telesign

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.

"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 affirm

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

Challenge suspicious activity such as:

- Login attempts from a new location, device or browser
- Password resets
- High value transactions
- Changes to account details or personal information

Stop a fraudster 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
SIM swap detection 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 OTP to the compromised number to gain access to accounts.	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.	Very low risk: 14+ days ago Low risk: 3 and 14 days Medium risk: up to 72 hours High risk: same day
Porting history 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.	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.	None: No porting history Porting history: Porting date, Current/previous carrier, Current/previous country, Current/previous mobile network, Current/previous phone type
Call forwarding 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.	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.	False: Call forwarding is not enabled True: Conditional - calls are forwarding when busy or unavailable True: Unconditional - all calls are forwarded
Breached data: In the modern online world, every signup 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.	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."	Data breach checks: 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 Output: Phone number breached: True/false Additional data breached: True/false Breach date: 2017-05-25T00:00:00Z

telesign