White Paper

The Social Security Number: A Not-So-Positive ID

The case against using SSNs in identity management

LexisNexis®

Risk Solutions
Identity Management

There's a reason the Social Security number (SSN) was so named — and it had nothing to do with providing a secure personal identity for citizens. The U.S. Government implemented SSNs in the 1930s as a means of assigning retirement benefits to workers under the New Deal Act. But in the decades since, the SSN has evolved into a sort of "digital DNA" — copped by all sorts of non-government entities as the de facto standard for identifying and tracking individuals in various activities of daily life. From paying taxes to buying a mobile phone to enrolling in a college course, the SSN has become the key to the magic kingdom of American goods and services.

On the surface, it seems logical that organizations would use the SSN as a unique identifier for individuals. After all, more than 450 million SSNs have been issued to date, every individual is given a different number, and recipients are taught from the start to fiercely protect their number from getting into the "wrong hands." But the truth is that social security numbers aren't really that private or secure — and not only because of identity theft.

Let's look at some of the compelling reasons against using the SSN for identity verification and authentication.

Reason #1: SSNs aren't necessarily unique to one person.

Stealing or "borrowing" SSNs is not too tough a task for motivated people. Consider these facts:

- **In 2010, more than 8 million Americans suffered identity theft.** Based on news headlines and Internet searches, it's a wonder that number isn't higher. Incidents of hacked corporate databases, misplaced laptops and lost records — including patient files — have become a fairly regular occurrence. And it may surprise you to learn that a growing percentage of identity theft victims are children who already have SSNs; with no credit to monitor, fraudulent activity goes unnoticed because no one is checking a child's credit report. These SSNs can be sold illegally through websites and on the street for $40 to $80 each, according to one official from the Social Security Administration. Even more startling is that the Social Security Death Index is just an Internet browser away: enter a name, and voila, the thief has a list of last-known addresses and social security numbers of deceased individuals at their fingertips.

- **Nine digits really means six.** Until recently, the system used by the Social Security Administration to assign the 9-digit SSN wasn't completely random. For SSNs issued prior to June 25, 2011, the first three digits referred to the individual's state of residence. Thus, a number starting 512 meant that the person lived in Kansas when the number was assigned to them. The legend for this numbering scheme is readily available online, making it much easier for the enterprising thief to piece together information to create a more accurate and believable identity.

- **SSNs are more exposed than you might think.** Consider this: For years, SSNs were included on military IDs, and in some states, on drivers' licenses. Imagine the number of times these IDs are presented and documented when registering for various services, writing checks, boarding airplanes and more. We readily hand over our SSN to a multitude of people every week. Not only that, anyone with access to household files can find a SSN on a tax return, a mortgage document, medical records — even on some utility bills.

- **People make mistakes.** Often, a misused SSN isn't the work of a dubious mind but a sloppy typist. A typo in a 9-digit number is less obvious than a misspelled name or address, so the error may go unnoticed until a search later reveals that two names share the same SSN or that an individual has become associated with two SSNs.

Each year nearly 13 million workers pay taxes with the wrong SSN, suggesting that many of those workers are using a SSN that does not belong to them.

Remember: the fraudulent user may not necessarily be a stranger. Minor children have been known to use their parents' SSNs to access age-restricted web sites.

Reason #2: Many people don’t have a SSN.

They may object for personal or privacy reasons. Or, they may object for religious reasons. Religious objections to SSNs have been litigated all over the country in recent years, from DC to California. In fact, the issue was partially responsible for Congress passing the Religious Freedom Restoration Act in 1993. Another potential reason a person may not have a SSN is because they are a non-U.S. citizen in this country temporarily. (Keep in mind there were more than 690,000 international students attending American colleges and universities during the 2009-2010 school year. They all need services from banks, utilities and other organizations that typically favor SSNs for identification.) The fact that these groups are functioning in American society without using SSNs proves that this is not the only effective identification tool.

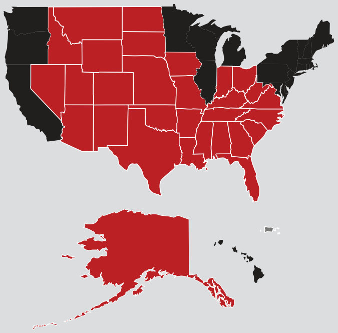
Reason #3: The uptick in privacy-related legislation casts a negative spotlight on the use of SSNs.

More and more states are enacting legislation to restrict or prohibit the collection, use or disclosure of individuals’ SSNs. In the State of New York, two senate bills were introduced that specifically prohibit organizations from requiring an SSN for website access, among other uses. **As of October 2011, 38 states had some type of SSN-restriction law on the books.** On the federal level, the Social Security Protection Act of 2010 limits the U.S. government’s use of and access to SSNs.

So what’s the alternative?

Take for example, a parent or guardian who has consented to their child using a children’s social website. In response to COPPA regulation, websites that cater to children must ensure children are protected online. Many social websites must obtain guardian permission for children to access their content.

States that prohibit or restrict the use of SSNs as part of business operations.



In order to prove it is actually the parent providing permission and not the work of a precocious child, the website could go beyond a simple request of name and SSN. Instead, basic demographic information could be paired with one or two dynamic knowledge-based quiz questions that couldn’t easily be found on a bill or similar piece of mail lying around the house. This gives the social website greater confidence that the user presented is who they claim to be, and not the child assuming the parent’s identity.

In another scenario, a healthcare clinic that serves a large demographic of non-American patients wants to begin offering extended patient access through their online portal. While online portals are a great tool in helping patients participate in their healthcare decision making, too many barriers to sign-up can prevent patient adoption.

Instead of requiring a piece of information that may not be possessed by their patients, the clinic could run other identity elements, such as name, address, and DOB and then send a one-time password to the user’s mobile phone number on file in order to complete enrollment. The process is simple, streamlined and is inclusive to patients of all backgrounds.

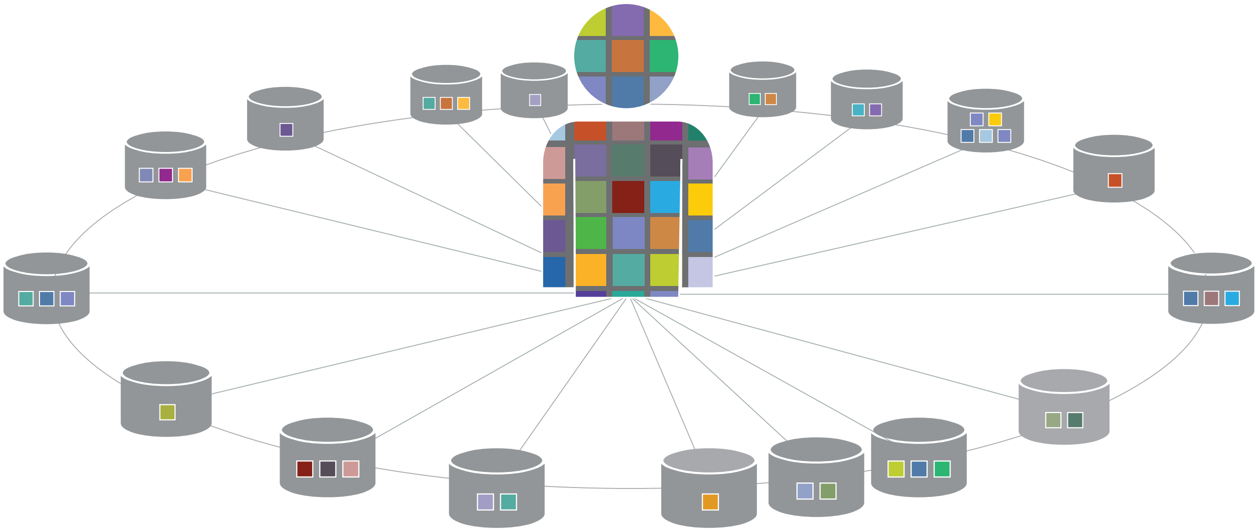
In yet another example, consider a government agency that provides subsidized phone service to qualified low-income families. Simply running an SSN would not provide enough information to determine if the applicant is qualified for the benefit.

The agency could first ensure the recipient is who they say they are by running them through a simple series of verification checks. The confirmed identity could then be matched against income records and other applicable financial data using data linking technology to ensure the recipient is qualified to receive the benefit.

From an unknown prospect to a well-known customer

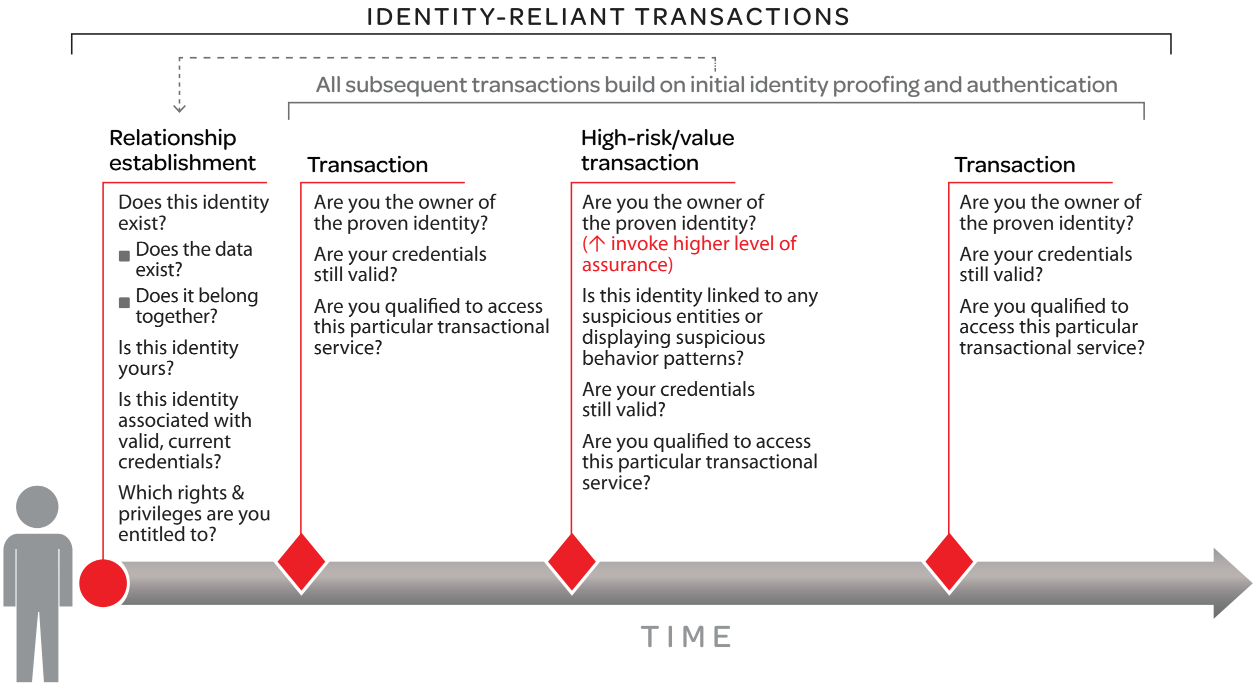
The use cases outlined above all rely on robust identity proofing systems that bring together, in real-time, data from tens of thousands of disparate sources. The person being IDd doesn't even have to furnish the information themselves. By having instant access to this multifaceted view of the individual, the organization can verify an identity with 99.9% confidence. What's more, this level of assurance can be achieved for tens of millions of individuals while shielding personally identifiable information from the organization's view — a feature critically important to complying with privacy laws, Fair Information Practice Principles and other regulations that govern data sharing and retention.

Increasing Volume & Importance of Identity-Reliant Transactions



But simply increasing the pile of "digital DNA" isn't a complete — or effective — strategy. You should carefully consider how the information will be used, and in what circumstances. In other words, ask only what you need to know. For each customer/constituent and type of transaction, your ideal identity management solution should determine, in real time, what your organization needs to know to complete the request.

What You Need to Know Changes Throughout Customer Lifecycle



IDENTITY-RELIANT TRANSACTIONS

All subsequent transactions build on initial identity proofing and authentication

Relationship establishment

Does this identity exist?

- Does the data exist?
- Does it belong together?

Is this identity yours?

Is this identity associated with valid, current credentials?

Which rights & privileges are you entitled to?

Transaction

Are you the owner of the proven identity?

Are your credentials still valid?

Are you qualified to access this particular transactional service?

High-risk/value transaction

Are you the owner of the proven identity? (↑ invoke higher level of assurance)

Is this identity linked to any suspicious entities or displaying suspicious behavior patterns?

Are your credentials still valid?

Are you qualified to access this particular transactional service?

Transaction

Are you the owner of the proven identity?

Are your credentials still valid?

Are you qualified to access this particular transactional service?

TIME

This might cause concern among security personnel who aim to reduce risk by restricting access. But with a flexible, multi-factor authentication program, you can find a balance between security and service, and appropriately manage the different types of transactions that occur at various points in customer/constituent lifecycles.

Multi-factor authentication uses at least two independent elements or "factors" to verify an identity. This combination may be derived from:

- Something the user knows, such as a user name, password, PIN or answers to questions;
- Something the user has, such as a token, access card or key fob; and/or
- The user's own unique characteristics, such as a fingerprint, voice or iris (i.e., biometric).

Multi-factor authentication in action

Let's say Kenneth, a bank customer, is asked to go through a set of challenge-response questions every time he wants to access his accounts. This could get frustrating for him rather quickly – especially if he's trying to do something relatively low-risk like verifying whether a check cleared. Instead, the bank could use a multi-factor authentication approach, using a standard voice biometrics program and requesting a simple PIN for routine inquiries, while employing an additional dynamic, knowledge-based quiz when he wants to transfer funds. This assures a level of security consistent with the risk, while taking the customer experience into account.

Here's another way multi-factor authentication can be applied: While attending a conference in Mexico City, Rita accesses her mobile phone's account management interface to turn on international calling. A single identity-check question pops up on the screen, and after answering it, international calling is activated. A couple of weeks later she's in Jamaica for vacation and again wants to make international calls. In this case, she receives a one-time password via secure text (her preferred form of communication) to authenticate her identity before approving her service. The process is conveniently completed and she feels reassured about the security of her account. Rita travels frequently to Mexico City for business, but she's never been to Jamaica – and the identity management service knows it.

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 "cloud service" to gain two appealing benefits: **1) It reduces costly data storage and disaster recovery; and 2) it relieves the organization of having to keep up with changing technologies.**

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

At LexisNexis, many of our high transaction volume customers in government and healthcare do not collect the SSN as an input during their customer enrollment/ onboarding.

Even without the SSN, **they are able to experience excellent results (a 91- 96% success rate) in uniquely identifying an individual and proceeding to** identity verification and/or quiz generation for identity authentication.

Real-time access to vast, diverse data sources

The accuracy with which you're able to verify that individuals are who they say they are 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 SSNs and other 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—even without inputting an SSN.

In addition, solutions that are connected to such an expanse of data sources can provide more information about each individual. For example, "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 consumer's perspective) unnecessary to the process.

"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 real time.

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 management 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 the individual.

- **Match it with current consumer 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 consumer insights are required, analytics will be applied to the data.

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 consumer 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 person with an additional question, and/or access an additional data source.

Multiple authentication factors to meet consumer/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), as outlined in the examples on pg. ___.

To support different customer 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 protocols, such as OpenID Exchange and Open Identity Trust Framework.

There are any number of ways to verify and authenticate without that number.

As cases of identity theft rise, and customers and lawmakers demand more protection of personal privacy and sensitive data, organizations can't afford the risks associated with using SSNs in identity proofing. Forward-thinking enterprises have realized that a robust, flexible identity management strategy is the most effective approach for allowing customers access to goods and services, providing quality customer service and still meeting security objectives.

For more best practices in identity management contact LexisNexis® Risk Solutions:
Website: http://idmanagement.lexisnexis.com
Email: idmanagement@lexisnexis.com
Phone: 877.221.5292

This document is for educational purposes only and does not guarantee the functionality or features of LexisNexis products identified. LexisNexis does not warrant this document is complete or error-free. If written by a third party, the opinions may not represent the opinions of LexisNexis.

The LexisNexis Risk Solutions Identity Management services are not provided by "consumer reporting agencies," as that term is defined in the Fair Credit Reporting Act (15 U.S.C. § 1681, et seq.) ("FCRA") and do not constitute "consumer reports," as that term is defined in the FCRA. Accordingly, this service may not be used in whole or in part as a factor in determining eligibility for credit, insurance, employment or another purpose in connection with which a consumer report may be used under the FCRA. LexisNexis and the Knowledge Burst logo are registered trademarks of Reed Elsevier Properties Inc., used under license. Copyright © 2012 LexisNexis. All rights reserved.
NXR01699-0 0811