Product sheet

Multifactor authentication services

Verify a consumer's identity during remote transactions

With the advent of newer and more adaptable communication technologies, remote transactions continue to increase. There is a need for more efficient ways to secure these transactions and prove the identity of an individual on the other end of a remote channel.

Multifactor authentication uses a combination of elements to verify a consumer's identity. It's based on the premise that an unauthorized person is unlikely to be able to supply the same proof elements as the true consumer to prove his or her identity. If one of the required components in an authentication transaction is missing or supplied incorrectly, the consumer's identity is not established with sufficient certainty to allow the requested transaction to proceed. This prevents potential fraud.

Two or more of the following credentials are used in multifactor authentication:

- **What the user knows —** Password, PIN, unique information.
- **What the user has —** Mobile phone, bankcard, token.
- **Who the user is —** Biometric verification such as fingerprint, eye iris, voice, typing speed.

Our multifactor authentication service uses a one-time password (what the user knows) delivered to the consumer's mobile phone or landline (what the user has) via a verified phone number. Through the one-time password (OTP) authentication process, businesses and government agencies can strengthen their authentication process in high-risk transactions, adhere to regulations or secure high-value consumer transactions quickly — with little to no additional impact on the consumer.

Our OTP offers organizations the option of having us create a unique alphanumeric code generated for each authentication transaction or providing us with a unique code delivered to a verified consumer phone via text or voicemail.

- How long has the consumer had the phone number?
- Is the number being forwarded?
- Is the number assigned to a prepaid phone?
- Has the number been ported?

Beyond message delivery

In addition to delivering a generic or customized alphanumeric password to the verified phone, Experian® provides other capabilities in our OTP offering:

- **Verification of phone to consumer —** Before attempting an OTP send, we independently verify that the phone number provided by the consumer can be linked to that consumer.
- **Phone attributes verification —** We validate other phone attributes, such as porting, forwarding, account tenure and contract type.
- **OTP included in final verification results —** Because our OTP service verifies consumer information, we can include the verification in the result delivered as part of the transaction.

- **Autodefault to additional authentication tools —** If the OTP fails, other Experian authentication tools can be triggered to continue consumer verification remotely. This avoids costly exception processing, which could require in-person interaction.

Using an OTP service strengthens the security of remote transactions. But on its own, it's still vulnerable to fraudulent attacks. Organizations must deploy a multifaceted risk strategy to provide the highest level of identity verification in remote transactions.

Building a comprehensive risk authentication strategy

Mobile phones are susceptible to malware attacks, phone numbers can be stolen and re-registered in less than 24 hours, messages can be forwarded or intercepted by fraudsters without the legitimate consumer's knowledge. These are just a few of the vulnerabilities inherent in relying on an OTP alone for authentication. To be most effective, the OTP should be bundled with an overall risk authentication strategy that considers many elements in determining the identity of the consumer attempting a remote transaction.

In addition to our OTP offering, we provide a comprehensive suite of services that can be customized to build a far-reaching, adaptable fraud mitigation strategy to meet an individual organization's unique needs while still giving consumers a low-friction experience. Using a combination of an OTP, identity scoring, device proofing and other services, organizations can create a comprehensive risk strategy. By leveraging the strength of multiple identity verification tools in various combinations, organizations can achieve the highest level of confidence in the remote consumer's identity.

Experian's authentication services

- Identity scoring.
- Theft risk scoring and monitoring.
- Knowledge IQ^{SM} (out-of-wallet questions).
- One-time password.
- Device attribute verification.
- Document verification.
- Foreign identity proofing.
- Synthetic identity detection.

Our combination of expert consulting and a variety of authentication services allows organizations to build and adapt a fraud risk mitigation strategy that will adjust not only to meet the organization's changing needs, but also to simultaneously combat emerging fraud schemes as they develop.

About Experian Decision Analytics

Decision Analytics helps agencies make better, more insightful decisions and ensure that the largest number of legitimate consumers receive benefits and services. Clients use Decision Analytics' data intelligence, analytics, technology and consulting expertise to expand consumer relationships; manage and mitigate risk; prevent, detect and reduce fraud; meet regulatory obligations; and gain operational efficiencies. Decision Analytics provides the intelligence used by government agencies and leading businesses worldwide to confidently assess the potential risks and rewards of critical business decisions.

To find out more about multifactor authentication services, contact your local Experian sales representative or call 1 888 414 1120.

Experian
475 Anton Blvd.
Costa Mesa, CA 92626
T: 1 888 414 1120
www.experian.com