White Paper

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

We haven't been formally introduced.
But I'd like my Social Service Benefits now, please.

August 12, 2011

LexisNexis®

Risk Solutions
Government

That cover statement might seem a bit extreme. But consider this: In 2010, the U.S. federal government issued $125 billion in "improper payments" — defined as overpayments, underpayments, inadequately documented payments, and fraud. While these losses are attributable to many factors, government officials say the problem most often stems from administrative errors or inadequate documentation and verification of recipient information before starting the eligibility determination process.

In other words, government agencies don't always know who they are dealing with —therefore failing to ensure the right benefits and services go to the right people. But it's not only about "truing up" a name and a benefit at a single point in time. Agencies must also stay apprised of any changes to the individual's status that may render him or her ineligible for future payments.

Consider the case of a Minnesota resident who received an $85,000 worker's compensation settlement for a back injury, yet proceeded to apply for government assistance without reporting this income. The man also failed to report his other significant assets, including a 24-acre farm in Minnesota and a farm in California worth $89,000. He was ultimately charged with wrongfully obtaining assistance and welfare food stamp program fraud.

Identity proofing is critical to mitigating these problems. Identity proofing involves two processes:

1) Verifying, through electronic or manual means, that the individual is who they say they are, and
2) Authenticating that identity through knowledge-based mechanisms, such as quizzing the user on something only they know the answer to (i.e., "What was your high school mascot?")

It's important to understand that in this context, we are not referring to "network authentication," which is more about managing access to networks or computer systems/applications.

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 citizen's 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 percent boost in productivity (based on cases per full-time employee). And, with 95 percent of clients using the online system, 95 percent reported it was easy to use and efficient.

The Cost of Improper Payments

In July 2011, two New York women pleaded guilty to selling $7 million worth of fraudulently obtained food stamps for cash. One of the women was a former employee of New York City's Human Resources Administration.

A man claimed to have been displaced from his home and vehicle as a result of Hurricane Katrina in New Orleans. He collected $18,000 in assistance before officials discovered he was actually living 1,000 miles away in Cedar Falls, Iowa, during and at least four months prior to the storm.

Racine County, Wisconsin, estimates that it catches about 35 people per month who use fraudulent means to receive more assistance than they should.

The Public Wants Access to Government Online

In a TechWeb survey of 322 federal, state and local government workers and consultants, "Reducing the cost of combatting fraud, abuse and improper payments" and "Increasing agility to deal with new types of fraud and abuse" were cited as the two most important reasons to invest in data analysis methods, tools, applications and services.

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. But convenience aside, there are drawbacks to digital connectivity.

- **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 billion people are posting personal information on Facebook and other social networking sites — details like birth dates and pet's 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 persist 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 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.

Low Income & High Income Users are Online

By the way, don't make the mistake of assuming that low income people — the population most likely to use government services — aren't online. The proliferation of mobile devices has narrowed the "digital divide" between low-income and higher-income populations. A Bill & Melinda Gates Foundation study showed that 44 percent of people living below the federal poverty line regularly used public library computers with Internet access. And internet services provider Comcast, as part of regulatory compliance, recently announced reduced-rate Internet services and computer vouchers for low income families.

The Case for Identity Proofing

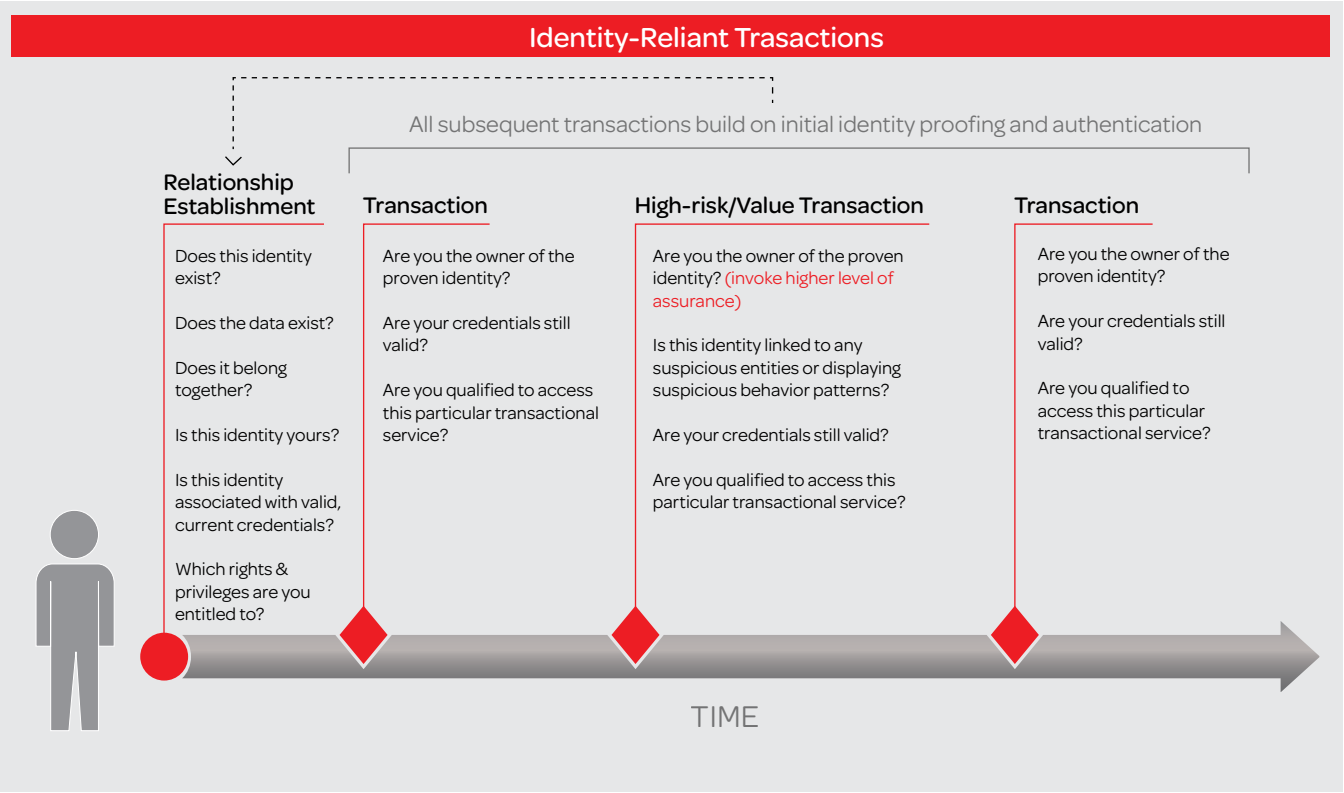
The challenges of delivering online services are clear, but successfully overcome with a well-designed approach to identity proofing at the enrollment level. It's not a one-size-fits-all strategy; identity proofing requirements will vary from agency to agency depending on the agency's mission. Let's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

Case 3: Pilot Screening

For another example of low-friction identity proofing, consider how one federal agency gets pilots through airport screening on a routine basis.

Security is paramount for everyone entering airport gates. Yet it would be extremely inefficient for pilots to be subjected to standard screening processes on their way to multiple flights a day. Instead, pilot access is streamlined and controlled by an identity proofing program. When pilots enroll in the program, their identities are proven, their employment status and flight credentials validated, and their fingerprints recorded. Subsequently, each time a pilot passes through the security area, he presents his employee badge and submits his fingerprint. The identity management system matches the fingerprint to the pilot and checks currency of flight credentials. This process provides a very high level of assurance without unnecessary hassle or delay.

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.

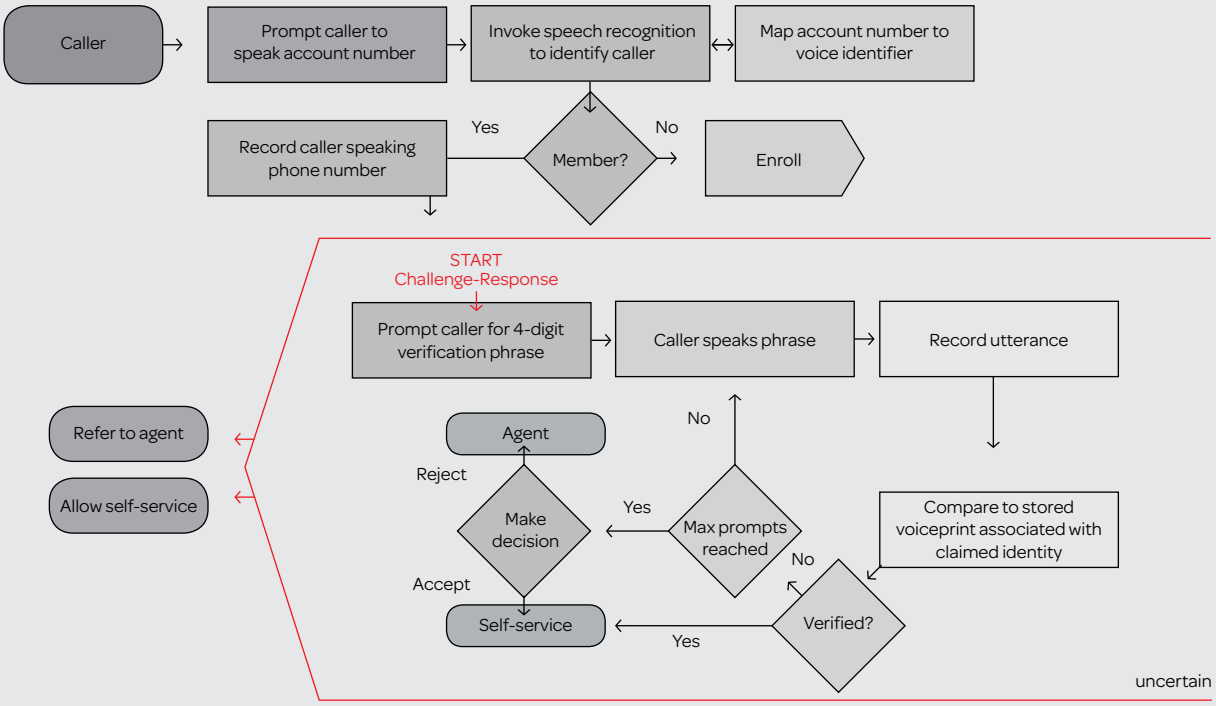
Taking this process deeper, analytics operating in the background can spot links between constituent data and suspicious entities, or recognize suspicious patterns of verification failure. Analytics can also be used to determine if the current transactional pattern of behavior is typical for the constituent, and trigger the appropriate treatments in accordance with your business rules.

Identity Proofing Capabilities Benefit a Wide Range of Social Services Agencies, Including:

- Child Support
- Children and Family Services
- Disaster Services
- Education
- Foster Care
- Homeless
- Public Housing
- Retirement
- SNAP
- TANF
- Unemployment
- WIC
- And more

Sample Transaction with Voice Verification

An additional knowledge-based "challenge-response" quiz is invoked only if the identity cannot be verified to the level of assurance required by this organization for this particular type of transaction.



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.

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 fuse 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 predict 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 set up, 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?

It's time to face identity challenges head on.

With citizens frustrated by the state of our nation's fiscal health — and an initiative by the federal government to increase the debt ceiling and to slash improper payments by $50 billion by 2012 — identity proofing should already be on your radar as a business and IT strategic objective. To paraphrase an old adage, the key to success is not only who you know, but what you know about them.

Check out our blog at: idmanagement.lexisnexis.com

For more best practices around identity in the government space, contact LexisNexis:
www.lexisnexis.com/government
888.579.7638

About LexisNexis® Risk Solutions

LexisNexis Risk Solutions (www.lexisnexis.com/risk) is a leader in providing essential information that helps customers across all industries and government predict, assess and manage risk. Combining cutting-edge technology, unique data and advanced scoring analytics, Risk Solutions provides 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 government solutions assist law enforcement and government agencies with deriving insight from complex data sets, improving operational efficiencies, making timely and informed decisions to enhance investigations, increasing program integrity and discovering and recovering revenue. For more information, visit www.lexisnexis.com/government.

LexisNexis®

LexisNexis®