eBook

Beyond authentication: Identifying the person behind the number

TeleSign

What is more personal than personal identity?

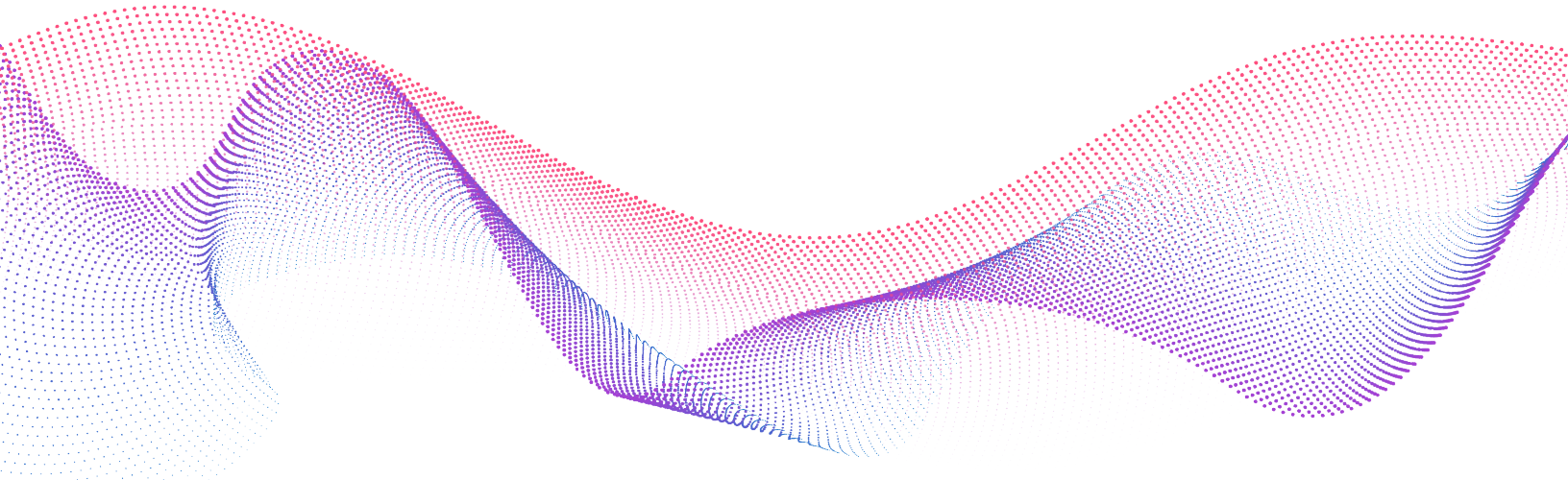
Victims of identity theft often experience emotions similar to when a loved one dies: loss, anxiety, helplessness. In addition, and perhaps overwhelmingly, victims of identity fraud lose confidence in the business they feel did not adequately protect them, often assigning the anger directly to the company instead of the fraudster. In fact, a recent study shows that 85% of customers would avoid using a brand after losing trust.

Building and analyzing digital identity

Today, customers expect you to keep them and their digital transactions safe. To do so, you must ensure the users who enter and interact in your ecosystem are who they say there are—at every touchpoint, every time.

In face-to-face transactions, such as withdrawing money from a local bank, identity and verification happen quickly by showing a government-issued driver's license and proof of address. If the face and signature on the card match the person providing it, the transaction can safely occur.

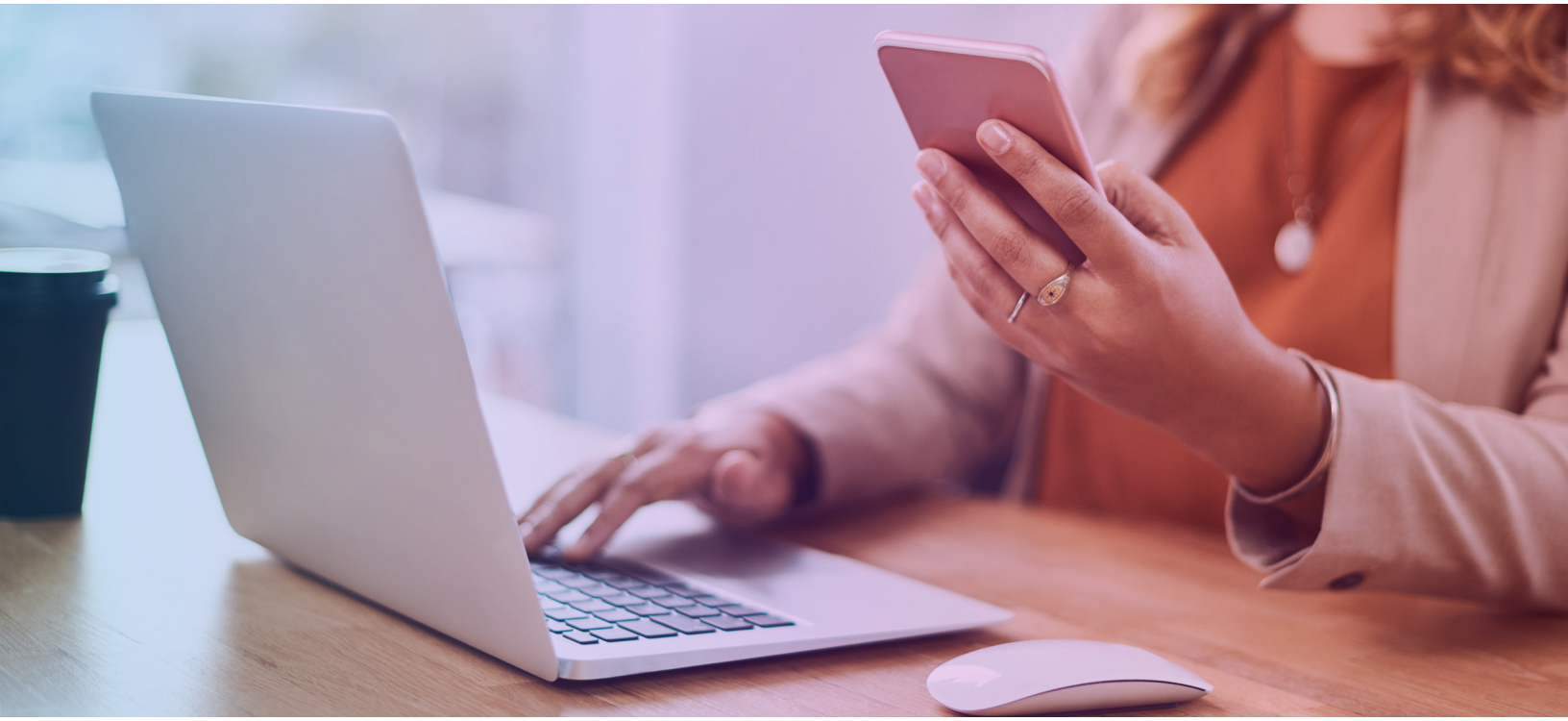
In the digital world, identifying the person attempting to access your ecosystem is more complex, making it critical to follow a consistent and evolving process to build a trusted identity of the user.



Using multifactor authentication as baseline fraud prevention

Customers expect to provide a username and password when creating an online account. They understand its importance in securing a place in your ecosystem and beginning a business relationship with your brand. Though necessary, both you and your customer know that a username and password is no longer enough to verify and authenticate identity. The next step in building and verifying a digital identity is two-factor authentication (2FA).

2FA, or multifactor authentication (MFA), provides a critical, foundational step to protecting your ecosystem and keeping your customers' trust. From global retailers to your local credit union, 2FA is universal and has become a user expectation when creating accounts and transacting. 2FA remains a solid defense against stolen passwords. When customers receive a one-time passcode (OTP) to verify their identity, it ensures they possess the mobile phone. But 2FA does little to verify the person behind the phone number.



Who's the person behind the phone number?

Bad actors have moved beyond stealing passwords to taking over accounts and identities. Today's fraudsters gather details from various sources to assume a victim's identity: stolen email, passwords, and numbers purchased from a breach on the dark web; sophisticated malware and social engineering scams; answers to knowledge-based identifiers from social media postings, and more. If the data is out there, fraudsters will find it and use it in their schemes.

Although 2FA remains essential, fraudsters—as they always do—learn and adapt. 2FA adds a layer of security and protects against account takeovers through stolen or guessed passwords. Unfortunately, fraudsters have found ways around these security measures by exploiting unencrypted burner phones in SIM farms, deploying batches of VoIP numbers, conducting social engineering and SIM swap attacks, and developing and implementing other constantly evolving fraud techniques and practices. Traditional 2FA lacks a digital identification and risk assessment to determine the person's legitimacy behind the phone.

Hidden behind the scenes, phone numbers hold critical insights about the end-user. These identity and behavioral signals offer a complete snapshot of the person attempting to enter and transact in your ecosystem.

To decrease friction for your good users while making life more difficult for fraudsters, the best approach to prevent fraud is to use the information you already have: the phone number used in 2FA. With this approach, you can set up alerts for suspicious behavior with minimal friction to your customers.

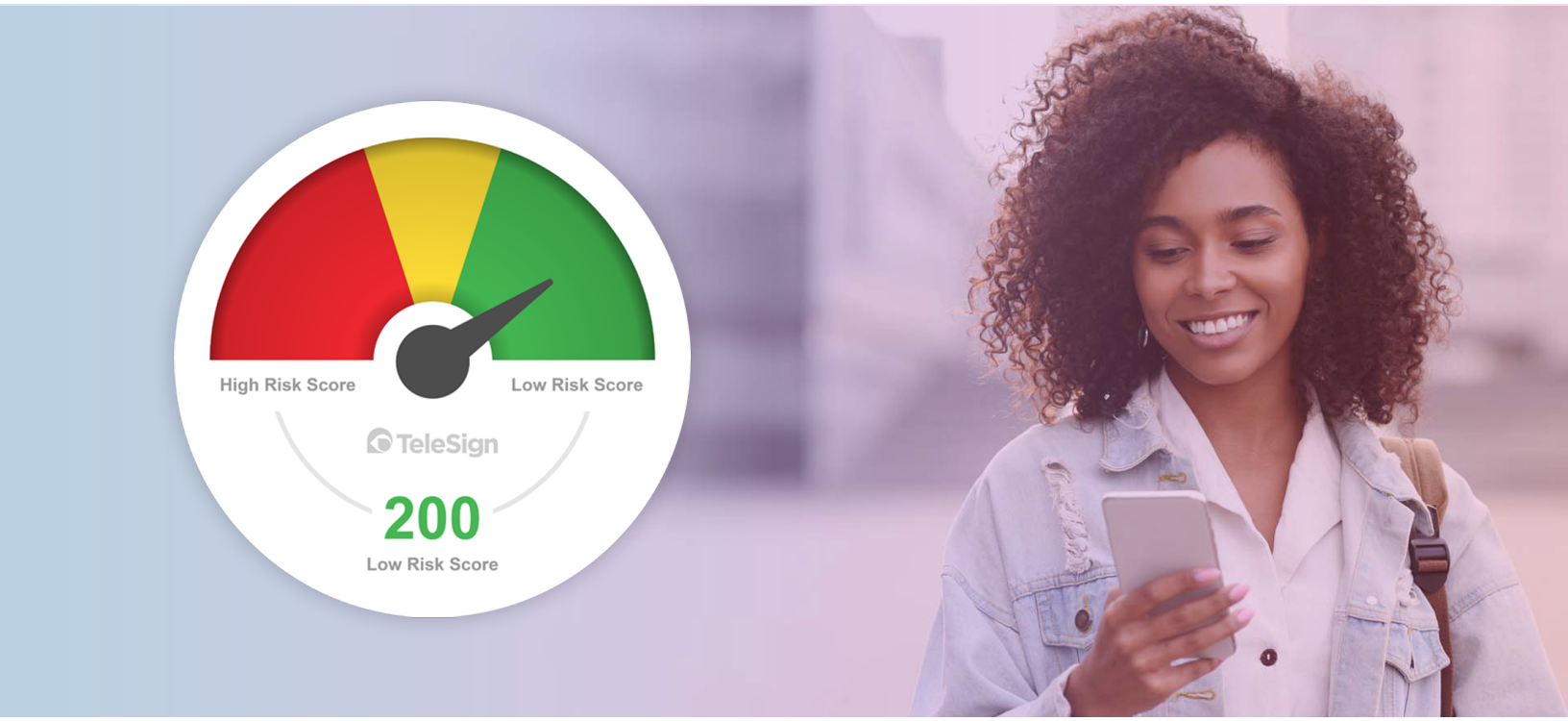
A dynamic, risk-based digital identity assessment adds security without necessarily adding friction, as the check for reputation and risk can happen instantly and seamlessly before or while your 2FA/MFA or biometric verification is happening.

Seamless verification and identification

Using the TeleSign 2FA with risk and reputation assessments, businesses around the globe are protecting their ecosystems from bad actors while providing superior customer service to verified customers.

TeleSign Score is an effective risk assessment that uses machine learning to analyze phone number data and delivers a phone number 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 flagging an interaction, the optional next step is to review the registration or transaction manually. 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.



Certain aspects that TeleSign deems risky result in a higher score. What types of behavior would negatively impact a user's score? A VoIP phone number, a burner phone, or a phone number that has recently changed devices (SIM Swap) each raises a flag and increases the risk score. Score goes beyond 2FA and helps you answer critical security and business questions, such as:

- Is this OTP being intercepted?
- Is this log-in an account takeover attempt?
- Are we wasting money sending an SMS and/or voice call to this number?
- 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.

There is an emotional impact to identify theft. You do not want that pain associated with your brand. When paired with multifactor authentication, Score is the ultimate gatekeeper for digital platforms and helps keep your customers happy, safe, and coming back.

Ready to deliver a trusted experience?

Get started