White Paper

Identity Proofing: The need to go beyond just credit data for positive identification

Millions of people don't have credit and millions of credit identity records are stolen each year; how can you accurately identify who is knocking at your digital front door?

June 2015

LexisNexis®

Risk Solutions
Government

Accessing Government Services: Easy and efficient... or exasperating?

There's no question that "logging on" is preferable to lining up at a government office to receive services. This convenience can backfire unless the identity proofing solution is comprehensive in its sources to positively identify all your clients including the "unbanked" or "thin" credit file portion of the population, which represent more than 100 million Americans. But convenience aside, there are other drawbacks to digital connectivity; mainly making it easier for fraudsters to defraud the government.

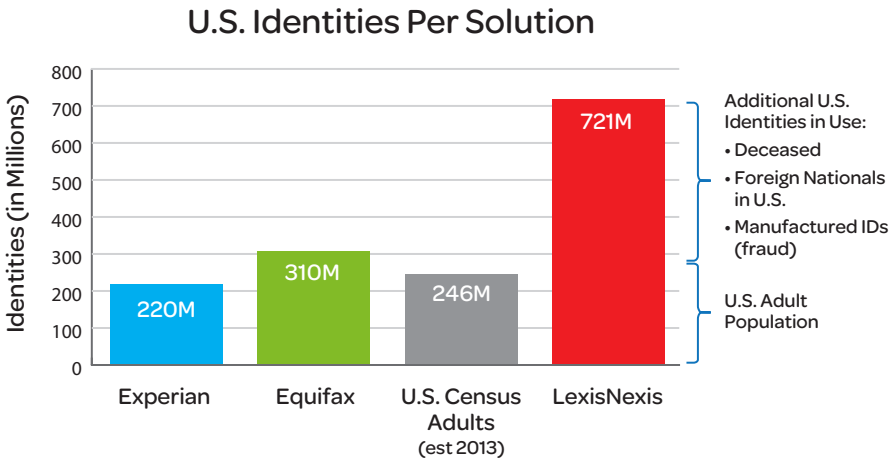
- **Identity theft is the fastest-growing crime in the U.S.** The fact that there are 30 billion connected devices in use today—from desktop computers to laptops to smartphones and tablets—increases the potential for information to get into the wrong hands. Devices may be lost or stolen; apps may be infected with malware. Not only that, 600 million people are posting personal information on Facebook and other social networking sites—details like birth dates and pets' names—making it easier for smart hackers to piece together identifying data for account takeover.
- **Investigating fraud takes time, money and resources.** Aren't your resources spread too thin as it is? While many government agencies have successfully recovered millions of dollars in improper payments, it takes a significant amount of manpower and technology investment to do it—expenditures that many governments have had to forgo in these leaner times. For instance, the State of California Health and Human Services Agency experienced a 33 percent reduction in Special Investigation Unit staffing between 2005 and 2010 due to cutbacks, while fraud continued to grow at an alarming rate.
- **Citizens can be skeptical.** A survey conducted in Nassau County, New York, revealed that individuals were leery of government websites that collected personal information, associating it with "Big Brother" and invasion of privacy. As a result of this insight, government agencies serving the area declined to use robust identity proofing when the recipient applied for or accessed government services online—a decision that contributed to fraudulent account holders and claims.
- On the other hand, citizens were quite accustomed to using personal information in the private sector for tasks like online banking. **What's the difference?** Having a non-governmental, third-party entity handling this data management implies, at least in the minds of citizens, that the data is secure and won't be used for purposes other than the intended transactions.
- **From an IT perspective, managing external interactions can be a nightmare.** Identity proofing in a closed internal network environment is one thing; you know quite a bit about the users, most of whom have likely gone through some type of background screening process before case workers determine if the citizen is eligible for

The issue with positively identifying the "unbanked" or "under-banked" population is that they do not show up on the credit rating agencies radar, thus requiring a source that goes beyond just credit data for identity proofing.

benefits. But managing electronic interactions across public and private networks with millions of people you don't know is an extremely complicated endeavor. Moreover, as pointed out above, efforts to implement rigid controls can turn citizens away from your site.

The Public Record and Advanced Data Linking Advantage

The LexisNexis® public record database contains over 720 million unique identities, which is amassed by over 10,000 unique sources, including three of the major credit bureaus. Studies conducted on this aggregated data acquired from these three sources indicate a 7% lift within the U.S. population, compared to a single bureau source. Credit bureau data is typically regional in nature with one bureau being strong in the Southeast, another being strong in the Midwest and the third being strong in the West. Public Record databases cover the entire country, including the populous Northeast and the underbanked and unbanked populations as a whole. This additional coverage is important because it allows government agencies to identify more fraud and reduce false positives, which will make their program more robust and improve the ROI.



(Source: US Census, Experian Website, Equifax White Paper, LexisNexis Internal Data)

Public record databases contain many of the 60 million unbanked and underbanked populations typically not captured in credit bureau data. At LexisNexis, our public records database is backed by LexID®, our patented linking technology, which helps identify and flag "identities" that may have been used in fraudulent transactions. These fraudulent, or synthetic identities, are often the result of many of the data breaches that have occurred in the last several years. Criminals use various combinations of identity elements that contain real names, real addresses, real social security numbers (SSNs), real dates of birth (DOBs), real employment data and real income data to create synthetic identities that appear to be real on the surface. However, public records databases, through their breadth of historically aggregated identities, can recognize a synthetic identity when it is presented to a government agency when requesting access to a system, or attempting to enroll in a program remotely. LexisNexis can do this because the combination of stolen identity elements have never been seen together in our identity database. As a result, our analytics can very quickly verify the stolen identity elements belonging to another person. The benefit of using public records is twofold: it will allow government agencies to quickly identify scenarios where criminals are posing as someone else to request a refund and stop the payment and also prevent the actual citizen and agency from spending months of time to resolve an identity theft case.

LexisNexis sustains its position as a leader in identity analytics as a result of maintaining approximately 1/3 of the U.S. adult population within our database. A good number of these identities are typically not contained within credit bureau databases. To help address this challenge of the unbanked, the Fair Isaac Corporation (FICO) and LexisNexis entered into an agreement with one of the major credit bureaus to develop "a new credit scoring model for the millions of people with weak or no credit histories who are now considered "unscorable"[1].

The LexisNexis public record database includes identities of individuals who do not use credit, such as:

- the wealthy because they do not need to use credit to purchase goods and services,
- the poor because they cannot obtain credit,
- people in transition who are recovering from the recession and working to rebuild their credit before making major credit transactions, and
- people between the ages of 18 and 29 due to their preference to use debit cards according to a recent study by creditcards.com[2].

Identity Fraud Knows No Boundary

In late 2014, LexisNexis announced the launch of the LexisNexis® Fraud Defense Network, the first-of-its-kind alliance that seeks to link organizations across all industries with resources, information and actionable intelligence to predict, detect and mitigate the risks that fraud presents. Fraud management and prevention is traditionally entity- or industry-specific because there has not been a structured effort to share insights and solutions across industries. The Fraud Defense Network provides companies and organizations from finance, retail, telecommunications, insurance, government, law enforcement and health care with a dedicated platform to share best practices and contribute to the body of knowledge of fraud.

Additionally, participants in the Fraud Defense Network can leverage the LexisNexis® Contributory Risk Repository, a contributory, cross-industry database that houses information about fraudulent and suspicious events. By sharing information across companies and industries, LexisNexis is able to identify patterns of potentially fraudulent activity across company and industry borders, leaving fraudsters nowhere to hide.

The Case for Identity Proofing

The challenges of delivering online services are clear, but can be successfully overcome with a well-designed approach to identity proofing at the enrollment level. It's not a one-size-fits-all strategy; identity proofing requirements will vary from agency to agency depending on the agency's mission. Let's look at some examples:

Case 1: Disaster Services

A federal agency provides aid to citizens after a disaster. The organization must ensure efficient delivery of benefit payments to residents who have been displaced, while maintaining processes to prevent fraud and improper payments. Not only that, the agency must also meet strict regulatory requirements for timely payments—a mandate that can only be achieved when the verification process is fast, accurate and streamlined.

Accordingly, this agency has very specific identity proofing requirements to answer what officials need to know:

- Is the identity being presented by this individual valid (i.e., not made up or assumed from a deceased individual)?
- Can we verify that the applicant owns this identity (i.e., not using a stolen or borrowed one)?
- Did the applicant own or occupy the premises during the specific time period when the disaster occurred?
- This information enables the agency to provide needed aid to landlords and tenants, while making sure that it is not dispersing aid to former residents who had moved away before the event.
- Has the applicant already received a payout from an insurer for this property during the timeframe in question? This prevents double-dipping by applicants who have been covered privately for previous non-disaster-related loss.

In this case, the information needed at the beginning of the relationship ("Who are you?") differs from what is required downstream in the relationship (benefits received). The agency and its contractors need to authenticate that citizens attempting to collect checks and gain access to food, clothing, housing and other services are the validated, verified identities who qualify for assistance. And that the payment timeline meets regulatory requirements.

Case 2: Retirement Benefits Proof

Here, identify proofing is designed to improve customer service over repeat visits. Rather than having the user go through the same steps every time they log on, the system only asks what it needs to know to facilitate the transaction. We call this "friction reduction" or "data minimization."

In this case, a retiree of a teacher's union registers on the online retirement system so she can receive her pension electronically and perform ongoing tasks such as tax withholdings and assigning beneficiary designations. She is asked to provide her name and ID number upon registering, and answer several knowledge-based authentication questions. An identity management service then verifies the asserted identity and checks to make sure the employee ID number is valid.

Later, because her identity has been proven and linked to authentication factors at enrollment, subsequent interactions are "fast-tracked." When the retired teacher submits a request to change her benefits, the system performs an invisible check to confirm her identity. This process, which uses two-factor authentication, is quick and painless for the user, and reduces the organization's operating costs.

You needn't ask for much

Though the use cases outlined above rely on a lot of personal data, it doesn't have to be furnished by the user. Identity management systems bring together, in real-time, data from tens of thousands of disparate sources to form a multifaceted view that enables the organization to verify an identity with 99.9% confidence. This level of assurance can be achieved for tens of millions of individuals while shielding personally identifiable information from the agency's view. That's good news for citizens worried about privacy, and also ensures compliance with Fair Information Practice Principles and other regulations that govern data sharing and retention. Taking this process deeper, analytics operating in the background can spot links between constituent data and suspicious entities, or recognize suspicious patterns of verification failure. Analytics can also be used to determine if the current transactional pattern of behavior is typical for the constituent, and trigger the appropriate treatments in accordance with your business rules.

Identity Proofing Fundamentals: An introduction

The identity proofing capabilities we've described in this paper can be integrated to existing business applications as callable services. You can implement them on-site or through a hosted, managed service. We find that, increasingly, organizations are choosing the managed service via "the cloud" to gain two appealing benefits: 1) It reduces costly data storage and disaster recovery; and 2) it relieves the agency of having to keep up with changing technologies and best practices.

Whether installed or hosted, constituent identity proofing solutions should encompass four technology fundamentals:

1. Real-time access to vast, diverse data sources

The accuracy with which you're able to verify that customers/citizens are who they say they are—and the percentage of the population that can be accurately verified—depends partly on the amount and variety of data your identity proofing system can access.

Best-in-class solutions offer very wide (diverse) and deep (historical) data. They reach far beyond credit bureau data, standard demographic information and "hot lists" to tap billions of public records from more than 10,000 diverse data sources. They can verify the identities of hundreds of millions of individuals.

In addition, solutions that are connected to such an expanse of data sources can provide more information about each individual. "Out-of-wallet" data points—meaning information not usually carried in an individual's wallet, such as the model of a car the consumer owned during a certain year—can be used to generate a changing set of challenge-response questions for dynamic knowledge-based authentication.

This approach also enables you to achieve the desired level of identity assurance in each instance using the least intrusive form of authentication. In other words, you can avoid asking for sensitive information that seems (from the constituent's perspective) unnecessary to the process.

2. "Data linking" to connect relevant identity elements into meaningful, purpose-specific views

Access to vast quantities of diverse data is only an operational benefit if you can do something useful with it—in the blink of an eye.

A best-in-class solution will not only be able to verify the identity of an individual, but will also have the ability to link familial relationships to the identity of that individual. For example, when requesting a copy of a birth certificate in a "closed record" state, access is restricted to specific familial relationships and/or person(s) acting on behalf of the birth certificate registrant in order to protect the confidentiality rights.

Extended verification of this kind relies on strong data linking capabilities. But data linking is also fundamental to almost all identity proofing functions. It's the key to turning raw data into information relevant to a particular transaction. And because data linking provides a more complete profile of the individual and a clearer picture of the risk of the transaction, it enables systems to invoke the right measures to achieve the degree of security required in each use case.

In general, your identity proofing solution should be able to instantly:

- Locate data relevant to the identity being presented by your constituent.
- Match it with current constituent inputs. These might include voluntary inputs like answers to knowledge-based questions, a voice or fingerprint, or a one-time pattern-based PIN, etc. They could also include data about the location and device (IP address, computer settings, etc.) these inputs are coming from. If the location is Los Angeles, for example, is the device actually set to Pacific Time and/ or is the browser configured to use English?
- Normalize and use it. Normalization involves resolving anomalies in data formatting, and eliminating redundancies to improve consistency and cohesion. Data is fused into a compact, highly efficient form for better real-time performance.
- Filter and organize it into a multifaceted view that provides what you need to know for this particular transaction with 99.9% confidence.

In some implementations, data linking is all that is required to provide the service requested by an operational system. The identity proofing solution might return appended data for an online form or a simple binary (e.g., pass/fail or yes/no) authentication result. In other cases, where risk scoring or constituent insights are required, analytics will be applied to the data.

3. Analytics to quantify identity risk and tailor methods to the needed level of assurance

Analytics can detect patterns of behavior, such as suspicious patterns of identity verification failure indicative of fraud or data integrity problems. In constituent identity proofing, analytics are also used to quantify identity risk by assigning a score representing the level of identity fraud risk associated with a particular transaction. The score is then delivered to the requesting operating system, where your configured rules and thresholds trigger an action, such as accept, refuse review, etc. Scoring of this kind provides an objective, consistent, repeatable way of making high volumes of complex decisions. Rules that you configure within the identity proofing solution enable it to make intelligent dynamic decisions about when more information or higher levels of authentication are needed to arrive at your specified level of assurance. In the case of borderline scores, for example, the system can challenge the constituent with an additional question, and/or access an additional data source.

4. Multiple authentication factors to meet constituent needs

In today's dynamic business environments, organizations that engage in identity reliant transactions need a high level of security and an equal degree of flexibility to support a wide variety of organizational platforms and end-user devices.

Choose a solution that enables what we call "variable assertion." This means that the solution supports many different ways for identities to be asserted, verified and authenticated—and that it can apply various appropriate degrees of security to different types of transactions. Users, for example, might assert their identities based on something they have (e.g., cell phone), something they know (e.g., password) and/or something they are (e.g., a voice print and a location).

To support different citizen needs and preferences requires flexible deployment; today's best-in-class solutions can provide identity proofing services simultaneously to operational systems across any number of channels and interact with user devices of all kinds. They can also play within emerging identity management platform architectures, such as OpenID Exchange and Microsoft's Open Identity Trust Framework.

What about mobile devices?

Trend watchers predicted that by 2014, the use of mobile internet will outpace desktop internet usage. How will this affect identity proofing requirements? Mobile devices provide a convenient alternative to fobs and other hardware-based tokens for use in multifactor identity authentication. Devices that users already have on their person can be loaded with software that enables it to perform authentication tasks in a number of flexible ways. One way is by downloading a PIN-generating mobile client to the registered smart phone. During account setup, users create their own visual passline by clicking squares in a grid. Later, at transaction time, this passline pattern enables them to respond correctly to a dynamically generated identity proofing challenge.

Mobile Phones Pose New Fraud Challenges

70 million mobile phones are lost in the U.S. every year. It makes you wonder: Who's getting ahold of this personal information?

Identity Proofing: Government's first line of defense against fraud and improper payments

The more your identity management service can tell you about your constituent, the better you can balance multiple business objectives. You'll also improve the service experience for your constituents, and leave them feeling more confident that government resources are being managed efficiently and responsibly.

Online government services are intended to streamline processes, reduce costs and make life a bit easier for citizens. Yet the very functionality that yields these benefits begets a whole new set of challenges for the enterprise. (In some ways, life was simpler when all interaction was performed in-person with a picture ID.) However, with the right identity proofing strategy, anchored by robust master data management and rules based solutions, your organization can maximize the full potential of enrolling beneficiaries online or in field offices while

- Mitigating fraud;
- Reducing improper payments;
- Increasing service delivery and efficiency by preventing caseworkers from having to review fraudulent applications; and
- Addressing citizens' concerns for privacy—not to mention their frustration about government waste.

Look to the Florida Department of Children and Families as testament: After implementing online self-service portals in 2004 to augment traditional channels, the agency improved its error rate to -0.5%—the best in the nation —and achieved a 250% boost in productivity (based on cases per full-time employee). And, with 95% of clients using the online system, 95% reported it was easy to use and efficient.

For more information:

Call 800.869.0751 or visit
lexisnexis.com/risk/healthcare

About LexisNexis Risk Solutions

LexisNexis Risk Solutions (www.lexisnexis.com/risk) is a leader in providing essential information that helps customers across industries and government predict, assess and manage risk. Combining cutting-edge technology, unique data and advanced analytics, we provide products and services that address evolving client needs in the risk sector while upholding the highest standards of security and privacy. LexisNexis Risk Solutions is part of Reed Elsevier, a leading publisher and information provider that serves customers in more than 100 countries with more than 30,000 employees worldwide.

Our health care solutions assist payers, providers and integrators with ensuring appropriate access to health care data and programs, enhancing disease management contact ratios, improving operational processes, and proactively combating fraud, waste and abuse across the continuum.

LexisNexis®

[1] http://www.washingtonpost.com/news/get-there/wp/2015/04/02/a-new-kind-of-credit-score-for-those-with-no-credit/

[2] http://www.usatoday.com/story/money/2015/04/15/a-third-of-millennials-have-never-had-a-credit-card/25777653/

This white paper is provided solely for general informational purposes and presents only summary discussions of the topics discussed. This white paper does not represent legal advice as to any factual situation; nor does it represent an undertaking to keep readers advised of all relevant developments. Readers should consult their attorneys, compliance departments and other professional advisors about any questions they may have as to the subject matter of this white paper. LexisNexis and the Knowledge Burst logo are registered trademarks of Reed Elsevier Properties Inc., used under license. Other products and services may be trademarks or registered trademarks of their respective companies. Copyright © 2015 LexisNexis. All rights reserved. NXR11126-00-0615-EN-US.