

Solution Brief

Account takeover fraud

As more people build their presence online, the opportunity for fraud increases—it's estimated that account takeover attacks rose 72% in 2021 alone. Without a proper strategy in place, account takeover fraud can be hard to detect until the damage is already done. Once a cybercriminal gains access to an account, they are free to carry out a myriad of nefarious acts that create costly issues and cause harm to your business and your customer.

It's harder to maintain trust than to lose it

Account takeover fraud results in a loss greater than money and resources: customer trust. Once a fraudster gains access to a customer's account, they have free rein to wreak havoc. In stopping fraudsters, businesses face the challenge of choosing between friction and customer experience. A solution that effectively prevents account takeovers while not hindering the customer experience is necessary for all businesses operating in the online world.

1 in 5

logins is an account takeover attempt.

Arkose Labs

Telesign account takeover protection

Change suspicious activity such as:



Sign-in attempts from a new location, device or browser



Password resets



High value transactions



Changes to account details or personal information

“At Affirm, we have the best algorithms for evaluating financial risk, and Telesign has the best digital identity data to recognize possible fraud.”

Head of Financial Partnerships



Stop fraudsters in their tracks

Leverage Telesign Phone ID global attributes to unlock real-time digital identity intelligence you need to detect fraud. Strengthen authentications, evaluate risk and build a safer user experience—all without adding friction to your workflows.

Ensure you don't send an OTP to a recently compromised number

Account takeover attribute	Why it matters	Telesign delivers
<p>SIM swap detection</p> <p>SIM swap fraud is a form of identity theft where a criminal electronically or physically steals a mobile phone number by assigning it to a new SIM card. Fraudsters then send the one-time passcode (OTP) to the compromised number to gain access to accounts.</p>	<p>SIM swap is a growing attack with costly consequences. Consumers lose millions while enterprise accounts are penetrated. Once a SIM has been swapped, 80% of attacks are effective.</p>	<p>Very low risk 14+ days ago</p> <hr/> <p>Low risk 3 and 14 days</p> <hr/> <p>Medium risk up to 72 hours</p> <hr/> <p>High risk same day</p>
<p>Porting history</p> <p>Port-out fraud happens when the fraudster poses as their victim and opens an account with a different cell phone carrier and has the victim's phone number transferred — or “ported out” — to the new account with the different carrier.</p>	<p>With billions of identity records available on the dark web, fraudsters use stolen information to gain enough knowledge on a person to convince a new carrier to port-out the victim's phone number.</p>	<p>None No porting history</p> <hr/> <p>Porting history</p> <ul style="list-style-type: none"> Porting date Current/previous carrier Current/previous country Current/previous mobile network Current/previous phone type
<p>Call forwarding</p> <p>Call forwarding or call diversion scams will redirect a telephone call to another phone number. Often a fraudster will call a victim and ask them to dial two digits and the * or # key and then another phone number.</p>	<p>Often, the fraudster promises this is the way to claim a prize or connect them to another party. Instead, all calls are forwarded to another phone number to help the fraudster circumvent OTPs. This attack primarily targets landlines.</p>	<p>False Call forwarding is not enabled</p> <hr/> <p>True Conditional - calls are forwarding when busy or unavailable</p> <hr/> <p>True Unconditional - all calls are forwarded</p>
<p>Breached data</p> <p>In the modern online world, every sign-up and sign-in, like and comment, or add to cart and purchase encompasses trillions of digital interactions that create risk. Online activity gives fraudsters an opening to penetrate networks, compromise data, and steal personally identifiable information (PII), which means everyone is a target.</p>	<p>Millions of data records are breached every day. Telesign Breached Data monitors a dark web database of more than 166 billion breached data records across email, passwords, IP addresses, usernames, PII, geographic locations, phone numbers, financial information, and more. When a user has been identified in this database and takes an action on your site, you're alerted of a potential risk.</p>	<p>Data breach checks</p> <ul style="list-style-type: none"> Name, Address, State, City, County, Country, Device model, Device name, DOB, Age, IP addresses, National ID, Social Security Number, Email, Password, Password plaintext, Username, Phone number <hr/> <p>Output:</p> <ul style="list-style-type: none"> Phone number breached: True/false Additional data breached: True/false Breach date: 2017-05-25T00:00:00Z

Proximus Global, combining the strengths of Telesign, BICS, and Route Mobile, is transforming the future of communications and digital identity. Together, our solutions fuel innovation across the world's largest companies and emerging brands. Our unrivaled global reach empowers businesses to create engaging experiences with built-in fraud protection across the entire customer lifecycle. Our comprehensive suite of solutions – from our super network for voice, messaging, and data, to 5G and IoT; and from verification and intelligence to CPaaS for personalized omnichannel engagement – enables businesses and communities to thrive. Reaching over 5 billion subscribers, securing more than 180 billion transactions annually, and connecting 1,000+ destinations, we honor our commitment to connect, protect and engage everyone, everywhere.



© Proximus Global 2025. All rights reserved.

Learn more at proximus.com/proximus-global