

Understand identity and prevent fraud while optimizing the user experience

Modern and simple identity verification is key.

It's now harder than ever to prove who you are, especially with the rise of fraud and the move to digital platforms. Documents that prove your identity can be forged, and more and more situations require verifying identities—opening a bank account, accessing medical records, and enrolling in college—making it crucial to protect our identity. How do you combat fraud by making sure people are who they say they are? The solution is to validate, then verify.

Benefits of Okta + LexisNexis® Risk Solutions

Risk-based: Security options and decisioning to support a risk-based authentication approach.

Scalable: Easily supports growth in user base and adoption.

Choice: Authentication technique versatility to minimize user friction.

Identity Binding: Improved user identification that works with authentication methods.

Reporting and Administration: Online self-service options for ease of administration and ability to audit.

Verify identities continuously

The first step is validation through strong identity verification, which helps prevent the creation of fake accounts. During the registration or application process, identity proofing prompts individuals for information that only they'd know—and doesn't rely on easy-to-find data. It asks questions like, "What was your approximate mortgage payment in 2002?" The right individual will know, but fraudsters will be forced to guess.

The next step is continuous validation to prevent bad actors from accessing services and systems. You already know that passwords aren't enough. Multi-factor authentication is stronger than a single password, but we can make it even stronger. This is where identity verification comes in, ensuring a person is who they say they are.

With Okta + LexisNexis Risk Solutions, organizations can better prevent, detect, and investigate fraud while keeping the experience frictionless by:



Leveraging outside, comprehensive data on users for identity verification



Managing identities and access from the cloud, freeing your workforce to focus on better user services



Protecting user identities with powerful yet simple multi-factor authentication

One identity platform for all

The Okta Identity Cloud is a modern platform built on open standards and integrates with all types of applications, on-premises or in the cloud. It's a powerful digital hub for secure identity management and authentication. Better yet, it has the automation and auditing features that today's IT teams need. Organizations of all sizes use Okta to secure and manage access to their applications, internal or external, effortlessly.

Okta's Adaptive Multi-Factor Authentication (AMFA) uses risk-based analysis to align with their organization's approach to risk management. The authentication approach is customizable with options such as SMS, push, and voice.

Okta provides further protection by identifying potentially malicious IP addresses and blocking threats to prevent user lockouts.



Machine learning and statistical models detect when your organization is under attack from bots



Suspicious IP requests, such as those from password spraying and phishing, are blocked aggressively until the threat subsides



Protection from credential stuffing, botnets, and brute force and DDoS attacks

Digital identity verification that learns over time

LexisNexis Risk Solutions leverages insights from billions of data assets to digitally determine whether the user logging into a system is authentic. LexID matches records of users as they move through life and change over time, giving a complete and precise picture of a person rather than a single snapshot. This system automatically searches and accounts for potentially mismatched records from marriage, changes in name usage, juniors/seniors, moves, and more. It also resolves these records to a single identity, including all the information from multiple records. All of which make identification simpler in the future.

LexisNexis Risk Solutions uses a multi-layered security approach with four lines of defense:



Looks for risk factors such as device ID behavior and attributes, geo-location including VPNs, proxies, and malware bots



Handles document authentication, assigns identity attributes and scores, and tracks identity anomalies



Assigns a fraud score and reason codes, tracks speed and frequency of attacks, and tracks patterns in attacks to look for correlations



Successfully manages knowledge-based authentication, biometrics, and one-time passwords

A complete and powerful solution to secure account creation

Okta's Multi-Factor Authentication, combined with LexisNexis Risk Solutions Identity Verification, delivers a seamless, innovative solution that helps organizations validate and verify identities to provide a seamless and secure experience. LexisNexis Risk Solutions authenticates identities in near real-time, leveraging the power of billions of data records. With the addition of Okta's authentication options, organizations can analyze user behavior from interactions across other devices, platforms, and industries across the globe. Protection can then be extended to include account takeover, identity theft detection, and synthetic identity account registration detection.

Benefits of future proofing your authentication capabilities:



Matches the authentication experience to the risk of a transaction



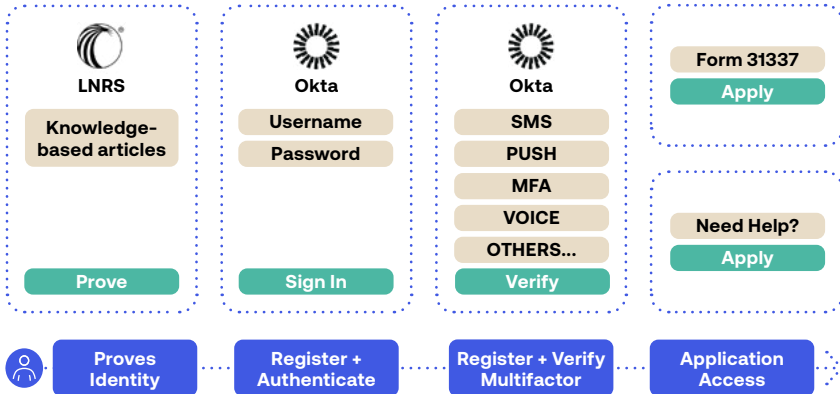
Reduce authentication times and friction to provide a superior experience



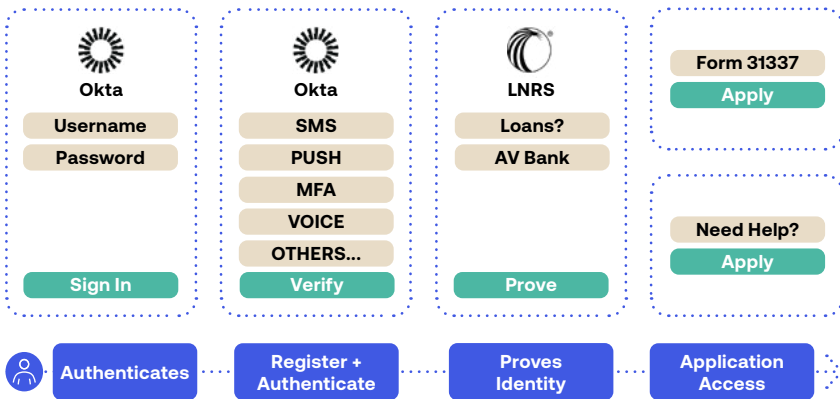
Fortified protection against cybersecurity attacks and online fraud with adaptive authentication and identity verification

Integration Use Cases

Use Case 1: Account Registration



Use Case 2: Login



Customer Story: Kansas Department of Labor prevents fraudulent claims

During the COVID-19 pandemic, the Kansas Department of Labor (KDOL) saw a rapid increase in claims for unemployment and federal pandemic programs, resulting in a record amount of fraud. In an effort to secure its systems, KDOL acted quickly to modernize and strengthen its architecture by assembling a team of IT experts and vendors, including Okta and LexisNexis.

KDOL deployed Okta MFA for an extra authentication layer to protect the department and customer identities, leveraged Okta ThreatInsight to thwart bot attacks and prevent fraudsters from entering the system, and LexisNexis to verify identities.

Using the two solutions, KDOL has stopped over 7.68 million bots and fraudulent login attempts. Read more [here](#).



For more information on this integration, visit okta.com/partners/lexisnexis-risk-solutions.
 If you have more questions, please contact our sales team at okta.com/contact-sales.

About Okta

Okta is the leading independent identity provider. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. We provide simple and secure access to people and organizations everywhere, giving them the confidence to reach their full potential. To learn more, visit okta.com