White Paper

Evaluating Identity Proofing: Three Core Capabilities Your Solution Should Possess

A perfect match makes for better business.

LexisNexis®

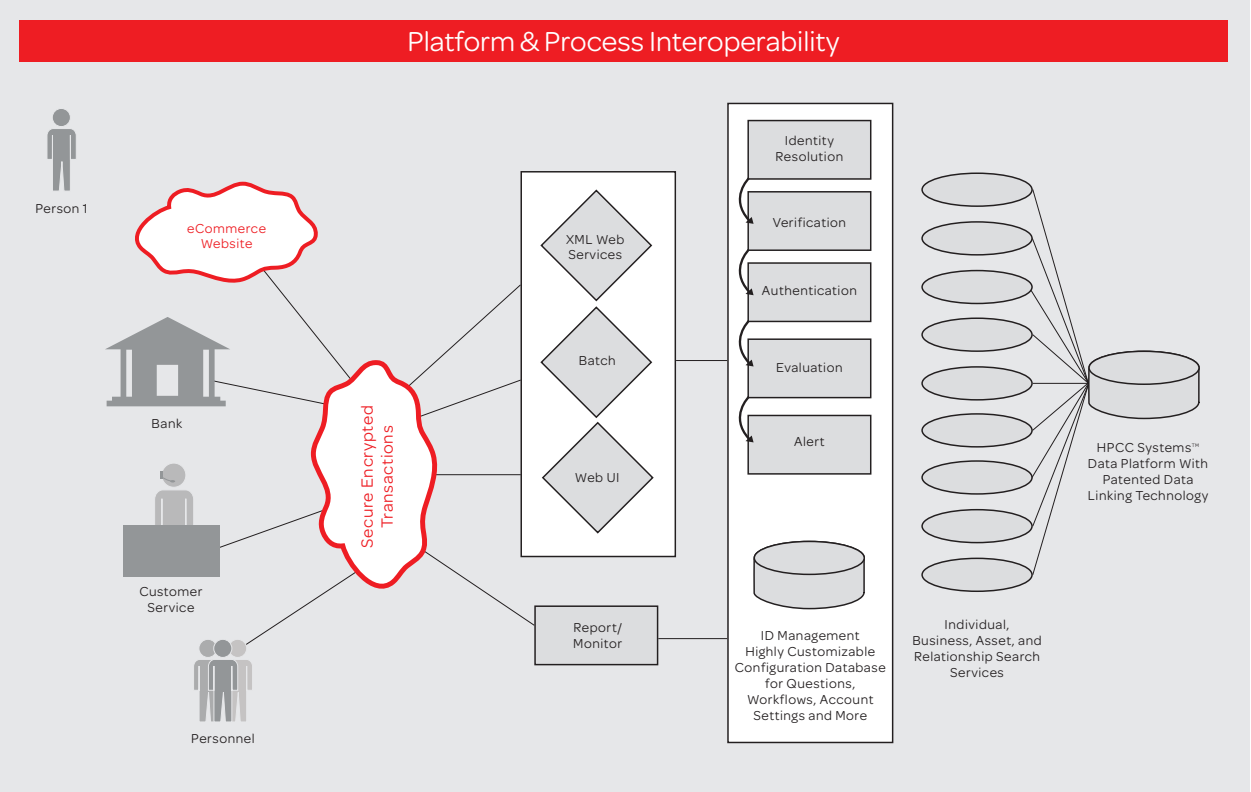
Risk Solutions
Identity Management

With an ever-growing array of products, point solutions, end-user devices and technologies like biometrics and open identity platforms, choosing an identity proofing solution can be a challenge. The solution must provide reliable identity verification and authentication; variable risk assurance through the real-time detection of fraud and other high-risk conditions; and compliance for regulations governing identity verification and authentication, as well as data access and use.

Identity Proofing as a Business Enabler: Key Considerations

Before your solution can address these needs, it must meet not only your technical requirements but also your unique business processes and objectives. Whether implementing an end-to-end solution or a standalone service, customization is key. Your solution should be configurable to your specific policies, workflows, channels and operating systems, with scalability and flexibility to meet changing needs across the enterprise. To further increase efficiencies and decrease cost and risk, look for solutions that offer:

- Seamless integration across multiple platforms, from tiered web services to XML over HTTPS
- Emerging open platform architectures, such as OpenID Exchange
- A service-based architecture with flexible access options
- Batching capabilities
- Standards-based access to information systems and data for regulatory compliance
- Role-based access management with a consolidated reporting framework for easy auditing
- Dedicated account management to ensure you get the most out of the solution



In addition to platform and process interoperability, there are three key capabilities to look for in best-in-class identity proofing solutions:

Core Capability #1: Resolve

Why: To correct and limit data inaccuracies for reliable, real-time identity proofing.

Identity resolution is the first step of identity proofing, providing real-time, standards-based access to multiple data sources to confirm whether an identity exists. It should also provide simultaneous, multiple search functionality and powerful data linking technology to filter and connect data into actionable intelligence. In addition, it should alert you to possible errors or red flags, such as a transposed Social Security number, while attempting to provide correct returned information to resolve the identity with minimum data input and maximum accuracy.

What You Should Look For:

- **Housed Data** – For faster, more secure identity proofing, look for solutions that store data in-house. This affords more control over the quality, security and availability of the information, ensuring fewer points of failure so the data is there when you need it.
- **Vast, Diverse Databases** – Effective solutions can access multiple datacenters to compile vast sources of diverse public and proprietary information to proof an identity.
- **Alternative Data Sources** – Using non-credit header information provides identity resolution for consumers with limited information, such as young adults and recent immigrants.
- **Data Linking Technology** - Look for built-in processing logic and sophisticated matching technology to perform simultaneous searches, confirming identity while also identifying suspicious patterns and errors.
- **Data Normalization and Fusing** – This important function resolves data anomalies, eliminates redundancies and fuses data to improve consistency, cohesion and efficiency.

Core Capability #2: Verify

Why: To quantify risk, improve decision making and support regulatory compliance.

Identity verification solutions should leverage millions of public and proprietary data points to return detailed search results to the user's desktop in milliseconds. The technology should also offer one-to-one and one-to-many matching capabilities. This means it should be able to identify and link disparate pieces of data around a single identity—confirming the data is valid, that the attributes belong together, and whether they are associated with multiple identities. In addition, the solution should provide configurable scoring and risk indicators that return results based on your business rules, such as whether an error results in an immediate "fail" score or prompts additional steps.

What You Should Look For:

- **Configurable, Rules-Based Scoring** – Solutions should provide a range of "pass/fail" and index scoring models you can configure to meet varying internal policy, process and risk assurance requirements.
- **Risk Indicators** – The technology should provide risk indicators explaining possible errors or red flags, customizable to address conditions such as risk tolerance and specific transaction.
- **Compliance** – All confidential data should be encrypted with a minimum 128-bit encryption algorithm and comply with federal and industry security standards, from the Patriot Act & ISO 27002 to AICPA/CICA and your organization's unique security controls.
- **Flexible Deployment** – Via a web application, a web services interface or embedded into an existing application as part of a configurable identity proofing workflow, your solution should give you flexible access options to match your specific business needs.

LexisNexis® Advanced Data Linking Technology

Via its high-performance computing cluster and proprietary ECL declarative programming language, which makes analyzing large data sets easier, more accurate and efficient, the patented data linking technology from LexisNexis® can refine, link and fuse data from 10,000 disparate sources to resolve identities with 99.9% precision—instantly providing:

- Anomaly Detection – data verification and "cleansing" to discover data despite misspellings, transposition and other errors
- Streamlining – eliminates duplicate public records
- Relevancy – results displayed based on relevancy of results to original search terms
- Cross-Referencing – instantly and simultaneously links billions of names, addresses, phone numbers and "out-of-wallet" data points with appropriate people, businesses and locations

Core Capability #3: Authenticate

Why: To increase assurance, improve the customer experience and meet multiple business objectives.

The final capability of an effective, holistic identity proofing solution is strong knowledge-based authentication, which is integral to striking a balance between protecting your business and serving your customers. Look for solutions that scour multiple "out-of-wallet" data sources, such as former residence and telephone history, in addition to your business's unique data to generate targeted and non-intrusive challenge questions in real-time. The solution's quiz engine should be adjustable to meet the level of assurance required for specific transactions, allowing the user to select from a series of checks based on the user's business rules and channels.

In what county do you currently live?	What model car was registered to you in 1997?	In which of the following cities have you NEVER lived or used in your address?
○ Houston	◉ Honda Civic	○ Louisville
○ Forsyth	○ Ford Taurus	○ Hermitage
◉ Douglas	○ Toyota Camry	◉ New Hope
○ None of the Above	○ Nissan Sentra	○ McCordsville
		○ All of the Above

The LexisNexis® Advantage

- Data coverage/linkages enabling consistent verification and authentication across diverse populations
- Multiple data centers to ensure redundancy with failover capacity so data is available 24/7
- Compliance assurance: OFAC, Patriot Act, FACT Act and other regulatory requirements
- Flexible, scalable solutions to meet specific business and technical requirements
- Multi-channel solutions operating across consumer contact points
- Holistic approach, including pre- and post-implementation support services, for an effective identity management solution across the business and customer lifecycle

What You Should Look For:

- **Flexible Quiz Engine Capability** – Your solution should offer intelligent quiz engine capabilities to address changing conditions such data availability and question relevancy. It should also be able to determine in real-time the number of questions required to fulfill assurance requirements for a specific transaction or individual.
- **Robust Quiz Template Library** – Effective solutions provide deep and wide data repositories for the best possible quiz generation rate. Your solution should have the ability to leverage customer-supplied data, as well as your organization's existing data sets to create a library that will help you quickly authenticate your customers, while creating as little customer "friction" as possible.
- **Configurable Security Settings** – Look for solutions that provide customizable security features for challenge quizzes, with configurable settings such as how many times a question can appear, the number of incorrect answers that prompt a "fail" score or how long the system waits until a time out.
- **Non-SSN/FEIN Identifiers** – To protect your customers' privacy and comply with regulations governing the use of personally identifiable information, your solution should give users the option to enter an alternate unique identifier in place of a Social Security number or Federal Employer Identification Number for non-intrusive authentication.

Conclusion

As technologies continue to drive change in digital identity proofing, it is critical to implement a reliable, customizable and scalable enterprise identity proofing solution that not only meets your technical requirements but also supports your business processes and objectives. Best-in-class solutions like those from LexisNexis® offer this holistic approach—combining industry-leading technology and standards-based data access with customized support services that enable businesses to increase efficiencies, decrease risk, lower costs, achieve compliance and meet multiple business objectives. To learn more, visit http://idmanagement.lexisnexis.com