WHITE PAPER SPONSORED CONTENT

telesign

A best practices approach to digital onboarding for financial services

# Reduce customer friction and stop costly fraud

**Financial institutions that adopt the right strategic and technological frameworks for onboarding improve customer experience while thwarting fake accounts and fraud.**

Never before have banks had the ability to reach so far and wide to gain new customers. Thanks to the internet and mobile apps, a company's footprint knows few limits. Customers can find you online or in an app store and sign up for your financial services from almost anywhere in the world.

Onboarding is a crucial step in the conversion process. It's critical to balance ease of use for your customers alongside strong security protocols to meet regulatory requirements. If it's too difficult to create an account, customers will go elsewhere, but a lack of security may spawn fake accounts, fraud, and other problems for your business. These issues can lead to a lack of confidence among customers and, in turn, diminished revenues.

Streamlining sign-up processes for customers while keeping fake users out is imperative. As digitization continues to change the way banks and fintech providers do business—including across borders and around the world—it's crucial that security frameworks and technologies meet the demands of a complex digital world. To create a secure, frictionless onboarding experience, organizations should concentrate on identifying and authenticating users and analyzing risk quickly and effectively.

# Best practices for approaching banking and Fintech customer onboarding: maintain security and ease-of-use

## 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. It's estimated that up to 20% of sign-ups are abandoned.

At the same time, making things too easy for new users creates an entirely different set of problems, particularly for financial institutions who are legally required to comply with Know Your Customer (KYC) standards.

For financial institutions, the cost and hassle of fake accounts can be considerable. Fraudulent activity is on the rise across web and mobile applications, leaving consumer accounts vulnerable to takeover and resulting in financial and reputational losses for companies.

The bottom line: Strong security and anti-fraud detection are essential for modern banking institutions to maintain compliance and protect customers.  Although digital security is the foundation of consumer trust, many businesses lack the right strategic frameworks and technologies to address fraud protection on their own, which means they may 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

**70%**

increase in fraudulent accounts in 2021[1]

**48%**

of fraud comes from accounts that are less than a day old[2]

**US $20B**

of losses from synthetic identity fraud[3]

**25%**

of internet traffic attributed to bots with malicious content[4]

**49%**

of consumers are frustrated by long and complicated onboarding[5]

**59%**

of adults expect to spend less than 5 minutes completing a new account sign-up[6]

**83%**

of potential customers abandon registration when they encounter complex sign-up processes[7]

1. https://www.ftc.gov/news-events/news/press-releases/2022/02/new-data-shows-ftc-received-28-million-fraud-reports-consumers-2021-0
2. https://fintechmagazine.com/sustainability/addressing-problem-new-account-fraud
3. https://bankingjournal.aba.com/2021/10/report-synthetic-identity-fraud-results-in-20-billion-in-losses-in-2020/
4. https://www.cpomagazine.com/cyber-security/bad-bot-traffic-report-almost-half-of-all-2021-internet-traffic-was-not-human/
5. https://auth0.com/blog/what-your-customers-really-want-from-your-login-box/
6. https://www.prnewswire.com/news-releases/ibm-survey-pandemic-induced-digital-reliance-creates-lingering-security-side-effects-301312086.html
7. https://auth0.com/blog/debunking-common-misconceptions-about-passwordless-authentication/

## Finding balance: Usability and strong security can coexist

A fundamental challenge during onboarding is verifying customer identity quickly and efficiently without prolonging the onboarding experience.

---

## Implementing best practices for customer verification is necessary to maintain compliance and avoid security gaps and loopholes that can impact your company's revenue and reputation. 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 these gaps create 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.

## The best practices for financial digital onboarding:

### Dynamic risk scoring

Assess the risk of every new user to prevent new account fraud, which can minimize KYC program costs. 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 verification workflows. Detect suspect devices like VoIP numbers and SIM farms to ensure that only legitimate users complete the onboarding workflow. Using phone numbers 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 collecting a phone number at sign-up, an organization can validate a customer'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, benefiting 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.
- Digital identity protection operates at a global scale. 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.
- Crack down on synthetic identity fraud so fraudsters can't apply for credit cards and loans with a mix of real and fabricated information.

**CUSTOMER SUCCESS:**

### Affirm seamlessly evaluates financial risk and digital identity

Consumer identity verification has become more complicated with the rise of eCommerce. Affirm, a modern banking solution, provides customers with an alternative to traditional credit cards so they can buy now and pay over time.

With the speed of eCommerce purchases, Affirm needed a solution to build a complete digital risk assessment in seconds.

Affirm partnered with Telesign to add programmable communications and digital identity solutions to their tech stack. After putting the solution in place, Affirm has been able to enhance the risk assessments given to providers, leading to higher sales conversions. And as an added bonus, Affirm has been able to automate payment reminders with Telesign's communications capabilities.

- 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.

## 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 banking. 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