State of Digital **Identity Fraud**

February 2024 – v.1.0

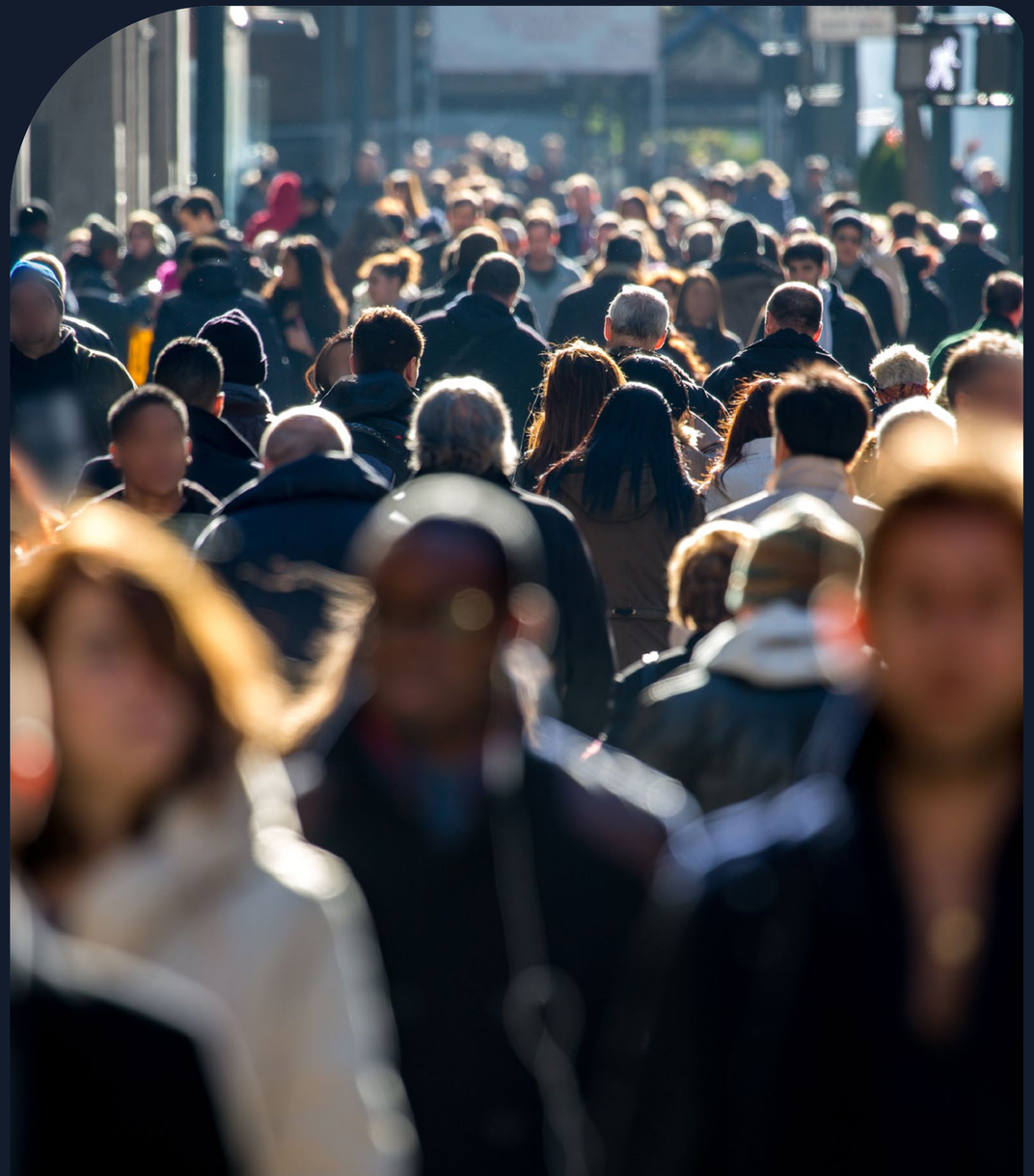
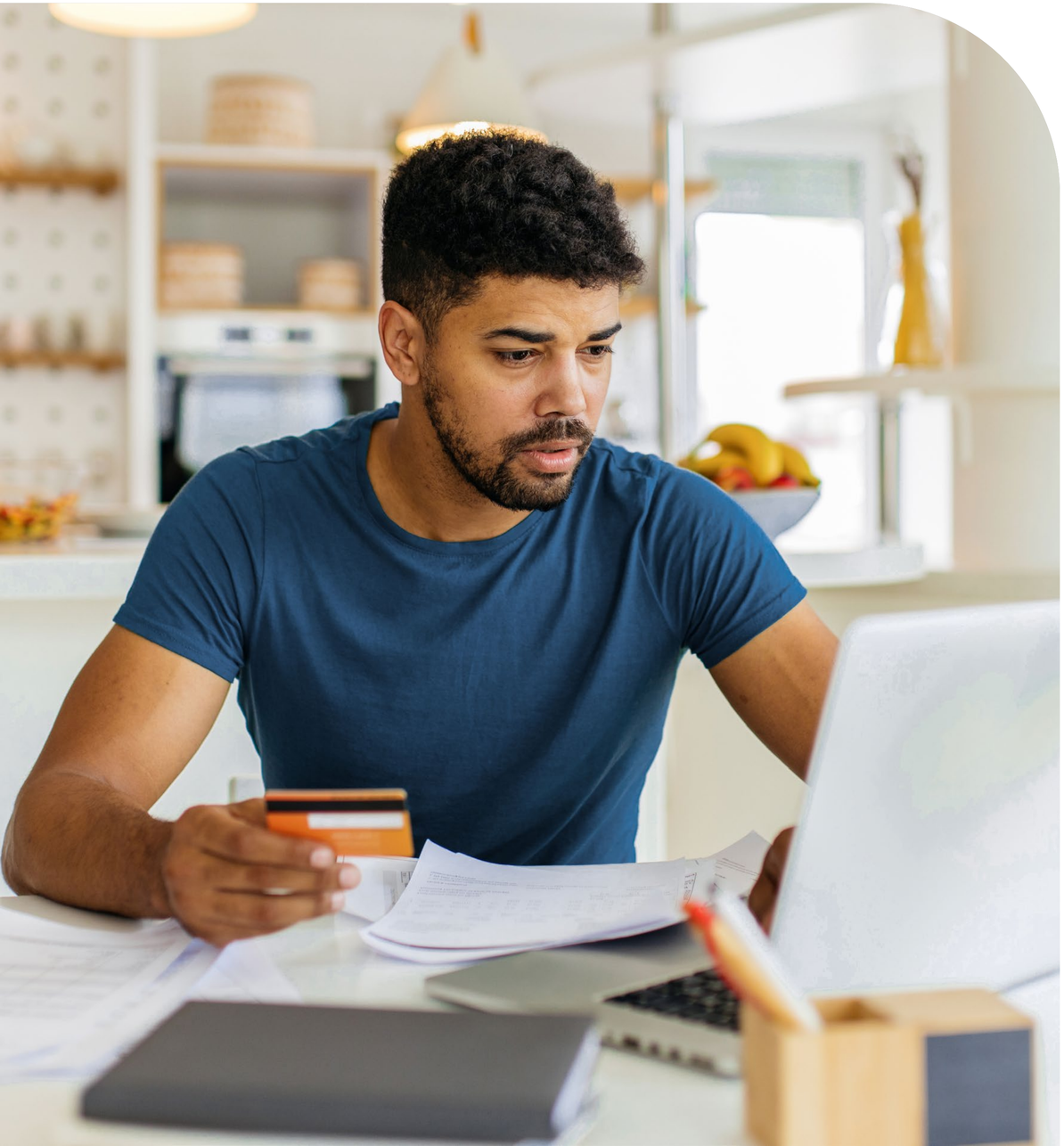


Table of **Contents**

From nuisance to massive liability

From the creation of fraudulent bot-generated user accounts to costly account takeovers of high-value customers to identity hijacking during the account recovery process, online fraudsters continue to exploit every gap in the security of online accounts. Let’s dive into the world of fraud and how we can help mitigate risk surrounding the topic.



The impact of fraud on businesses

More than just an inconvenience

Fraud generated by automated bots and real-life bad actors and fraudsters remains a significant threat for nearly two-thirds of midsized to large e-commerce companies. And fraud costs, as a percentage of annual revenue, also are on the rise. Not only can this impact your cost of acquisition by having to pay for fraudulent users in your scalable SaaS systems, but it can lower the customer lifetime value by violating mutual trust between customers and companies.

Here's what you need to know:

24%
of account takeover fraud victims had their contact information fraudulently changed

Aite-Novarica 2022 U.S. Identity Theft: Adapting and Evolving

Account Takeover attacks increased
354%
YoY in 2023

Sift's Q3 2023 Digital Trust & Safety Index

The global average cost of a data breach reached
$4.45 M
in 2023

The 2023 Cost of a Data Breach Report

Merchant losses from online payment fraud will exceed
$91 B
annually in 2028

Online Payment Fraud: Market Forecasts, Emerging Threats & Segment Analysis 2023-2028

As you can see, without having a plan in place to mitigate the risk of fraud, you can lose millions of dollars per year.

Let's explore what types of fraud companies are facing today.

How fraud is typically committed

Online fraud – a colossal challenge

The surface area for fraud is so vast that no attack vector takes priority over others. However, here are a few key types of fraud we've seen cause the most significant damage to a company's reputation and bottom line:

Synthentic Identity Fraud

Synthetic identity fraud uses just enough information about a real person that an account seems real. According to Lexus Nexus, a synthetic identity is a combination of fabricated credentials where the implied identity is not associated with a real person. Fraudsters may create synthetic identities using potentially valid social security numbers (SSNs) with accompanying false personally identifiable information (PII).

Impersonation Fraud

Impersonation fraud is the act of using someone else's name to sign up for or sign into an account. Whether the fraudster is selling goods from suspicious origins or illegally purchasing goods or they are trying to gain some other sort of advantage, the results can be devastating. Between reputation soiling, compromised business integrity, misinformation, impersonation fraud can add complication and erode trust for all involved.

Promo Abuse Fraud

Promo abuse allows a fraudster to use a VoIP number or other type of disposable phone number to create multiple fake customer accounts to take advantage of a customer promotion designed for limited use.

SMS Traffic Pumping Fraud

SMS pumping, also known as artificially inflated traffic, happens when fraudsters take advantage of a phone number input field to receive a one-time passcode, app download link, or other SMS message. If this input field lacks controls, the attackers can inflate traffic and exploit your app. Fluctuating traffic can cost an organization as the demand on services suddenly spikes and puts unexpected pressure on providers.

Social Engineering Fraud

Social engineering fraud is a broad term that allows a fraudster to leverage trust to convince a victim to give them information that will allow the fraudster to obtain confidential information (like a username, password, or other information) or something of value that leaves the person voluntarily compromised.

SIM Swap Fraud

SIM swap fraud is when a fraudster is looking to use a stolen phone to take over a victim's phone number to execute a nefarious or questionable act. The idea is that they are able to get into an account, even when there are protection factors like second factor authentication (2FA) because they are in possession of the phone and are able to verify their "identity."

Strategies to avoid new account fraud

There are multiple types of fraud and we see these happen in the following contexts. The first is relatively self-explanatory, and really focuses on when a user opens a new account. The remaining types of fraud are when an account is compromised. When an account is compromised, it's likely when a user logs in to their account, tries to manage or use their account to transact business. Let's get started.

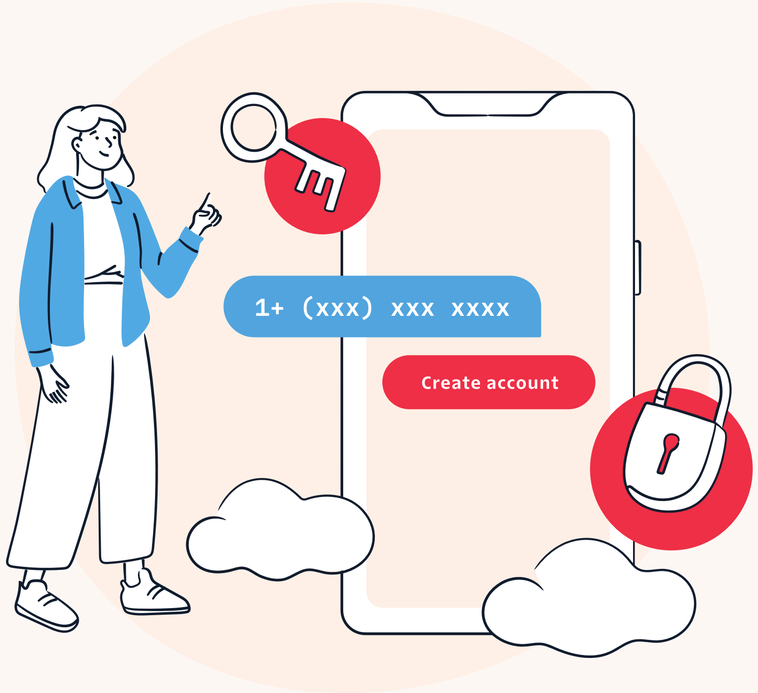
Use methods that simplify user flows and reduce friction

When a customer wants to open a new account with your business, the last thing you want to do is make that experience cumbersome.

At the same time, you want to cultivate their confidence in your commitment to keep their information safe. So, how do you build a frictionless experience while garnering trust?

Let's walk through the steps to avoid new account fraud:

- **Step 1: Remove unnecessary activation steps** - Boil your onboarding process down to the minimum viable checkpoints to simplify the user experience.
- **Step 2: Meet customers where they are** - Use the customer's preferred channels to verify their identity.
- **Step 3: Passively confirm user identities** - Confirm their presented identity with phone intelligence data to ensure a match.
- **Step 4: Prioritize reliable deliverability** - Choose the right vendor to help execute verification strategies to avoid customer frustration.



QUICK TIP
Phone numbers reveal useful information that can be used to verify the authenticity of an account.

First, phone numbers are identified as either a landline, mobile, or Voice over Internet Protocol (VoIP). Second, phone numbers are associated with countries of origin. Finally, phone numbers can be tied back to telecommunications carriers. Organizations can review spikes in traffic and usage that are anomalies. Or review if a mobile phone's SIM card has been swapped out. These strategies might identify if a phone number has been compromised and help businesses filter out potentially fraudulent traffic from specific geographies while also identifying phone numbers associated with real devices owned by real people. Wow!

Ways to avoid account compromise fraud

From logins, password resets, and transactions

After account creation, a customer likely wants to do three things: log back in, do business on or manage their account on your website. With proper user verification and identification on the first interaction, brands are setting themselves up for success. Comprehensive validation strategies means that you can confirm your best customers faster and keep bad actors out.

How can we protect our customers at each step of the way?

Step 1: Re-authenticate the user

What your client really wants to do is get in, get what they need, and get on their way. Offer them a frictionless, yet secure, login flow with two-factor authorization such as silent network authorization.

Step 2: Enable step-up validation

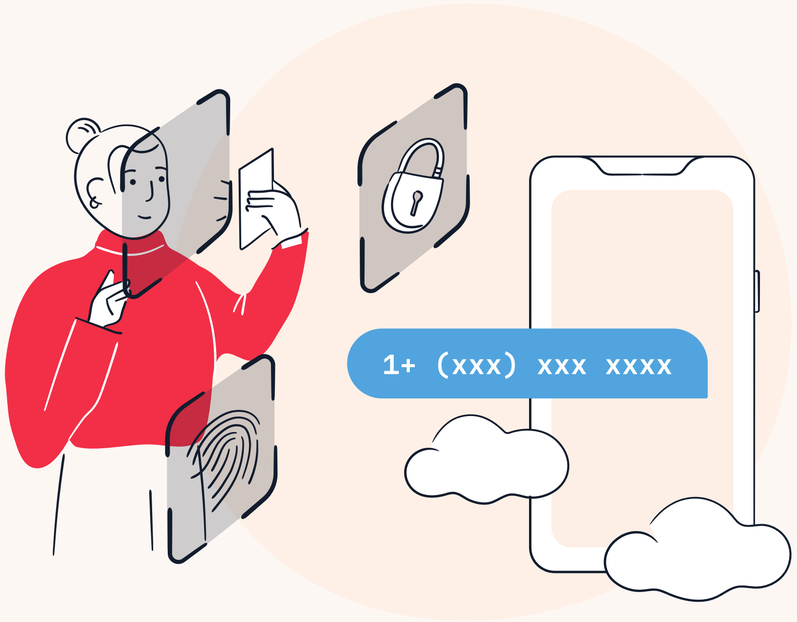
When additional risk signals are raised or more sensitive information is accessed, quick and effective automated validation and step-up security (like asking for additional information) are key to fast tracking good users and adding friction for bad users. This reduces risk to both a loyal customer and the business.

Step 3: Leverage preferred channels, securely

Customers want to edit their preferences, passwords, and channels simply. Allow them to avoid the support site while you reduce costs by answering their questions on their preferred channels, securely.

STEP-UP SECURITY: *Email verification vs. phone verification*

Unlike email, a phone number is a more deterministic method to confirm the user is still in control of their device. Because email can be accessed by any device, email verification lacks the ability to determine the intent or identity of the user.



Twilio helps organizations around the world avoid fraud.

Read a few of our customer's stories:

stripe deliveroo CHOCO duolingo Rappi

Fraud defense checklist

Follow these 9 steps to avoid fraud

- [ ] **Create seamless points of validation**
  Use friction-free authentication that relies on deterministic connections to mobile carriers where available with fallback alternatives such as push notifications, SMS, or voice.

- [ ] **Ensure accuracy**
  Get the full phone number, including the country code, and make sure the national formatting protocol is correct. This is important, as phone numbers are formatted differently worldwide.

- [ ] **Simplify for mobile**
  On mobile platforms, where the device itself might have a phone number directly associated with it, use push verification to keep customers in your app.

- [ ] **Verify validity**
  Just as emails can be fraudulent, so too can phone numbers. The most common method for confirming a working number belongs to the account holder is by sending a one-time code–usually a 4 to 6-digit token–via SMS and asking the recipient to enter that code back into the application.

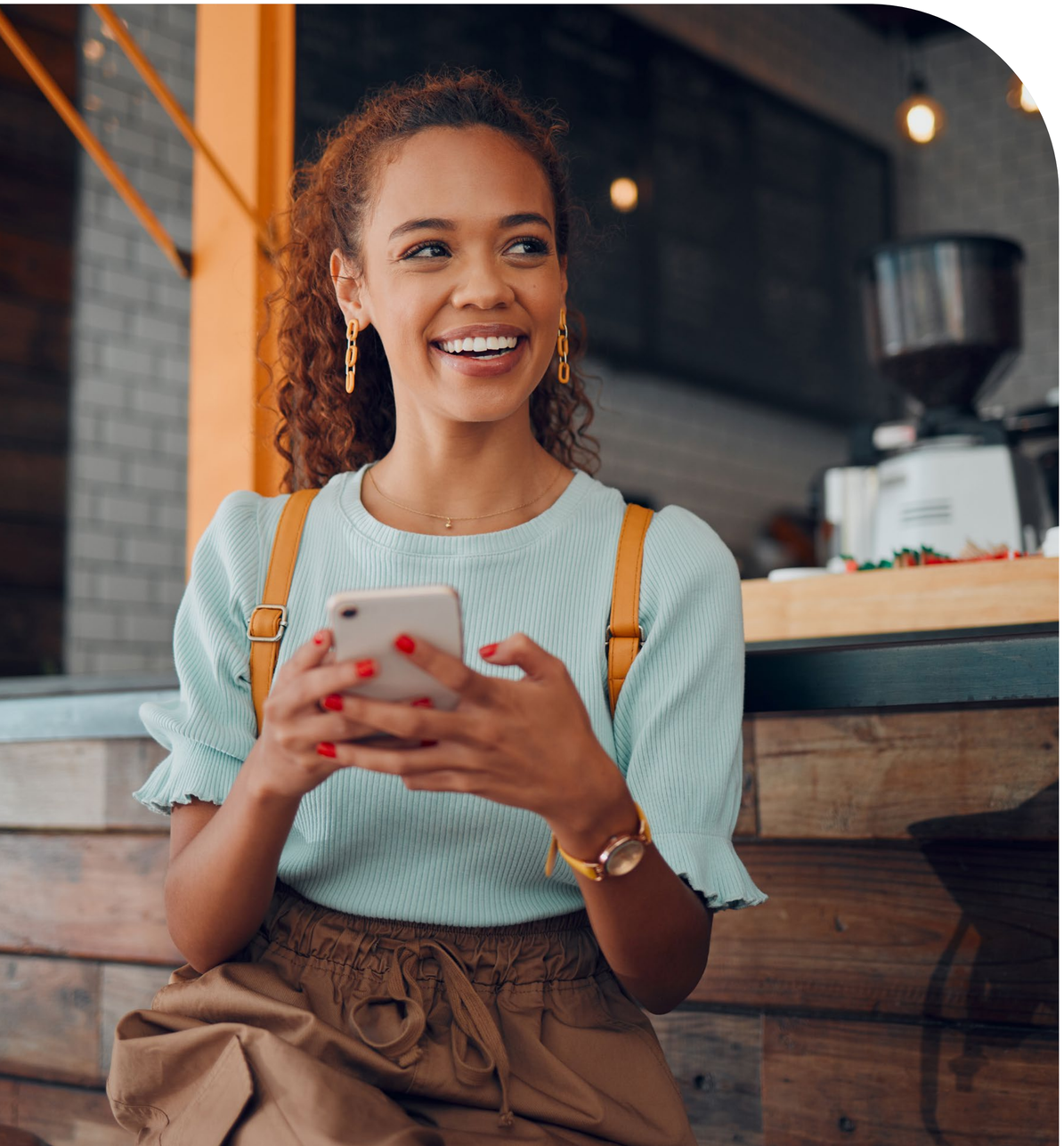
- [ ] **Consider voice alternatives**
  When you are **sending an SMS- based code**, offer the option of a voice call, having the code read aloud over the phone, or **other messaging channels** like WhatsApp, Facebook Messenger or Google Business Messages.

- [ ] **Bolster contact center security**
  Fraudsters commit call center fraud by contacting an organization's call center pretending to be someone they're not. Having agents ask the caller to respond to a phone number verification process before continuing with a conversation will help stop many instances of fraud in their track.

- [ ] **Protect transactions**
  Block financial accounts opened with an email address/ password pair from making withdrawals until a user's identity is verified by phone number. This presents the account owner with a clear trade- off: provide a phone number, and you can access your money.

- [ ] **Implement 2FA**
  Consider implementing a **cloud- based two-factor authentication** protocol into your app. Once a user verifies their identity via a registered phone number, each subsequent login will require an authentication token that a fraudster wouldn't have access to: your user's mobile device. Without that second factor, the impersonator can't log in and commit fraud.

- [ ] **Consider SIM swap detection**
  SMS is also vulnerable to SIM swap attacks. Once the fraudster has a mobile operator convinced that they're you, they can have a new SIM card issued with your mobile number, gaining the ability to access your two-factor authentication (2FA) codes. Butnit's not common for a user to do a SIM swap before making a large external funds transfer or other high value transaction, so checking for a SIM swap before sending an OTP is a great way to deter fraudsters.



The future of fraud protection

Seamless user experience, world-class protection

With fraud more rampant than ever, it may seem that combatting it will require you to jump through more hoops than ever. But in truth, advancing technology is making it easier to offer protection against fraud without compromising the user experience. A few examples include:

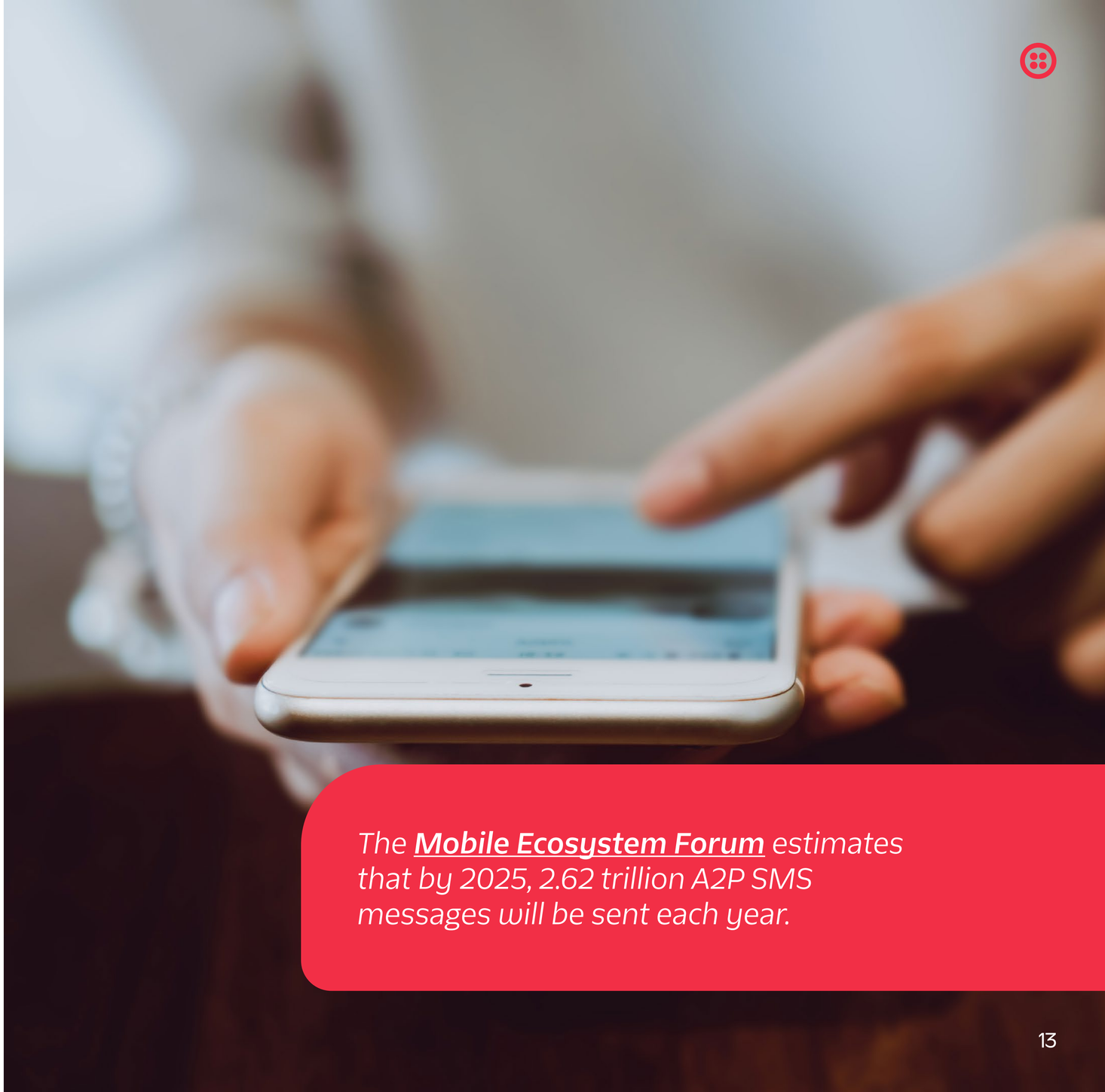
Verify Silent Network Authentication combines deterministic SIM data from our unrivaled partner network of mobile carriers globally with authoritative data signals to verify whether a user is genuine. This means companies can automatically weed out fake users with no input required from genuine users. It provides a completely passwordless, pain-free, and more secure way to sign up or sign back on.

Fraud Guard (included in Twilio's Trusted Activation product) prevents SMS traffic pumping (aka Artificially Inflated Traffic) related fraud by monitoring SMS traffic anomalies.

Verify Geo-Permissions (preferred countries) allows a customer to customize which countries they allow user verification requests to originate from. For example, if a customer is only based in the US - they wouldn't want to pay for SMS OTPs that are requested in Spain.

Verify Rate Limiting allows you to customize how long an OTP token is valid for. Whether it's 1, 2, 5, or ten minutes, you can customize it based on your business' needs. In addition, you can customize the limits you want to enforce for additional flexibility. Looking to limit login tries to five attempts? No problem.

Ultimately, enhancing authentication and fraud prevention solutions is really as easy as finding the right partners with the right tools.



*The **Mobile Ecosystem Forum** estimates that by 2025, 2.62 trillion A2P SMS messages will be sent each year.*

Thanks for reading

If you would like to learn more about what Twilio can do for your business, please ***contact the Twilio sales team*** *or give us a call at 844 814 4627.*

Today's leading companies trust Twilio's Customer Engagement Platform (CEP) to build direct, personalized relationships with their customers everywhere in the world. Twilio enables companies to use their communications and data to add intelligence and security to every step of the customer journey, from sales to marketing to growth, customer service and many more engagement use cases in a flexible, programmatic way. Across 180 countries, millions of developers and hundreds of thousands of businesses use Twilio to create magical experiences for their customers.
For more information about Twilio (NYSE: TWLO), visit: www.twilio.com.

All rights reserved. Copyright @ 2024 Twilio Inc.