EQUIFAX®

FraudIQ Authenticate

A Smarter Way to Authenticate Customers

Being able to positively confirm an identity helps ensure the security and authenticity of remote high-value, high-risk or sensitive consumer requests to help reduce the risk of losses due to fraud.

Minimize fraud risk by knowing that applicants are who they say they are when they sign up.

Whether users are receiving federal benefits, applying for credit, or accessing sensitive information, organizations today are concerned about the risk of fraud, identity theft, and security when offering online services. Positively confirming identities without disrupting the consumer's experience may help you win new customers.

FraudIQ® Authenticate is a set of remote authentication tools — a combination of knowledge and ownership methods — delivered through a flexible, risk-based platform that you can use to confirm identities and help ensure the security and authenticity of account applications and transactions. Rather than relying on only one type of authentication method, FraudIQ Authenticate allows you to waterfall to the most relevant and effective authentication method for a given transaction, from passive, behind-the-scenes device recognition to more stepped-up methods like one-time passcodes, and document verification, to knowledge-based authentication for riskier transactions.

By flagging suspect transactions earlier in the process, you can stop problems before they occur, potentially saving time and money in the corresponding manual review while helping to protect your organization's reputation.

FraudIQ Authenticate offers a far-reaching and comprehensive solution to verify and authenticate individuals using consistent and objective score-driven policies that incorporate multiple data assets including credit history data, demographics and more. You can feel more confident that the user's "claimed identity" is correct — they are who they say they are — and that the information presented to support the application is authentic and belongs to that user.

Equifax expertise is derived from more than a hundred years in business and from managing more than 800 million consumer identities and more than 88 million businesses worldwide. We have unmatched insight gained through the implementation of identity proofing and fraud prevention systems for government agencies and some of the world's largest financial institutions and other businesses.

FraudIQ Authenticate is comprised of the following:

- A risk-based authentication platform
- Device - Device authentication and identity check for fraudulent use
- Passcode - Two-factor authentication with one time use passcodes
- Questions - Knowledge-based authentication questions

EQUIFAX®

Risk-Based Authentication

A risk-based authentication process unobtrusively verifies the identity of the consumer to help guard against fraud without interjecting unnecessary additional steps. This kind of layered security analyzes and detects behavior patterns and other fraud indicators across multiple institutions and industries.

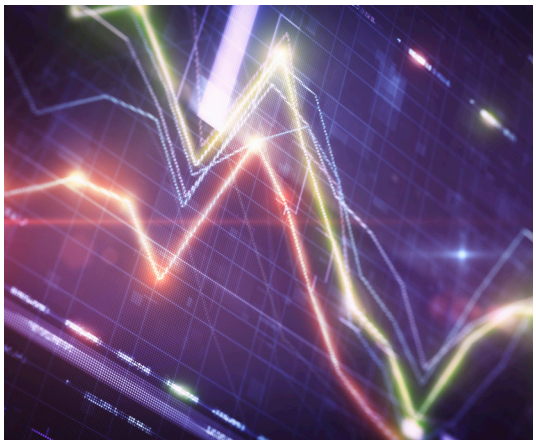
The first step is to verify the consumer's identity. Identity verification is usually done through a check of official records or through verification of financial account information. The historical challenge to remote identification has been to verify and authenticate individuals who have limited financial backgrounds primarily due to the fact that the data needed is unavailable in traditional sources. FraudIQ Authenticate leverages our proprietary utility and telecommunications data and many other proprietary and unique data resources along with credit history to help find and identify those applicants.

Equifax's unique datasets, analytics and proprietary matching logic, combined with our in-house risk and fraud expertise, provide important insights into application activity that is not available anywhere else. Our solutions detect potentially fraudulent activity in real time, providing early warnings that cost-effectively isolate high risk applications without negatively impacting the overall customer experience. The patented interactive session binds the applicant to the identity information entered and leverages an analytical model that provides a fraud risk score as part of the overall assessment.

- Monitors identities across dozens of industries, thousands of institutions, and billions of identity and credit events to find suspicious activity that any single institution couldn't see on their own
- Returns real-time views into velocity and behavioral patterns that look at identity events in time frames as small as seconds
- Uses proprietary keying technology to effectively validate the components of an individual's identity — driving down false positive rates
- Includes differentiated data, including demographic marketing data, employment data and utilities and telecommunications account data, that improve the coverage of population not found in the credit file

Stepped-up authentication applied only where there is a high potential for fraud — saving frustration for the consumer and expense for the business.

Detect patterns across institutions and industries that are indicative of fraudulent activity in real time.



KEY FEATURES AND BENEFITS

Reduce fraud through identity authentication

Minimize manual processing time and costs

Reduce website abandonment rate by providing a frictionless customer experience

Incorporate into your business processes based on security or fraud mitigation needs

Isolate high-risk applications without negatively impacting the applicant's experience

Improve compliance with USA Patriot Act and FFIEC authentication guidelines

Device

Verify the reputation of the device used to access your systems — in combination with applicant identity proofing or as a standalone capability. This helps to determine if the applicant has a fraudulent purpose. Information about where a device really is and whether it is associated with other devices used in known fraud helps passively identify known and potential fraud before an applicant has access to your systems and private data. This capability can be used upon initial login as reputation authentication or for returning users as a "remember me" function.

Passcode

When concerned about potential fraud or a high-risk transaction, offer a stepped-up level of two-factor authentication by providing an expiring 6-digit passcode via SMS at account opening or online credentialing. Verifying the mobile phone number against service provider records helps confirm that the device is associated with the applicant.

Questions

When positive identity confirmation is required, knowledge based authentication confirms an applicant's identity by presenting multiple-choice questions that should only be known by that actual person. The dynamically-generated questions are based on credit file information and other non-credit proprietary and non-public data.