BIOCATCH
Less Friction. Less Fraud.

6 Steps for an Identity Proofing Strategy

Keep fraud out of digital account openings with this six-step identity proofing plan using behavioral biometrics.

1

Inspect initial applicant data and behavior

To sort good prospects from fraudsters, assess applicant data for risk as soon as it's submitted.

Compare user behavior to known fraudulent behaviors, automated attack and device information to spot risk.

2

Prefill and collect personally identifiable information

Instead of relying on personal data supplied by applicants, use digitally captured documentation or information directly from parties of record to fill out forms.

Before a form can be submitted, inspect any information an applicant entered for suspicious behavior patterns.

3

Verify legitimacy of collected data

Bring together traditional identity information, digital information and applicant location data to confirm the applicant is who they say they are.
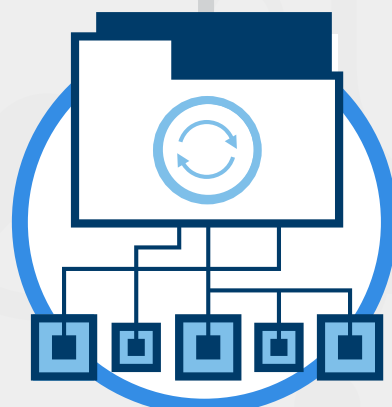
4

Reconcile information and behavior with existing records

Streamline the identity proofing process by comparing the data you collected with third-party or in-house transaction records.

If the applicant has a preexisting account, compare their previous and current behavior.

5

Introduce enhanced authentication measures for risky applicants

Ask the applicant for additional information or documentation, like sending a one-time password, if they are close to failing the process.

Continue monitoring user behavior for more opportunities to pinpoint unusual activity.

6

Decide if the applicant passes or fails

Is the applicant legitimate? Based on the data gathered and behavioral monitoring throughout the process, decide whether to pass, fail or refer the applicant for further investigation.

BIOCATCH
Less Friction. Less Fraud.