telesign | routemobile

Proximus companies

Protect and engage throughout the customer journey

Reduce friction and combat fraud in e-Commerce

Businesses that adopt the right strategic and technology framework throughout the customer journey can improve customer experiences, boost revenue, and thwart fraud.

Table of contents

State of e-Commerce

Today, e-Commerce businesses and retailers can reach far and wide to connect with customers. There are unprecedented opportunities to attract customers and increase conversions. In fact, retail e-Commerce sales in the U.S. topped $1 trillion globally in 2022, up over 50% since 2019.[1] But these opportunities come with challenges as well.

Online retailers are seeing rapid growth in sales *and* fraud. Online retailers reported $100B lost globally to fraud in 2023.[2] e-Commerce losses attributable to online payment fraud were estimated at $41B globally in 2022, growing to $48B in 2023.[3] Retailers have also seen a rise in promo code abuse and chargebacks. And 71.6% of consumers worldwide lost money in 2022 due to online shopping scams[4]—which could ultimately lead to diminished confidence in patronizing e-Commerce sites.

Secure online shopping experiences are a must—but not at the expense of great customer experiences. If it's too difficult to create or access an account, customers will find another service to avoid the friction. On the other hand, insufficient security may spawn fake accounts, increase promo abuse, and cause a variety of additional problems within your e-Commerce platform.

Savvy e-Commerce businesses know that every sign-up, sign-in, and interaction with customers must be streamlined and safe. As companies grow, so does the risk of fraud—in size and scope. It's crucial that their fraud protection framework and technology can scale to handle the e-Commerce industry's unique challenges.

At the same time, these businesses must leverage omnichannel and conversational engagement strategies to build trust and improve customer experiences.

Engaging with customers across the entire journey is essential. From pre-sale inquiries to post-sale support, shipping notifications, returns, exchanges, loyalty programs, and reviews, there are numerous touchpoints where businesses can delight customers. Tools like chatbots, omnichannel messaging platforms, and timely engagement solutions play a crucial role in these interactions. Effective customer engagement not only enhances satisfaction but also fosters loyalty and trust.

Businesses utilizing omnichannel communication **retain**

89%

of their customers on average, compared to 33% for those with weak omnichannel strategies.[5]

Additionally, companies with strong omnichannel customer engagement see a

9.5% YoY

increase in annual revenue, compared to 3.4% for others.[6]

These figures highlight the importance of a well-rounded communication strategy in driving e-Commerce success.

Understanding e-Commerce fraud

Balancing usability for customers and protection against fraud is critical to your success. Because fraudsters are getting increasingly more sophisticated in their attacks on e-Commerce businesses and their shoppers, account integrity across the customer lifecycle is essential.

Not every e-Commerce business is the same—and some attract more attention from fraudsters than others. But across the board, e-tailers should take steps to address these leading types of fraud.

4 out of every 10

shoppers on a retail site are not human.[7]

Common cyber fraud terminology

Phishing

When a fraudster poses as a trustworthy entity and sends authentic-looking emails to trick victims into revealing sensitive information—like bank account numbers, credit card numbers, and account credentials.

Pharming

Involves sending victims to fake websites to steal personal or financial information and/or install malicious code on the victim's computer.

Whaling

Sometimes referred to as "spear-phishing," targets specific high-ranking executives within a company to trick them into sharing sensitive information or even sending a wire transfer to a fraudulent account.

Bots

Short for robot, this is a software program that performs automated tasks or mimics human user behavior. Because they can operate much faster than humans, fraudsters use them to create fake accounts at scale and launch account takeover attacks, scanning for website vulnerabilities and other malicious activities.

Types of e-Commerce fraud

1. Social engineering fraud

The most common types of fraud attacks against e-merchants in 2022 were through social engineering tactics like phishing, pharming, and whaling[8]—designed to get individuals to reveal personal information like passwords and credit card numbers. Reseller bots, which are designed to buy items faster than a human can (so a fraudster can resell those items at a profit) were also prevalent.[9] In fact, 47% of online traffic in 2022 came from bots, and 20% of that bot traffic went on to retail sites.[10]

2. New account fraud and fake accounts

Fraudsters attempt to create new accounts that aren't for real people—and they use bots to create them at scale when verification methods aren't in place. Once they're in, the types of potential fraud attacks are endless, from card testing and web scraping to inventory abuse and fake reviews that diminish seller credibility. Fraud from automated attacks was up 71% in 2022.[11]

3. Account takeovers (ATO)

This is a form of identity theft where account access is compromised, and someone who is not the legitimate owner of the account takes control of the account. Account takeover losses increased by 90% in 2021[12], and 1/3 of all login attempts on retail e-Commerce sites were account takeover attempts.[13]

4. Promo abuse

This is when fraudsters create multiple fake accounts to take advantage of discount codes, rewards, sales, and other types of promotions. Research suggests that $1B in rewards value is lost every year to fraud[14], and the promo abuse total for U.S. businesses in 2022 was $189B.[15]

5. Communications fraud

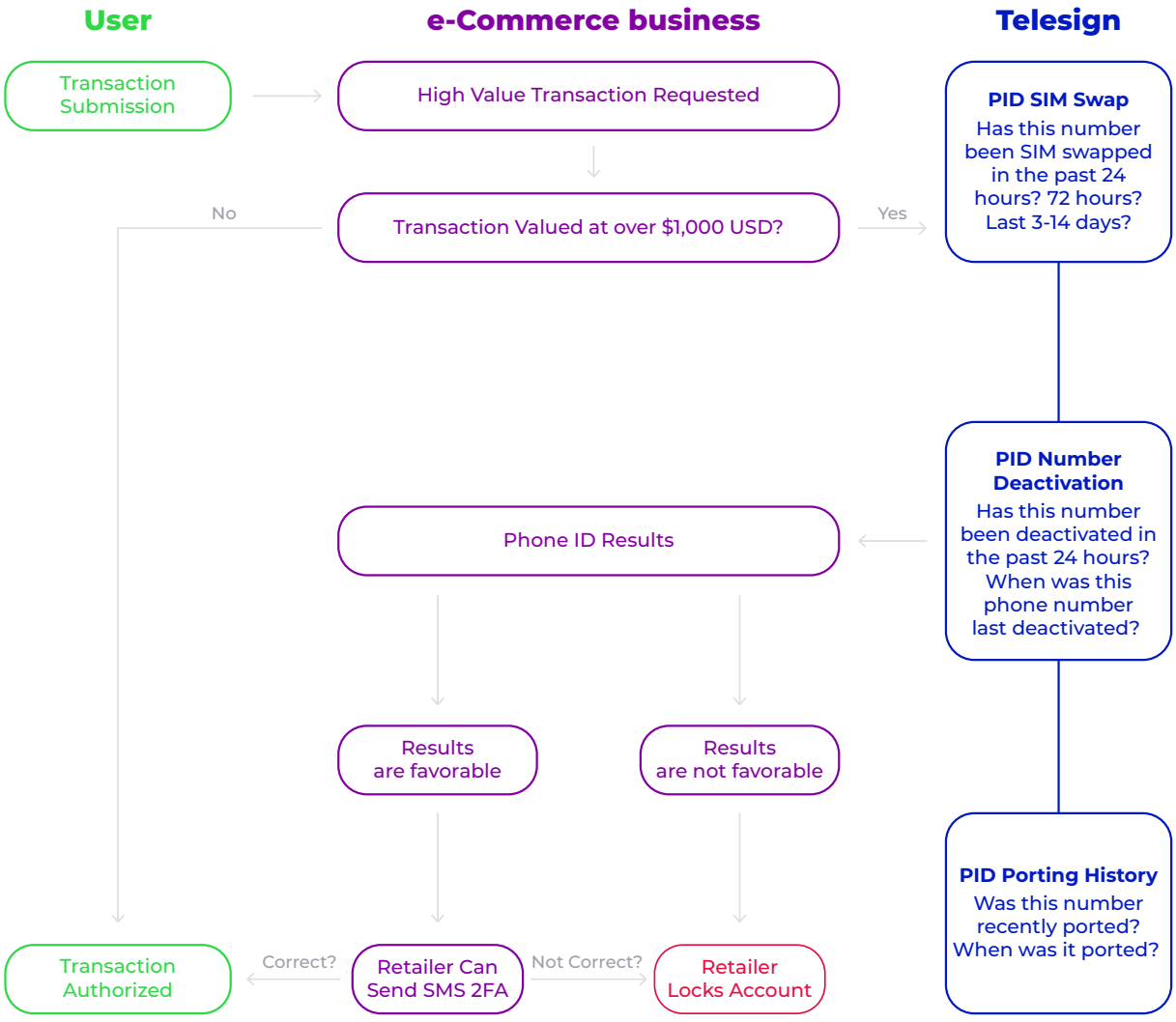
Referred to as toll fraud, SMS pumping, or International Revenue Share Fraud (IRSF), this type of fraud is unknown by many businesses. It involves fraudsters that exploit vulnerabilities in SMS messaging systems used by e-Commerce businesses to trick the business into sending messages to premium rate numbers—generating a large volume of traffic and fraudulent charges to the business. This type of fraud costs businesses more than $8B annually, and an average attack can result in $50K in damages.[16]

6. Chargeback fraud

This type of fraud, also known as first-party misuse (FPM), occurs when a customer intentionally disputes a charge, with the goal of receiving a refund, and keeps the product. This type of fraud is on the rise, with more than six in 10 merchants citing an increase in FPM over the past year.[8]

Protect against chargebacks and high-value losses

With the right verification solutions in place, e-Commerce businesses can greatly reduce risk for their customers, their brand reputation, and their bottom line.



The goal:
Protect and engage throughout the retail customer journey

Avoid an identity crisis

Today's consumers fear digital fraud and believe it's on the rise. 94% of consumers agree companies bear the responsibility to protect their digital identity and privacy.[17] Data breaches have a profound, negative impact on brand perception—and sometimes all it takes is a single data breach for a brand to lose a customer forever. In addition, many customers are likely to tell everyone they know not to trust that brand either.

43% of data breach victims stop using that brand.[15]

44% tell friends and families to avoid a brand after a data breach.[15]

30% post about it on social media.[15]

When a new customer interacts with an online retailer, it sets the tone for how they view the company. The sign-up process and account verification process must be simple, straightforward, and require minimal work from the customer.

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, 17% of online shoppers abandoned their cart because of a complicated checkout process.[18] At the same time, making things too easy, and granting access without proper authentication, increases the risk of fraud for the consumer and for the e-tailer.

E-Commerce companies find themselves coping with the cost and hassle of fake accounts. These fraudulent accounts are used for a variety of nefarious purposes, such as identity theft, fake product reviews, platform spam, promo code abuse, and phishing attacks—even to gain access to other systems for potential ransomware attacks.

The bottom line: strong security and potential fraud detection are paramount in e-Commerce. Although they're the foundation for trust and confidence, many businesses lack the right strategic framework and technology to address these issues on their own and 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.

E-Commerce concerns by the numbers

46%

of identity fraud incidents were eCommerce and "card-not-present" transactions.[19]

Dangerous bots make up more than

50%

of automated internet traffic.

New account fraud increased

109%

in 2022.[19]

Account takeover losses increased by

90%

in 2022.[12]

Online shopping cart abandonment rate on desktops is

72%[18]

24%

of online shoppers abandon their cart because the site wanted them to create an account.[18]

Chargebacks on e-Commerce orders rose

3.4%

in North America in 2022.[8]

A question of balance:
Usability and strong security can coexist

A recurring onboarding challenge is that in the name of “lower friction” adequate verification often doesn’t exist when a person signs up for an account. In some cases, there is no verification process in place to ensure the validity and the risk of the information entered. This means that bad actors can easily create fake accounts at scale, including the use of other people’s email addresses and credentials.

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

Inventory abuse

This is where scripted bots place high-demand merchandise into shopping carts but never actually check out.

Fraud as a Service (FaaS)

Online sellers worldwide are now seeing fraudsters offer illegal activity services to attack sites.[20] Other FaaS schemes include the purchase of fake and stolen emails, VoIP numbers, and SIM cards in bulk.

Bots and scripts

These can generate millions of user accounts in seconds, increasing the risks of data breaches through synthetic identity fraud.

Web scraping

Fraudsters can use bots to extract the HTML code of a website and steal sensitive information.

Card testing

Usually automated with bots, card testing is where stolen payment credentials are used to attempt small transactions online.

Biometrics

This fraud-fighting strategy is used to validate an individual’s identity through physical traits (like facial recognition), but it’s not foolproof or universal. 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. 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 to prevent fraudsters from gaining access at all points of entry. By analyzing digital identity signals at sign-up and at sign-in, a business can challenge risky interactions while delivering a quick and easy customer experience to legitimate users. It's a win for everyone—thwarting fraud before it starts.

Enhancing the e-commerce customer journey through omnichannel engagement

In today's competitive e-Commerce landscape, engaging customers at every stage of their journey is critical. Effective omnichannel communication strategies allow businesses to interact with customers through their preferred channels, providing seamless and personalized experiences. Here, we explore the essential touchpoints in the retail customer journey and how businesses can leverage these moments to build trust and foster loyalty.

Awareness and consideration

- **Brand awareness:** The journey begins when potential customers explore your brand and its offerings. Provide clear, engaging content across various channels, such as social media, websites, and email campaigns, to attract and inform potential buyers.
- **Marketing and promotion:** Offer personalized promotions and deals through tailored messaging to entice customers to take the next step. Utilize SMS, RCS, WhatsApp, push notifications, and email to ensure these offers are seen and acted upon promptly.

Evaluation and purchase

- **Mobile shopping:** Help customers find the right products through detailed product catalogs and responsive search features. Enable customers to easily browse product catalogs using WhatsApp and RCS. Use chatbots to guide users, answer queries in real-time, and provide interactive recommendations based on user preferences.
- **Order placement:** Simplify the order placement process by offering multiple payment options and a streamlined one-click checkout experience right through a customer's messaging app. Offer instant support to reduce cart abandonment.
- **Alerts and notifications:** Keep customers informed about their order status through real-time alerts and notifications. Utilize journey orchestration tools for comprehensive messaging solutions to ensure timely updates across all messaging channels.
- **Upsell and cross-sell:** During the purchase process, suggest complementary products or services to enhance the customer's shopping experience and increase sales. Deliver personalized recommendations through various channels to make this process seamless.

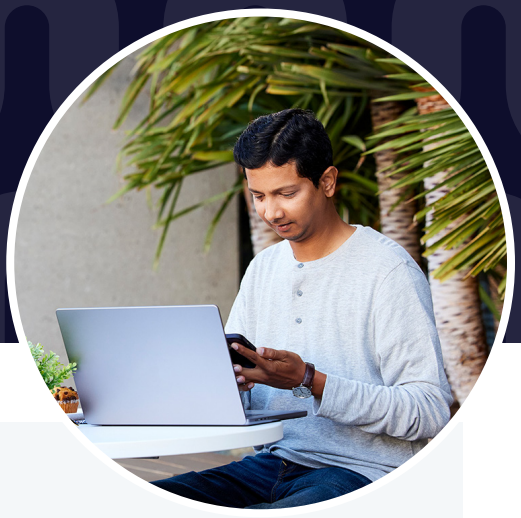
Customer care and support

- **On-demand support:** Offer robust customer support during the transaction process to help resolve any issues quickly. Enable omnichannel support through chatbots, email, and phone to ensure that customers can reach out through their preferred method.
- **Post-sale support:** Address customer complaints and issues efficiently to turn a potentially negative experience into a positive one. Provide easy access to support through multiple channels, such as chat, email, and social media.
- **Feedback and reviews:** Collect post-purchase customer feedback to understand customer needs and areas for improvement. Utilize surveys and review requests through SMS, email, or app notifications to encourage customers to share their experiences.
- **Loyalty program and referrals:** Build long-term relationships through loyalty programs and referral incentives that boost customer retention. Communicate these programs effectively through personalized messages that encourage participation and foster loyalty.

By integrating these touchpoints into a cohesive omnichannel strategy, businesses can create a smooth, engaging, and secure customer journey—while helping you build and maintain consumer trust.

Build trust at every point of engagement

The best way to keep customers in and keep fraudsters out? An always-on approach that delivers Continuous Trust.™



1. Safe, simple, and secure onboarding

Fast-track legitimate customers all over the world with quick and easy sign-up while intelligently challenging risky interactions. All it takes is a phone number to stop fraudsters from opening new accounts and gaining access to your shopping platform.

2. Account security across the customer lifecycle

Using phone number intelligence, you can unlock a continuous stream of real-time identity signals to protect you and your customer. Prevent ATO by automatically challenging suspicious activities like recent SIM swaps, personal information updates, password resets, and more. Automated traffic monitoring also helps protect businesses from IRSF attacks.

3. Communication for every encounter

Seamlessly engage customers via their preferred methods and devices, keeping them informed at every stage of the journey. Deliver optimized customer service experiences with one-way and two-way exchanges—so customers receive the notifications they expect and can reach the right service channels when they need them.

This process achieves protection by using:

Dynamic risk analysis

Weigh the risk of every user's interaction at sign-up and sign-in to prevent account fraud, platform spam, and promotional abuse. This type of risk analysis helps companies take the appropriate action to allow or block a user in milliseconds. The best-in-class solutions that offer this functionality integrate seamlessly with existing security frameworks and tech stacks.

Phone number intelligence

Curtail the creation of fake accounts and promo abuse with intelligence about the phone number integrated seamlessly into your verification workflows. Detect suspicious devices like VoIP numbers and SIM farms to ensure that only legitimate users can get through the onboarding workflow and get access to your e-Commerce platform. Using phone number and subscriber attributes, companies can monitor traffic for suspicious patterns and then compare account access requests against a global telecom fraud database.

Digital identity verification

Authenticate new sign-up and sign-in attempts, as well as account changes, to mitigate risk from bots and fraudsters and streamline verification to maintain the integrity of your digital platform. While SMS and Voice are the workhorses of MFA and OTP delivery, other options are viable, including email, WhatsApp, Viber, RCS, and push—just to name a few.

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. With this process in place, online retailers are equipped to make fast and smart decisions.

Omnichannel interactions

Be where your customers are. Enable one and two-way engagement across SMS, RCS, Email, WhatsApp, Viber, and more. Utilize these channels to provide timely and personalized communication, enhancing customer satisfaction and loyalty.

Journey orchestration

Build tailored customer experiences. Orchestrate the customer journey across multiple touchpoints. Use low-code/no-code flow builders to easily design, execute, and optimize customer journeys in real-time— enabling you to send the right message, to the right person, on the right channel, at the right time.

Email marketing and automation

An effective email marketing solution helps businesses deliver targeted email campaigns with high deliverability rates. Leverage advanced analytics and segmentation tools, to ensure that your email marketing efforts are effective and engaging.

Automated 24x7, 365 support

Use chatbots to automate customer interactions, providing instant responses to common queries and guiding users through their journey. Chatbots can handle various tasks, from answering FAQs to assisting with order placements and tracking.

telesign | routemobile

Proximus companies

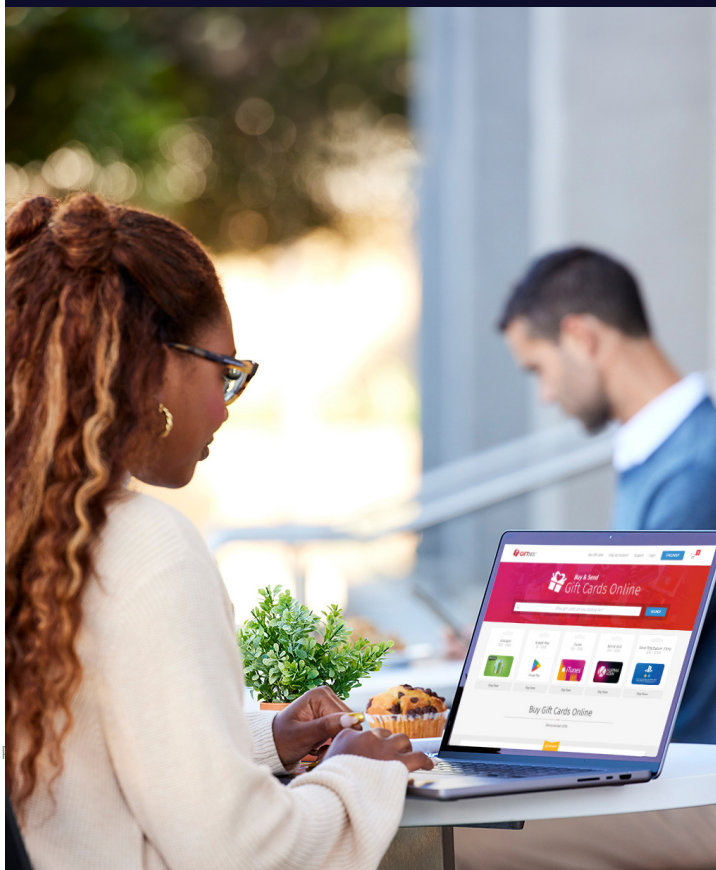
Customer success

GIFTNIX™

Giftnix combats e-Gift fraud with digital identity solutions

Online gift card store Giftnix needed to combat an influx of fraud without adding too much user friction at checkout. They integrated Telesign's Intelligence and SMS Verify into their existing workflows. Using this multi-layered security approach, they were able to:

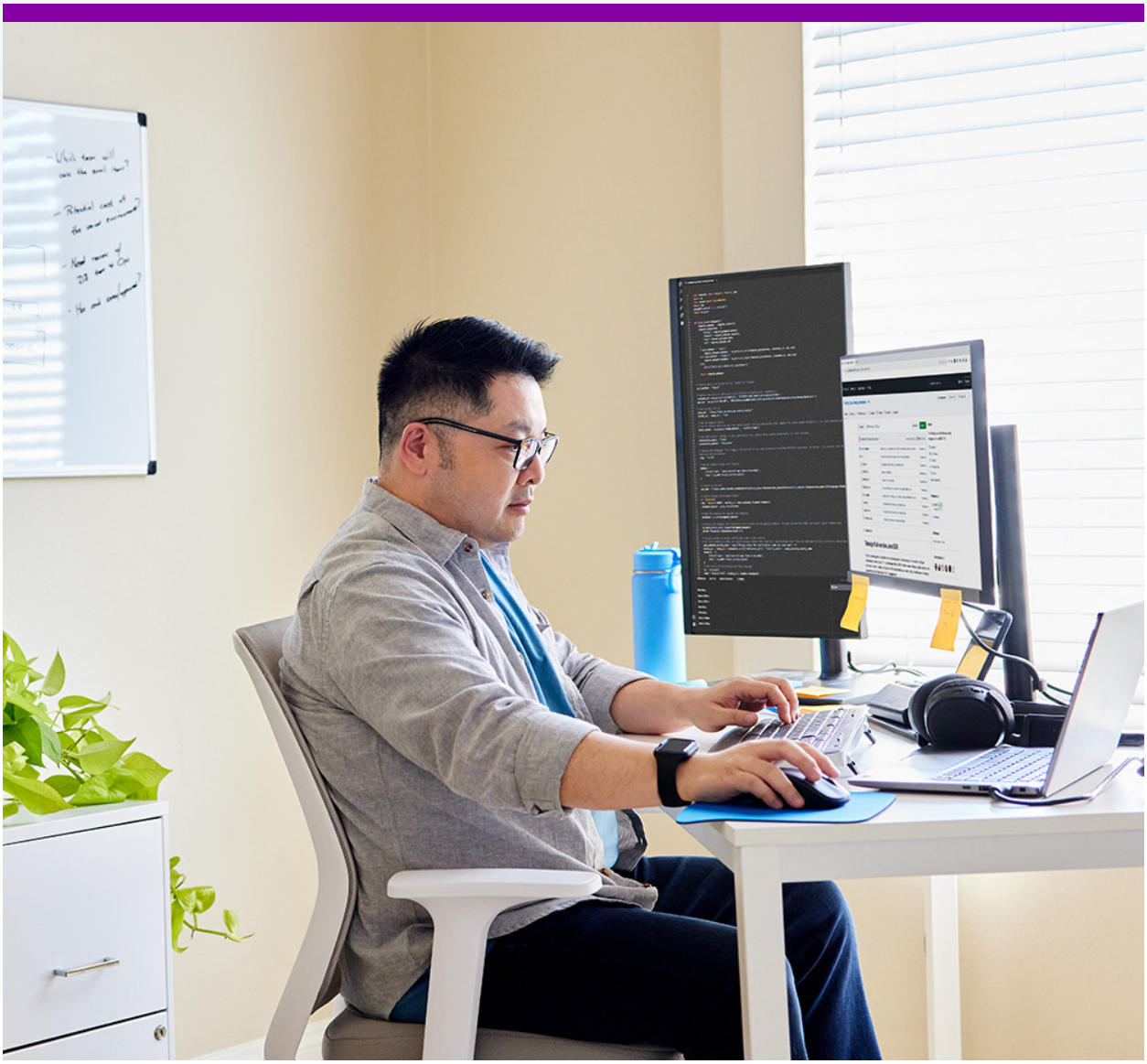
- Verify legitimate customers instantly, keeping fraudsters out.
- Reach customers globally via SMS for additional verification.
- Significantly reduce credit card chargebacks.
- Decrease customer service calls and boost satisfaction.



Putting verification into practice

Telesign's solutions connect all the dots quickly and seamlessly. By harnessing billions of global identity signals—online, mobile, behavioral, geographic, and more—verification solutions create a sophisticated risk model that e-Commerce companies can use to embed trust into the onboarding process and beyond.

IT and security teams will be happy to know that it isn't necessary to rethink or rebuild security infrastructure or data to implement these solutions—they seamlessly integrate into any existing tech stack. That's because the verification data, typically collected during sign-ups, already exists within a business. And if this isn't the case, the business can pull the required data from existing systems and databases—such as a mobile phone number.



A best practice model takes shape: from verification to engagement

When organizations adopt a more advanced, trust-based approach to digital verification—through a solution like Telesign—several important benefits occur.

Block fake accounts at sign-up and sign-in

Using MFA, machine learning, digital identity verification, and dynamic analysis based on billions of risk signals, they can establish trust in milliseconds.

Protect brand reputation

Delivering a safe, streamlined experience is key to building trust and turning anxious shoppers into confident buyers. Plus, it can block fraudsters that spread false news and generate other problems that can harm reputations.

Improve the shopping experience

Built-in omnichannel customer care includes order alerts, shipping notifications, secure communications, and peace of mind that encourages repeat business.

Boost customer engagement

Secure APIs can deliver two-way conversations for effortless and reliable customer communications across the world via customers' favorite methods, like SMS, RCS, WhatsApp, Voice, Email, and Viber.

Offer global protection

Online retailers can reduce risk as they expand their business beyond borders. With Telesign, it's possible to securely onboard customers in more than 200 countries and 90 languages.

Reduce the risk of chargeback fraud

By verifying identity, online retailers can know if activity on their site is coming from a real customer or not—decreasing the chances of fraud and chargeback losses.

Build confidence and accelerate growth

Verifying a customer's identity during the interaction means you can create the option to send even stronger offers with greater confidence to the actual customer and not waste offers sending to unverified recipients.

Fight promo abuse

When a fraudster is identified by a phone number, using fake emails and other tricks to get around outdated verification methods, the system simply won't work—which prevents them from gaming the system.

Reduce cart abandonment

By streamlining sign-up and verification, e-Commerce sites can build affinity from the start, which can in turn boost conversion rates.

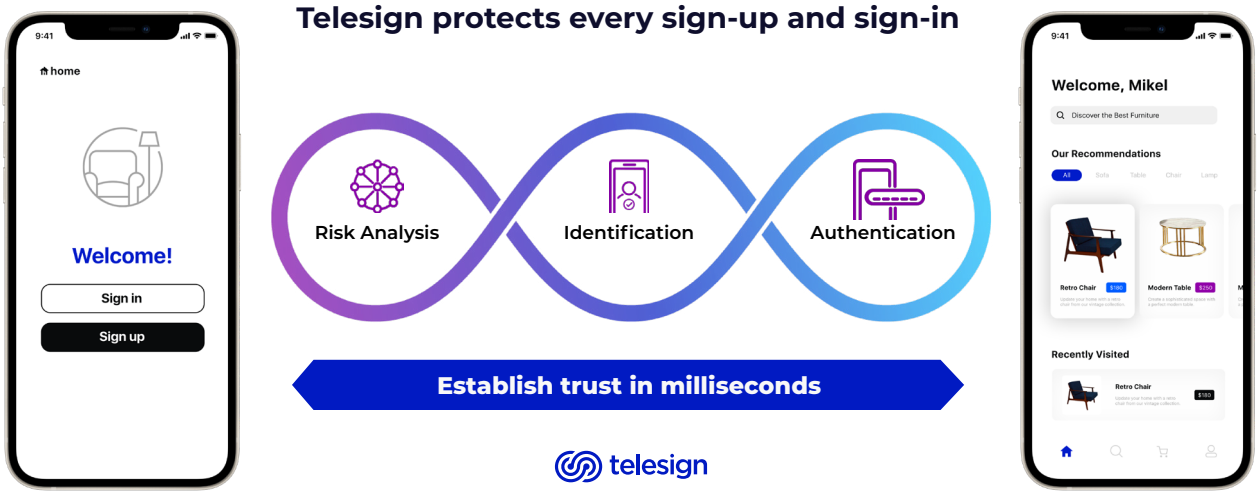
Build Continuous Trust™

Consumers often make split-second decisions about which brands they can trust with their data. Brands that invest in proactive fraud-fighting solutions and prove their trustworthiness are the ones that will win in the digital economy.

The answer to e-Commerce fraud: A balance of usability and protection

As the e-Commerce industry continues to grow, strong customer verification isn't just desirable—it's mission critical. With the right technology framework and approach in place, it's possible to deliver a smooth sign-up experience while protecting the business.

But the benefits don't stop there. Online retailers can lower customer acquisition costs and ensure that conversion rates are legitimate. Today, strong digital identity verification and secure engagement are at the center of e-Commerce—setting up businesses for continued and future success.



Ready to learn more?

Find out how to build and maintain a secure and trusted experience with your customers at every stage of their journey.

Talk to sales

Sources:
1 Digital Commerce 360.
2 Riskified, 2023.
3 Statista.
4 Statista.
5 Forbes.
6 Moengage.
7 Imperva.
8 2024 Global eCommerce Payments and Fraud Report, MRC
9 Statista.
10 Security Magazine.
11 The State of Fraud 2023, Signifyd.
12 Security.org.
13 Forbes.com.
14 Shopify.com.
15 Ekata/MasterCard.
16 2021 State of Communications Fraud, Technology Research Institute.
17 2023 Telesign Trust Index Report.
18 Forbes/Statista.
19 Javelin Strategy.
20 Statista.

About Route Mobile

Route Mobile empowers enterprises to engage and interact with their customers through seamless digital communication. With robust CPaaS solutions that offer unparalleled scalability and global reach, we enable Continuous Engagement.

About Telesign

Telesign protects and defends companies, customers, and the digital interactions between them. With powerful AI that delivers identity with speed, accuracy, and global reach, we enable Continuous Protection.

telesign | routemobile

Proximus companies