business. It scores big wins for both businesses and their customers.

For more information

Balance user friction and fraud with mission-critical identity verification.

Visit **telesign.com** for more information.

telesign