Progressive authentication integrated into Equifax Identity Proofing

Our patented identity verification and proofing platform empowers companies to enable easy, secure access to information by trusted parties. Our customers seek to minimize the costs of authentication and identity proofing, while maximizing the likelihood that an individual is who they claim to be, to protect online enrollment and registration, lost or forgotten credential recovery, and high risk transactions.

Our solutions offer touch-free identity proofing that queries credit and non-credit data sources to confirm identity with basic biographical information and challenges users with “out-of-pocket” questions. The identity proofing questions and answers are developed from a wide variety of private data stores to maximize the ability to uniquely identify an individual and to prevent fraud.

Identify devices as well as individuals

Equifax identity proofing can also 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.

- Data on nearly 1 billion devices used to access online services across several industries worldwide.
- Real-time fraud prevention at registration, login, and other transactions.
- Protection for every internet-connected device including PC, tablet, or mobile device.
- Passive detection that works within your existing workflow without affecting the user experience.

Incorporate real-time behavioral pattern and velocity detection

Equifax’s unique dataset, 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 patterns across institutions and industries that are indicative of fraudulent activity in real time, providing early fraud detection that cost-effectively isolates high risk applications without negatively impacting the applicant’s experience.

- 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 our proprietary keying technology to effectively validate the components of an individual’s identity - thereby driving down false positive rates.

Progressive Authentication

A comprehensive set of authentication methods in a single, integrated platform.

In an evolving threat landscape, multiple authentication methods provide improved risk and fraud mitigation – switch high risk transactions from one authentication method to another to maintain business continuity.
Improved online service and protection for your sensitive data

The need for organizations to share information among diverse groups of internal and external users has accelerated the move to online, real-time applications and cloud-based computing. With more remote users, more incidents of data breaches, and more demands for data access, IT executives seek stronger methods to verify the identities of those requesting access to sensitive data.

Progressive authentication is our term for a best practice we pioneered—using an integrated set of tools and processes for situation-based authentication of users seeking access to enterprise networks, data, and applications. Progressive authentication delivers secure one-time passcodes via tokens, email, biometrics, and SMS/IVR to end-user owned devices. Multiple authentication vectors ensure high-level security with user-required flexibility and usability.

How Equifax supports your move to progressive authentication

Our multifactor authentication offering, Anakam.TFA® Two Factor Authentication, offers a range of authentication methods in a single integrated platform. It leverages a host of existing devices or readily available technologies, including cell phones, voice biometrics, and email, to enable flexible multifactor authentication.

Out-of-band delivery of quickly expiring, one-time passcodes confirms that the person possessing the passcode is the one attempting to access your systems. To gain access, the user must then enter the one-time passcode on the login screen. SMS message: An SMS message sends the one-time code to a user’s mobile phone.

Interactive Voice Recording: The one-time passcode is sent via automated voice call to a user’s landline or mobile phone.

Voice biometrics: Unlike other biometric authentication tools, voice biometric systems do not require specialized hardware. The user only needs access to a mobile or landline telephone.

Hard & Soft token: Hard or soft tokens are effective alternatives to compromised hard token methodologies.

VPN-ready: Facilitate your implementation of progressive authentication by seamlessly integrating with the VPN solutions that already exist in your infrastructure. Using your VPN with two-factor authentication allows you to give remote offices, teleworkers, and partners access to critical applications, internal corporate networks, and sensitive data.

For tough security, answer the tough questions

With progressive authentication, you have complete control over how your organization deals with every new registration request and every user log-in. Finally, you’ll have a single platform to answer—dynamically and cost effectively—the tough questions that keep enterprise data security managers up at night.

Adjust authentication levels to fit real-time needs

Progressive authentication is the best way to operationally exploit multifactor authentication. Think of it as a dial, like a volume knob, to increase or decrease authentication measures according to the situation at hand.

For some low-risk, high-volume applications, single-factor authentication is sufficient. When sensitive data like financial information or healthcare records is involved, organizations need stricter security measures at registration and login—calling for a second authentication factor.

• Dynamically adjust authentication levels based on user roles, risk levels, threat reports, budgets and transaction types.
• Dial challenge severity levels up or down according to login locations, login frequency, end-users’ ISP changes, machine characteristics, or other criteria.
• Challenge suspicious transactions, policy violations, or out-of-norm behavior, not just at log-in.
• Introduce secure, takeless authentication for consumers, employees, or partners in any order and at differing security levels.

Key benefits

> Full compliance with NIST Level 3 requirement for strong two factor authentication, DEA Electronic Prescribing (EPCS), and PCI DSS guidelines
> Scalable to tens of millions of users for e-government and e-commerce solutions
> Tailored to enterprise use cases and business needs—invoke at any time within your workflow
> Implement inside your firewall on physical or virtual servers or in a cloud environment
> Dynamically adapts to risk levels, transaction types, user types and more

For tough security, answer the tough questions

With progressive authentication, you have complete control over how your organization deals with every new registration request and every user log-in. Finally, you’ll have a single platform to answer—dynamically and cost effectively—the tough questions that keep enterprise data security managers up at night.

“Dial” security measures up or down based on risk and other factors you define

• Who is this person claiming to be a trusted user?
• Does the user have a legitimate need to access this particular information or network?
• Are there any obvious “red flags” or abnormal indicators suggesting that this request merits more stringent attention?
• What authentication measures are most appropriate now for allowing or denying this user’s request?
• What channels, or vectors, should the organization use to securely deliver one-time passcodes to approved users?
Improved online service and protection for your sensitive data

The need for organizations to share information among diverse groups of internal and external users has accelerated the move to online, real-time applications and cloud-based computing. With more remote users, more incidents of data breaches, and more demands for data access, IT executives seek stronger methods to verify the identities of those requesting access to sensitive data.

Progressive authentication is our term for a best practice we pioneered—using an integrated set of tools and processes for situation-based authentication of users seeking access to enterprise networks, data, and applications.

Progressive authentication delivers secure one-time passcodes via tokens, email, biometrics, and SMS/IVR to end-user owned devices. Multiple authentication vectors ensure high-level security with user-required flexibility and usability.

Key benefits

- **Full compliance** with NIST Level 3 requirement for strong two factor authentication, DEA Electronic Prescribing (EPCS), and PCI DSS guidelines
- **Scalable** to tens of millions of users for e-government and e-commerce solutions
- **Tailored to enterprise use cases and business needs**—invoke at any time within your workflow
- **Implement inside your firewall** on physical or virtual servers or in a cloud environment
- **Dynamically adapts** to risk levels, transaction types, user types and more

How Equifax supports your move to progressive authentication

Our multifactor authentication offering, Anakam.TFA Two Factor Authentication, offers a range of authentication methods in a single integrated platform. It leverages a host of existing devices or readily available technologies, including cell phones, voice biometrics, and email, to enable flexible multifactor authentication.

Out-of-band delivery of quickly expiring, one-time passcodes confirms that the person possessing the passcode is the one attempting to access your systems. To gain access, the user must then enter the one-time passcode on the login screen.

SMS message: An SMS message sends the one-time code to a user’s mobile phone.

Interactive Voice Recording: The one-time passcode is sent via automated voice call to a user’s landline or mobile phone.

Voice biometrics: Unlike other biometric authentication tools, voice biometric systems do not require specialized hardware. The user only needs access to a mobile or landline telephone.

Hand & Soft tokens: Hard or soft tokens are effective alternatives to compromised hardware.

Dial challenge severity levels up or down according to login screen.

Introduce secure, tokenless authentication for consumers, employees, or partners in any order and at differing security levels.

Progressive authentication

Progressive authentication is the best way to operationally exploit multifactor authentication. Think of it as a dial, like a volume knob, to increase or decrease authentication measures according to the situation at hand.

For some low-risk, high-volume applications, single-factor authentication is sufficient. When sensitive data like financial information or healthcare records is involved, organizations need stricter security measures at registration and login—calling for a second authentication factor.

- Dynamically adjust authentication levels based on user roles, risk levels, threat reports, budgets and transaction types.
- Dial challenge severity levels up or down according to login locations, login frequency, end-users’ ISP changes, machine characteristics, or other criteria.
- Challenge suspicious transactions, policy violations, or out-of-norm behavior, not just at log-in.
- Introduce secure, tokenless authentication for consumers, employees, or partners in any order and at differing security levels.

For tough security, answer the tough questions

With progressive authentication, you have complete control over how your organization deals with every new registration request and every user log-in. Finally, you’ll have a single platform to answer—dynamically and cost effectively—the tough questions that keep enterprise data security managers up at night.

- Who is this person claiming to be a trusted user?
- Does the user have a legitimate need to access this particular information or network?
- Are there any obvious “red flags” or abnormal indicators suggesting that this request merits more stringent attention?
- What authentication measures are most appropriate now for allowing or denying this user’s request?
- What channels, or vectors, should the organization use to securely deliver one-time passcodes to approved users?

Adjust authentication levels to fit real-time needs

Progressive authentication is the best way to operationally exploit multifactor authentication. Think of it as a dial, like a volume knob, to increase or decrease authentication measures according to the situation at hand.

For some low-risk, high-volume applications, single-factor authentication is sufficient. When sensitive data like financial information or healthcare records is involved, organizations need stricter security measures at registration and login—calling for a second authentication factor.

- Dynamically adjust authentication levels based on user roles, risk levels, threat reports, budgets and transaction types.
- Dial challenge severity levels up or down according to login locations, login frequency, end-users’ ISP changes, machine characteristics, or other criteria.
- Challenge suspicious transactions, policy violations, or out-of-norm behavior, not just at log-in.
- Introduce secure, tokenless authentication for consumers, employees, or partners in any order and at differing security levels.
Progressive authentication integrated into Equifax Identity Proofing

Our patented identity verification and proofing platform empowers companies to enable easy, secure access to information by trusted parties. Our customers seek to minimize the costs of authentication and identity proofing, while maximizing the likelihood that an individual is who they claim to be, to protect online enrollment and registration, lost or forgotten credential recovery, and high risk transactions.

Our solutions offer touch-free identity proofing that queries credit and non-credit data sources to confirm identity with basic biographical information and challenges users with “out-of-wallet” questions. The identity proofing questions and answers are developed from a wide variety of private data sources to maximize the ability to uniquely identify an individual and to prevent fraud.

Identify devices as well as individuals

Equifax identity proofing can also 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.

• Data on nearly 1 billion devices used to access online services across several industries worldwide.

Progressively authenticate users based on their roles or transactions:

- Real-time fraud prevention at registration, login, and other transactions.
- Protection for every internet-connected device including PC, tablet, or mobile device.
- Passive detection that works within your existing workflow without affecting the user experience.

Incorporate real-time behavioral pattern and velocity detection

Equifax's unique dataset, 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 patterns across institutions and industries that are indicative of fraudulent activity in real time, providing early fraud detection that cost-effectively isolates high risk applications without negatively impacting the applicant's experience.

• 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 our proprietary keying technology to effectively validate the components of an individual’s identity - thereby driving down false positive rates.

Progressive Authentication

A comprehensive set of authentication methods in a single, integrated platform.

In an evolving threat landscape, multiple authentication methods provide improved risk and fraud mitigation – switch high risk transactions from one authentication method to another to maintain business continuity.