eBook

Building Trust at Every Stage of the Customer Journey

TeleSign

Trust can make or break your business.

Trust is so crucial that 85% of customers report that they would avoid using a brand if they lost confidence in it. While data breaches impact consumer trust, account takeovers (ATO) and financial fraud demonstrate that losing trust in a brand can come anywhere along the customer journey. For instance, the same study found that 43% of customers would lose trust in a brand over fake reviews on their platform. Another study found that 28% of customers would stop using a site or service if they experienced an ATO. Conversely, when consumers trust your brand, they are 7x more likely more to buy from you.

Lost trust in a brand is hard to recover. Rebuilding trust can take years and cost hundreds of thousands – if not millions – of dollars to mitigate the influence of fraud associated with your brand. The economic impact of lost customers and purchases can linger even longer. Protecting customer experiences from fraud is imperative to protect your growing enterprise.

Fraud is a broad category but is almost always some form of deception aimed at the fraudster's monetary or personal gain. Fraud is constantly changing, always adapting, and always a threat. It happens at any – and every – point across the customer journey. Protecting your brand, your customers, and your platform from fraud requires diligence and an always-on mentality. With more than 7 billion users online today, the stakes have never been higher.

Defending against fraud and building trust with your customers starts from your very first interaction or account creation – and never ends. In this eBook, we discuss some key points, attacks, and fraud methods to help you identify ways to secure your online customer experience and customer trust from your first interactions to your continued communications.

Building and maintaining trust is hard, but there are steps you can consider to make it easier.

Onboarding new customers

Trust begins at the first step in the customer journey.

Humans are wired to build trust. In face-to-face interactions, we develop trust through verbal, non-verbal, and contextual signals. Building rapport also builds trust: frequent positive or neutral engagements help others trust that you are not harmful. However, in the online world, you cannot see, talk to, or directly interact with a customer as you do in the physical world. The anonymity of the internet brings privacy to users but leaves a giant identity and behavioral void.

Understanding the risk of the person registering for your service with some certainty is critical to protecting your business. You could ask for photos of physical identity documents and a live picture of their face to ensure they match. You could even add a fingerprint and a physically mailed pin to their address on their ID as an added layer of verification. However, except for extremely high-value transactions, no reasonable person will take such onerous actions to identify themselves to you. In fact – they may prefer to remain quasi-anonymous on your platform.

So how do you strike a balance of protecting your platform and user base from fake accounts or identity fraud without sacrificing conversion and growth?

The value of verification

The verification process can be challenging for a business, given the high stakes involved and the balancing act between security and convenience. It is also an opportunity to develop long-term, brand-loyal customers and move ahead of the competition. Onboarding and fraud prevention can now be viewed as a selling point, an initial touchpoint that sets the tone for the overall experience. As in the physical world, identity verification is a requirement to protect customers and businesses from bad actors; in the digital world, it boosts efficiency and lowers costs by increasing the speed of the process and mitigating human error.

There are many ways to verify digital identity; some are as old as the internet (and still in use), and some incorporate the latest in human psychology and biology.

Knowledge-based identifiers

Knowledge-based questions and user information stored in a database offer increased security and are a common practice in the digital world. The process links users to the information they know or other information held by the enterprise network. Often these take the form of standardized questions, such as “What is the name of the street of your childhood home?” with the user providing an answer. The user might also be challenged to answer these questions when changes are made or when new devices or browsers are detected. While these challenges give some cursory security, many of these answers are available on the dark web from previous breaches, part of the public domain, or disclosed by the user on social networks or other online sources – making this one of the easiest challenges to overcome for bad actors.

Multifactor authentication

Two-or-more-factor authentication is a necessary building block for overall fraud prevention and is quickly becoming a user expectation. Most internet users have two or more primary email addresses and signing up for new addresses takes mere minutes. Phone numbers, however, are hard to fake. Most people only have one mobile number and obtaining additional numbers is costly and time-consuming. That natural time and cost barrier and 1:1 average ratio make phone numbers a great anchor for digital identity. Two-factor authentication can provide even greater protection when layered with mobile digital signatures, identity attribute brokerage, and additional digital identity solutions.

If two-factor authentication is good, it would seem that three-factor (or more) authentication is better, but this invariably leads to increased user friction. To find the right balance, many enterprises are moving to a combination of two or multifactor authentication (MFA) digital identity solutions, such as phone number reputation risk scoring. With this approach, businesses can set up alerts for suspicious behavior with minimal friction to users.

Biometric and behavioral

Biometric and behavioral methods are more commonplace today, especially in high-value transactions such as banking and mortgage mobile applications. Though fingerprint and facial recognition solutions add additional layers of protection by linking digital ID to the right person, bad actors continue to innovate and circumvent the system using both manual processes and the latest in artificial intelligence technologies.

Behavioral identification—such as analyzing the length of time between keystrokes or the speed of providing a digital signature—can be used to flag and alert companies to suspicious behavior. It also introduces the potential to falsely identify good customers using a new device or operating in a new environment.

You can implement one, several, or all current identity verification methods to meet your security and customer experience requirements. But a layered solution that alerts you to bad actors and suspicious behavior via risk scoring the identifiable information you collect is the most effective.

Maintaining account integrity

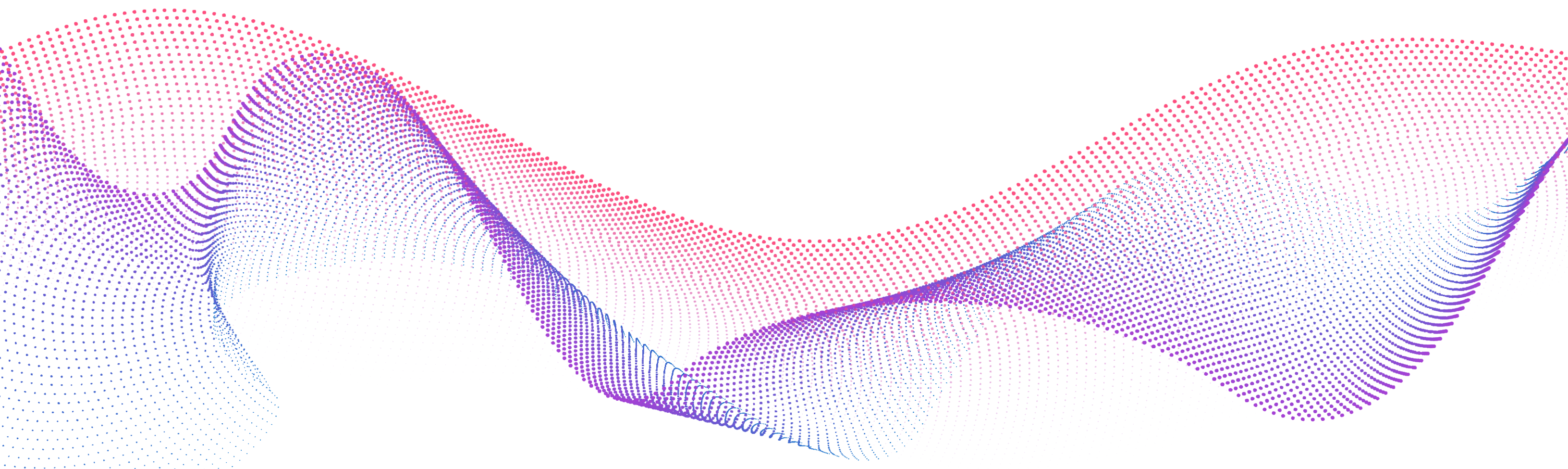
Verify identity; instill confidence.

After onboarding, your customers expect safety in your ecosystem each time they enter and on each transaction. Your customers have good reason to feel apprehensive when transacting online. 86% of people have been victims of credit card fraud, identity theft, or a data breach. Millions of usernames and passwords are breached every week: the largest data breach in history happened in 2021, with the leak of 8.4 billion passwords.

We are under constant attack online. Without effectively verifying and authenticating a user's identity, your customer's accounts are at risk, as is their trust in your organization.

Know the main types of account takeovers

Every time a customer logs in and accesses your platform, it is up to you to verify and authenticate that it is your customer and not an impersonator. If Jack Dorsey can get his Twitter account taken over, anyone can. But even with the strongest passwords, two-factor authentication, and never getting reeled in by a phisher – anyone can be a victim of a cyberattack.



Some fraud events are self-inflicted. Reusing passwords, for example, makes them susceptible to theft in breaches or social engineering schemes. Bad actors can then use a combination of psychological techniques (social engineering) to collect a user's login credentials or other identifying information to steal their identity or conduct a fraudulent transaction. However, with MFA you can mitigate this common user issue by forcing a new device or IP to authenticate with SMS or app-based one-time password (OTP).

Phishing attacks, a form of social engineering, have been around for as long as the internet, and they are still common today. In a phishing attack, bad actors send what appears to be a legitimate message to a user to steal their information or install malware or other malicious software on their computers—and the business ecosystem. When used with system weakness exploitation, social engineering remains an ongoing threat to you and your customers.

SIM swaps are low tech and high effort but offer high rewards to fraudsters. This social engineering attack often takes place after a phishing or password takeover. Fraudsters use the Personally Identifiable Information (PII) they procure in the phishing scheme and use it to convince the victim's mobile carrier to update the SIM card to a new device controlled by the fraudster. Once this occurs, a fraudster can intercept OTPs and gain control of the account recovery process to take complete control of the victim's high-value accounts. A SIM swap is one of the most effective—and damaging—types of fraud because it gives fraudsters control of a user's device, allowing them to circumvent two-factor authentication protocols.

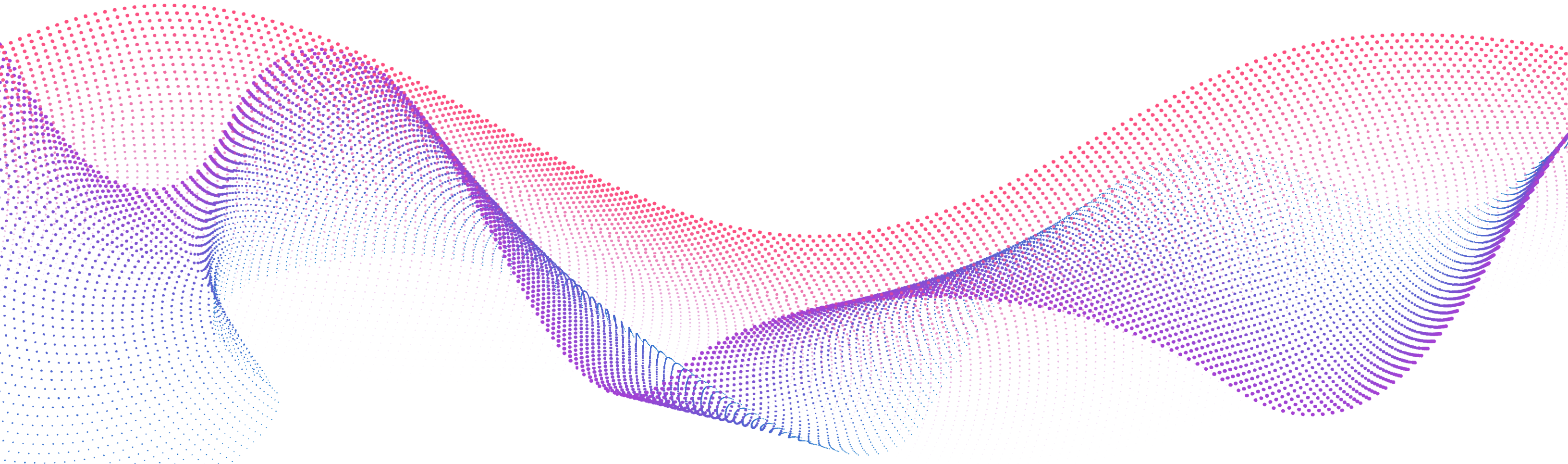
According to a 2020 Princeton University study, 80% of SIM swap attempts are successful, and they are on the rise. Since 2015, SIM swap fraud has increased 400%, and account takeovers have nearly doubled since 2017. The influx of SIM swap attacks is making mainstream headlines, like the cryptocurrency investor who lost $24 million or the eight fraudsters who stole $100M in cryptocurrency. As SIM swaps and similar techniques such as phone number porting and forwarding become more widely known and evolve, keeping your users and their accounts safe is critical.

Engaging customers to alert, support, and build trust.

Connect and communicate to guide your customers.

After authenticating a user’s identity, it is important to proactively communicate to your customers at key moments to verify their actions, notify and confirm changes that may impact them, and alert them to critical issues and suspicious behavior on their account or a system change. 82% of B2B buyers and 72% of B2C customers use multiple communication channels throughout their path to purchase. The availability of multichannel communication increases the bottom line. According to Forrester, when consumers can use their preferred communication channels, more than half are more likely to recommend, buy more, or make a first-time purchase.

Communication is critical to building trust with your customers. From alerts, reminders, and notifications to two-way voice platforms, you should connect and communicate at each touchpoint in your ecosystem via their preferred communication channel, whether it is SMS, MMS, RCS, WhatsApp, or Viber.



While communication between you and your customers is now often a user expectation and mutually beneficial, those communications should be private. You can leverage number masking (anonymous communication) to connect them with on-demand services employees--such as delivery drivers--while maintaining privacy on both ends.

As users become more concerned with what happens to their PII, it is essential to provide options to opt-out of sharing their information. And with the now ubiquitous use of ride-sharing services, dating apps, and peer-to-peer marketplaces, your customers are exposing more of their information. They want to feel confident that communicating with your business will not empower fraudsters to attack them.

From alerting your customers to potential fraud to announcing broader marketing campaigns and customer loyalty programs, your customers want to hear from you—and they want to talk to you.

+1 (510) 765-4321
Hi Jane! Welcome to LA. The front door code to Casa Azul is 4732. Enjoy your stay 😀

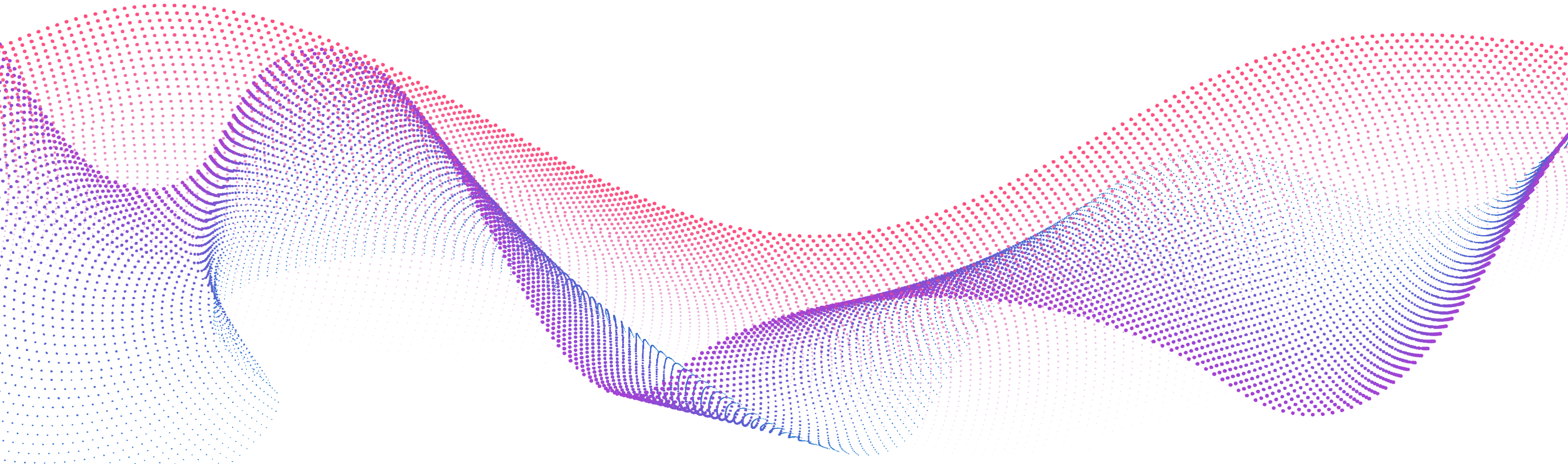
TeleSign helps you protect, defend, and connect with your customers on their journey

The common thread among fraud attempts is the mixture of technology and human error exploitation. Fraud prevention techniques, therefore, should be multilayered and dynamic.

While onboarding and customer login protection help prevent fraudsters from entering your ecosystem, it is equally essential to safeguard every transaction on your platform to protect your customers and your business from the fiscal and opportunity costs associated with fraud. It only takes one occurrence of fraud to destroy a customer’s trust in your business forever.

Verify identity

Digital identity solutions are crucial to protecting your customers at the transaction level and should be used together with multifactor possession, biometric, and knowledge-based verifications. Digital identity adds security without necessarily adding friction, as the check for reputation and risk can happen instantly and seamlessly before or while your MFA or biometric verification is happening.



While two-factor authentication remains a necessary, critical building block of fraud prevention, you should consider layering identity solutions into your fraud protection methods to protect against bad actors and keep your customers safe and coming back.

One additional layer of protection is to use mobile identity data gathered via two-factor authentication in combination with behavior patterns to verify the user behind the transaction quickly. Simply challenging suspicious scenarios with a one-time password and a dynamic risk assessment algorithm can help you block fraudulent transactions before they happen. You should also require additional verification for high-value transactions or anytime there is a change to the user's data, such as a new address or phone number.

At the same time, the customer experience cannot be overlooked. You should ensure that you fast-track your good customers while focusing on potential bad actors. To prevent customer fatigue while providing a trusted customer experience, you need a dynamic, risk-based assessment to detect fraudulent threats. Today, identity management requires linking online and real-world identities, tying together information such as physical address and date of birth with browser versions and cookies for effective risk scoring.

Monitoring these interactions can protect your platform in other ways. Most people associate transactions with money exchanging hands, but each time a review or rating is listed on an e-commerce platform, it can be considered a transaction as well. In the days when a negative review equates to lost revenue, selecting fraud prevention tools and holistic processes for identifying users and verifying transactions has never been more critical.

TeleSign enhances the customer journey through digital identity anchored in phone numbers and phone data. We enable scalable and secure onboarding and fraud prevention solutions while bridging communication gaps.

Our suite of digital identity solutions safeguards your customer accounts, including continuous customer identification, dynamic risk scoring, phone number intelligence, and communication tools:

Multifactor Authentication

MFA blocks 99.9% of account hacks. TeleSign can help you prevent unauthorized account access and make sure that your digital community is safe, secure, and streamlined with easy-to-implement, one-time passcodes, and multifactor authentication. Every time a phone number is ported, a record is created. TeleSign can evaluate a transaction to see if the phone number associated with the account was recently ported and flag it for a manual review.

Digital Identity Solutions

Using digital identity solutions, TeleSign acts as the ultimate gatekeeper for your platform. We provide a seamless registration process for good users while keeping fraudsters out and reducing fake accounts. We do this in several ways: We use verification products such as two-factor authentication with mobile identity solutions to build a risk profile of each potential user that attempts to enter your ecosystem. By leveraging a more holistic solution, we can cover a wide range of vulnerabilities typically only covered in piecemeal offerings.

ATO

We can help you trace and eliminate fake accounts associated with bulk/fake reviews created to beat an algorithm. As it stands, according to PC Magazine, up to 42% of online reviews are unreliable. Additionally, platform spam and bots degrade the customer experience. TeleSign works to rectify this to add trust between your platform and your customers.

Fraudsters often find free or cheap VOIP phone numbers on the internet. TeleSign's APIs can detect these types of phone numbers and allow you to screen these users out. This allows your platform to cut down on fake accounts that typically exist to cause havoc for your users through phishing schemes and account takeover. Detecting VOIP numbers is just one of the capabilities we offer. TeleSign can also use identity products to identify duplicate or bulk accounts created for promo or referral abuse.

Global Regulatory Compliance

In a world with constantly evolving privacy regulations, it can be tricky for businesses to stay ahead of the curve. TeleSign is GDPR, CCPA, and PSD2 compliant, and we can help your business stay compliant as well. TeleSign helps you provide the best customer experience for your users while avoiding costly fines and reputation damage. Our global privacy and security office makes sure that you can use TeleSign's technology to solve your pain points and do it all in compliance with current laws where you do business.

Your customers' journey in your ecosystem should be fast, easy, and safe. Focusing on all three can increase successful transactions and, more importantly, increase trust in your company. Customers who receive excellent customer service, feel confident and secure in your digital environment, and are communicated to at the right time and place in their journey are more likely to spend more and remain loyal to your business.

Ready to deliver a trusted experience?

Get started

TeleSign