STOP ACCOUNT TAKEOVER FRAUD

iddataweb

STOP ACCOUNT TAKEOVER FRAUD

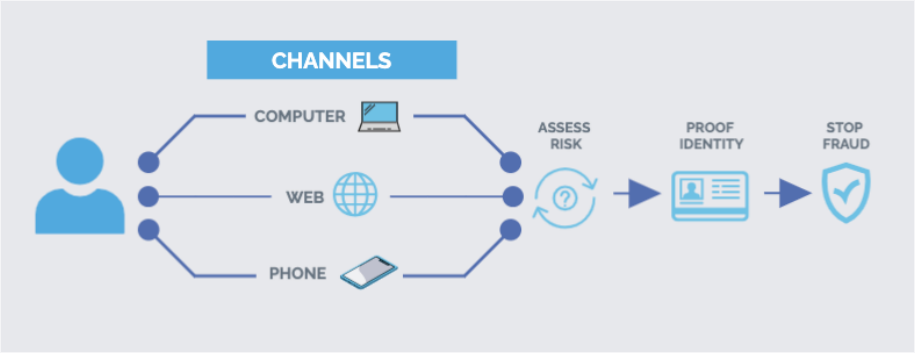
Identity Management and Online Fraud Detection Systems were never designed for modern account takeover fraud. Fraudsters have exploited the holes in the system – freely available PII, passwords and mobile device exploits – to take over accounts through all channels (web apps, contact center and mobile apps). Once fraudsters get into the account with stolen credentials, they change the password and/or MFA and own the account. Research has shown that 1 in 140 authentication attempts are Account Takeover (ATO) attempts and that approximately 22% of consumer accounts are targeted at least yearly according to the FTC.

So, how do you stop it? First, you need strong risk based authentication to determine risk when the user attempts to log in to the account (even with valid credentials). Then you need a better method than a one-time password (OTP) for multi factor authentication if the device, user or behavior is deemed risky. And third, if that fails, you need to proof the user's identity before resetting the password. Put the appropriate friction in place to deter fraudsters without alienating customers. It's a fine balance but if you have trust and confidence that the digital user is the physical user you are expecting, you will reduce fraud and give your customers confidence in your brand.

SO, HOW DO YOU ESTABLISH TRUST?

STEP 1: ASSESS RISK DURING AUTHENTICATION

ID Dataweb's risk engine profiles the user's device and behavior to determine risk during authentication. We look for device risk, network risk, location risk, user behavior risk and global fraud consortium reports. If the user is exhibiting impossible travel, multiple login attempts, coming from a TOR browser, recent porting of the device, or any number of other risk signals, ID Dataweb triggers a risk response and recommends MFA.



STEP 2: STEP UP TO SECURE ANTI-PHISHING MFA (NOT SIMPLE OTP)

If a user/device is deemed risky, ID Dataweb provides multi-factor authentication with FastTap MFA. FastTap MFA increases security beyond OTP by sending a link that can provide additional risk indicators within the MFA flow. The user receives a simple link to click for the MFA check but passively FastTap is also reviewing risk factors such as whether the device has been recently ported or SIM swapped. It compares the location of the MFA to the location of the original authentication to prevent phishing.

STEP 3: REQUIRE PROOFING DURING ANY PASSWORD RESET, ACH OR MONEY MOVEMENT (EFT) ACTIVITY

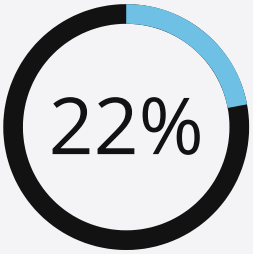
Put an identity verification workflow in front of the user before allowing a password change. This is a hurdle that a fraudster is unlikely to overcome if they have to pass not only "what you know", but "what you are" and "what you have" challenges. This step should give you multiple options on how to verify your user to ensure that they are who they say they are: mobile phone verification, dynamic KBA, government ID + selfie.

STOP ACCOUNT TAKEOVER FRAUD

iddataweb

AN ORCHESTRATION NETWORK IS THE GLUE FOR STOPPING ACCOUNT TAKEOVER FRAUD

ID Dataweb's Attribute Exchange Network (AXN) offers all of the tools to prevent Account Takeover fraud: risk based authentication, secure MFA, and identity verification. ID Dataweb partners with the best of breed vendors for each category to give you a single pane of glass into your identity fraud protection. With a single contract and single interface, you have access to our identity verification workflows and fraud/risk engine across all three channels: web, mobile and contact center.



of all consumer accounts are targeted for ATOs each year

AXN MANAGE

- Risk based authentication & MFA
- Adaptive Federation
- Ongoing re-verification of PII

FastTap MFA

- Fully brandable web-based MFA with less clicks than OTP
- Compare phone against desktop session to pinpoint ATO attempts

AXN VERIFY

- Web, mobile, call center
- Real time & self service
- Adaptive based on policy

These capabilities are simple to insert into any process with our easy to use templates and workflows. We are able to ensure the highest pass rates of the good actors with our unique workflows, giving users every chance to pass without having them call the contact center. Most importantly, you are able to establish digital trust with your users and prevent account takeover fraud.