STOP ACCOUNT OPENING FRAUD

iddataweb

WE STOP ACCOUNT FRAUD BY CREATING TRUST IN THE TRUE IDENTITY OF THE USER DURING ACCOUNT OPENING AND PASSWORD RESETS.

Identity Management and Online Fraud Detection Systems were never designed for modern account takeover and opening fraud. Fraudsters have evolved to know the PII and credentials used for these systems -- there needs to be a better way to establish the trust that the digital user is the physical user you are expecting to open or update the account. Research has shown that 1 in 140 authentication attempts are Account Takeover (ATO) attempts and that 4.1% of new account openings are fraudulent and using stolen synthetic identity information according to the FTC.

So, what can you do to stop it? Verify, verify, verify. Establish digital trust between the organization and its customers during account opening, authentication and any consequential transaction. 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?

Secure all of your channels because fraudsters will find the weak link. Ensure that the contact center knows if an account is under attack on the web site and vice versa. Put the same rigorous process in place for account openings and password resets, protect the account during credential issuance and step up authentication for consequential transactions.

During account registration, regardless of the channel, verify identities. Even if someone knows the customer's information they can't pass challenges that check for government IDs, biometrics, phone ownership AND possession, or dynamic KBA questions. Additionally, device and behavioral analysis will determine elevated risk that requires stronger methods of verification. When the account is created, the user will have to pass these challenges whether they are opening the account from the contact center, the website or a mobile app.

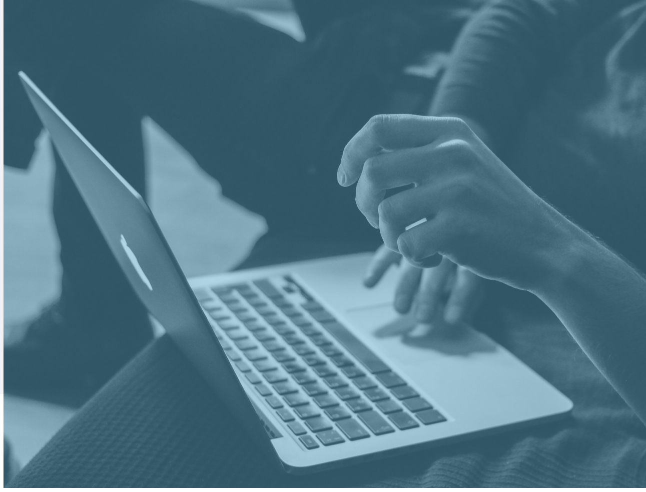
Risk based authentication and secure MFA are essential to protect the account once opened. With these methods, you can check for ongoing trust with the user. If they are accessing the account from the same device and has no other risk signals, then you have a maintained trust with the user. If anything is "off", then prompt for MFA to a device that has an established verified trust.

Perform the same level of scrutiny for any password resets as with the initial account opening. 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.

4.1% of new account openings are fraudulent and using stolen synthetic identity information

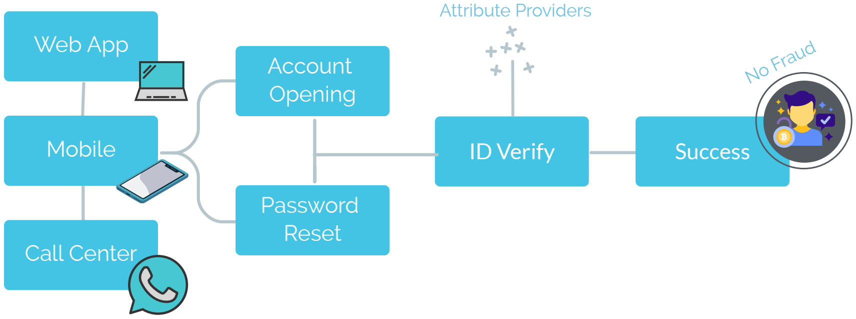
STOP ACCOUNT OPENING FRAUD

iddataweb



THE ORCHESTRATION NETWORK IS THE GLUE FOR STOPPING ACCOUNT FRAUD

The information needed for rigorous account fraud prevention does not sit in one place. It is on the user's mobile device, their government issued ID, the credit bureaus, the telcos, government databases and a variety of fraud prevention databases. It is unreasonable to think that you should have to build a system to do all of this. Enter the ID Dataweb's Attribute Exchange Network orchestration engine.



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.

Identity Verification is 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 and opening fraud.

MobileMatch

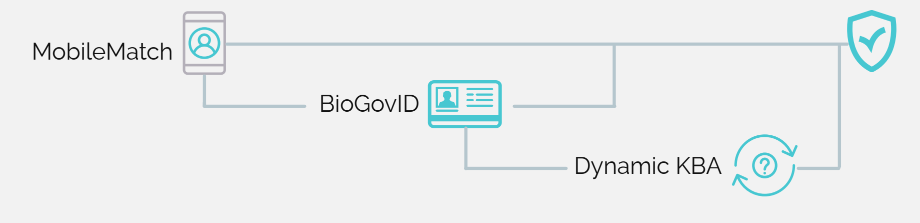
Verifies the user possesses a phone that matches who they're claiming to be.

BioGovID

Verifies the user biometrically matches an authentic ID they possess.

Dynamic KBA

Verifies the user knows personal details about who they're claiming to be.


MobileMatch
BioGovID
Dynamic KBA