White Paper

The Most Important Question in Customer/Constituent Identity Management

Discover the answers for balancing increased value with less identity risk.

February 2010

LexisNexis® | Health Care

The most important question in identity management is not: "Who are you?" It's "What do we need to know?"

Traditionally papers by identity management providers discuss definitions for identity validation, verification and authentication, delineating best practices around these steps. These are important topics, and it's good to see standards emerging in some industries to guide and regulate such practices.

In this paper, however, we want to shift the focus of the discussion to the broader business/government context in which identity management occurs. Effective customer/constituent identity management springs from this fundamental question:

"Given what we are trying to accomplish through this particular transaction, what do we need to know about this individual?"

Or, more elaborately: "What do we need to know to prove this individual is who they say they are and may have access to this resource based on those identity credentials?"

The answer is determined by the intersection of multiple factors: your objectives; product and service characteristics; population demographics and attitudes; the nature, value and riskiness of the transaction being performed; the point in the process and relationship where it takes place; and organizational risk tolerance.

Getting the answer right is increasingly critical to success.

Identity management is a business enabler

Getting the answer right is critical because across nearly every industry and government sector today, identity management is becoming a key enabler of core business functions.

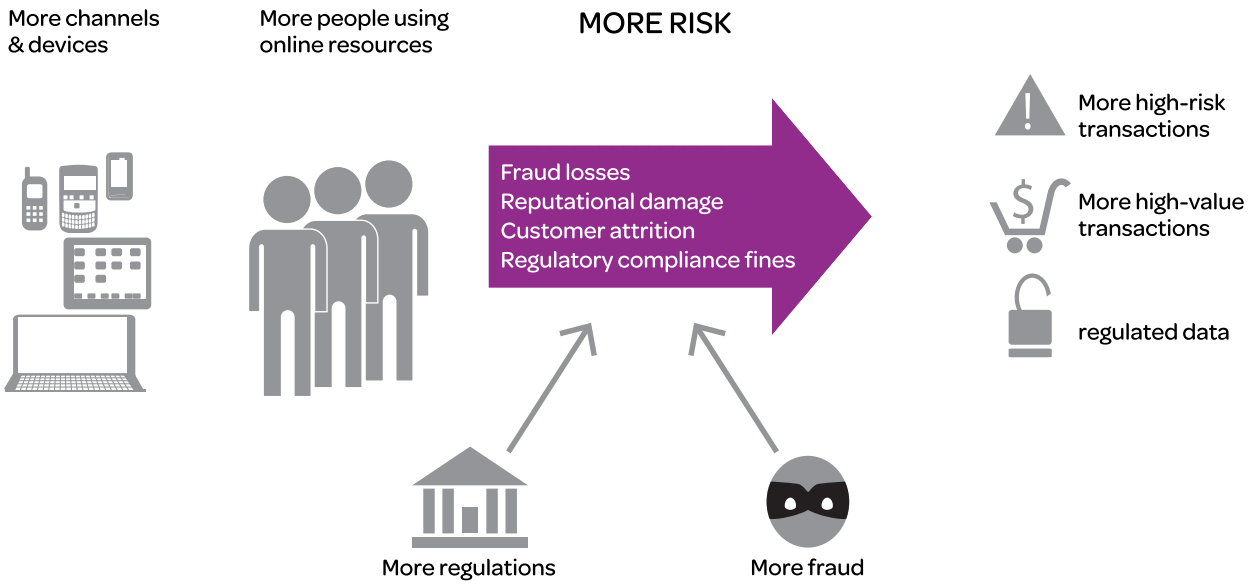
Businesses not yet subject to such regulation are nevertheless well aware that identity fraud is the fastest growing of crimes, affecting more than 11 million adults in the US in 2009. It's also a deepening source of losses for many businesses as they take measures to assume more of the risk for their customers and deflect the strongly negative impacts these fraudulent activities can have on attrition rates and brand reputation. Customers, they know, increasingly expect the businesses they patronize to protect their accounts and personal data.

Yet today identity management is as much about opportunity as obligation. How organizations make sure they're engaging with legitimate customers/constituents in legitimate transactions affects performance.

> "... enables the right individuals to access the right resources at the right times and for the right reasons — a crucial and increasingly business-driven undertaking for any enterprise"
>
> – Gartner, May 2010

For government, it means more effective service delivery, the ability to efficiently meet growing demand for services, and reduction of unnecessary cost and risk. For business, it means a potential new source of competitive advantage. As a recent Gartner report states, identity management is "increasingly recognized as delivering real-world business value," and "identity management agility improves support for new business initiatives and contributes significantly to profitability.

Increasing Volume & Importance of Identity-Reliant Transactions



Enhance existing customer/constituent-facing systems with new identity management capabilities

Identity management is changing to encompass these increasing business/government demands and application variability.

Point solutions and one-size-fits-all implementations are being supplanted by or absorbed into more comprehensive yet flexible approaches. These provide identity management coherency across processes and relationships as well as identity management consistency across multiple channels (internet, mobile, IVR, call center and in-person). At the same time, they enable organizations to efficiently implement a wide range of identity management implementations that bring the right identity elements together into the appropriate view and assurance level for each customer/constituent transaction.

Established organizations can layer new identity management capabilities onto existing systems in the form of services. Such services may be added to current operations via an installed or hosted service oriented architecture.

Why not just extend enterprise identity management solutions to customers/constituents? It's difficult to make applications designed for managing employee access to internal networks and facilities accommodate the diversity and dynamic nature of customer/constituent interactions. These external interactions may occur across the public internet or the private networks of other businesses in a market ecosystem. They're affected by economic conditions, attitudinal shifts among consumers and citizens, competitor actions and changing business models.

Moreover there are a couple of big differences between employee and customer/constituent identity management: First, you usually know much less about your customers/constituents than you do about your employees, who have gone through extensive vetting, often including background screening. Second, it is nearly impossible to mandate that customers use a specific method (e.g., smart cards, tokens, etc.) if they don't choose to. If you try to mandate a method that doesn't feel comfortable or convenient, they may simply take their business elsewhere.

For these reasons, in our experience, extending enterprise identity management to customer/constituent transactions doesn't work very well. Here's what does...

Don't do business without it

- Record number of identity fraud victims in 2009
- New accounts fraud, occurring over longer periods without detection, produced more dollar losses than any other type of fraud

– **2010 Identity Fraud Survey Report** Javelin Strategy & Research

Three key concepts

These concepts are at the core of the most successful customer/ constituent identity management solutions. They are general principles shared by diverse business-specific implementations.

1. Identity management is as much about business as about security

Identity validation (or "resolution"), verification and authentication, commonly regarded as security functions, have far-reaching business ramifications. How you perform them can strongly shape your interactions with customers/ constituents. Thus, while it's important to follow industry standards where available, you also want to make sure that how you implement identity management is tailored to your market or citizenry, business plan or agency mission and organizational risk needs.

There's no "one size fits all" solution to customer identity management. Take the case of a leading gas and electric utilities provider. When onboarding a new customer applying for a senior discount, the company needs to know:

- Is the identity being presented valid? (i.e., it has not been made up or assumed from a deceased individual).
- Can we verify that the applicant owns this identity? (i.e., is not using a stolen or borrowed one).
- Upon being granted access to the service, does the applicant qualify for a Senior Discount?
- Does the applicant occupy the premises for which the discount will be applied? Property occupancy, as opposed to ownership, is the critical piece of information for determining whether or not the individual should be given access to this program. Without it, seniors who own properties could provide discounted rates to tenants who are below the age threshold or arrange for discounts to be applied illegitimately to the residences of children, other family members or friends without the knowledge of the senior.

Compare this with what a government agency assisting citizens after a disaster needs to know. To offer efficient benefit delivery, while guarding against waste, fraud and abuse, the agency has very specific identity proofing requirements:

- Is the identity being presented valid? (i.e., it has not been made up or assumed from a deceased individual).
- Can we verify that the applicant owns this identity? (i.e., is not using a stolen or borrowed one).

"Fraud is eating your revenue and profits"

– Market Overview: Fraud Management Solutions Forrester Research, Inc.

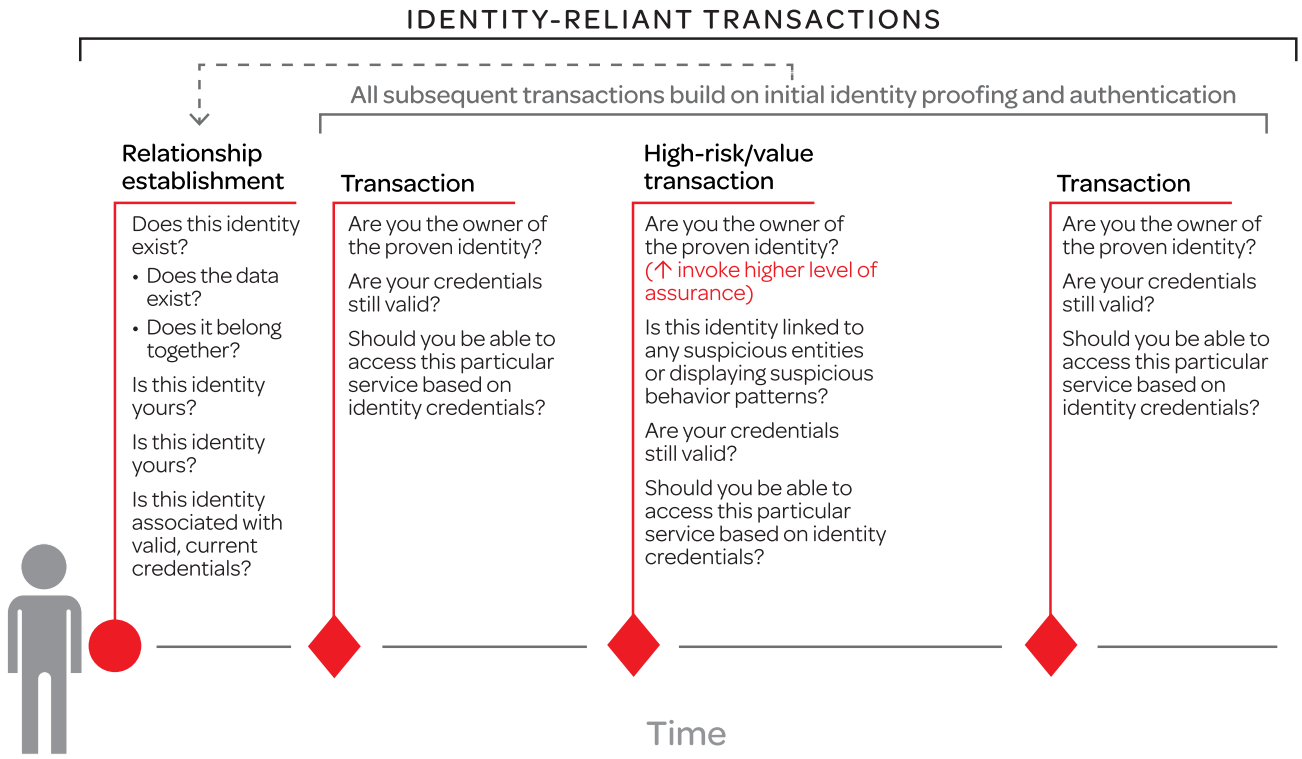
- Did the applicant own or occupy the premises during the specific time period when the disaster occurred? This information enables the agency to provide the right type of aid to landlords and tenants while making sure that it is not dispersing aid to former residents who had moved away before the event.
- Has the applicant already received a payout from an insurer for this property during the timeframe in question? This prevents applicant who has been covered privately for previous non-disaster-related loss from double-dipping.

Moreover for both the utility and government agency, what the organization needs to know when it first establishes the relationship is different from what it needs to know downstream in these relationships.

For example, the utility will need a way to authenticate that customers attempting to access online account management features are the previously validated, verified identities who opened the accounts. The government agency and its contractors will need a way to authenticate that citizens attempting to collect checks and gain access to food, clothing, housing and other services are the validated, verified identities.

For each customer/constituent and each type of transaction, the identity management solution finds out in real time what the organization needs to know. The success of this process depends on the next key concept.

What You Need to Know Changes Throughout Customer Lifecycle



2. "Know your customer" is the point of balance for multiple (even opposing) objectives

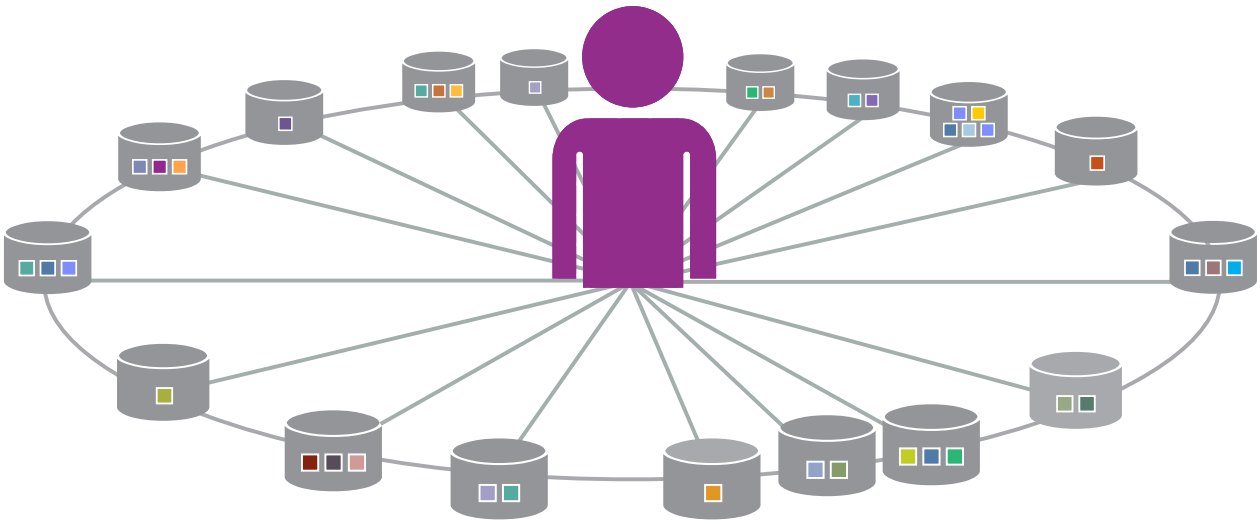
"Know your customer" is a phrase that traditionally has different meanings to customer/constituent service on the one hand and fraud management on the other. Service folks are concerned with raising customer/constituent satisfaction by increasing access and ease. Security folks are concerned with reducing risk by restricting access.

Effective identity management unifies these objectives. Fusing what you know about your customer from both a service and a security sense enables you to appropriately manage the different types of transactions that occur at various points in customer lifecycles.

Imagine Kenneth, a financial services customer. To access his online investment accounts, he is presented with a set of challenge-response questions. It's the fifth time he's gone through this exact same process at log-on.

The company could provide a better experience by invoking an identity quiz only when Kenneth attempts to perform a high-risk transaction, such as a balance transfer or address change. Moreover when a quiz is invoked it doesn't invariably consist of the same three questions set up by Kenneth when he created the account. Rather one of these is combined with a dynamic knowledge-based quiz. There might be a question, for example, about some nonfinancial fact in his personal history (e.g., "What was the name of the street you lived on after you graduated from college?) that is easy for him to answer.

Increasing Volume and Importance of Identity-Reliant Transactions



In real time, data from tens of thousands of disparate sources can now be brought together to form a multifaceted view that enables businesses and government agencies to resolve an identity with 99.9% confidence. This level of assurance can be achieved for tens of millions of individuals while protecting the privacy of these individuals by shielding personally identifiable information.

Kenneth notices that the level of security seems to adjust automatically to what he's doing: lower for things he does all the time, higher when it's something he rarely does or when he's trying out a new service. There's also more security when he's accessing his accounts from an unusual location, particularly a public wireless network. Overall, Kenneth has the impression that he is known and that the service is responding to him.

The more your identity management service can tell you about your customer/constituent, the better you can balance multiple objectives. Knowing more enables you to invoke the right identity management measures necessary to reach your desired level of assurance for each transaction. At the same time, you can improve the experience for your customers/constituents and tailor service features and offers to their individual needs.
But knowing more doesn't mean asking more.

3. Ask for only what you need to know

Knowing more can, in fact, enable you to ask for less information. In identity management industry jargon, the objective is "friction reduction" through "data minimization." Improve the customer/constituent experience by not asking for information you don't need.

Think about how this principle can streamline online prescription processing.

Low-friction process for physicians. When physicians are enrolled as users of the electronic prescribing network, they are asked to provide their name and State medical license number as well as to answer several knowledge-based questions. An identity management service then verifies the asserted identity and checks to make sure the license is current and that the physician is also licensed by the US Drug Enforcement Administration (DEA) to prescribe controlled substances.

Because the identity has been proven and linked to authentication factors at enrollment, subsequent transactions are accomplished with ease. When the physician submits a prescription, the system performs an invisible check to confirm that licenses are still valid. This process, which uses DEA-required two-factor authentication, is quick and painless for the physician. For example, in addition to inputting a correct username/password pair, physicians use a hard token as their second authentication factor. Alternatively, the second factor could be a hard-token equivalent (software that generates a one-time password from their smart phone) or a biometric (e.g., a fingerprint or a voiceprint).

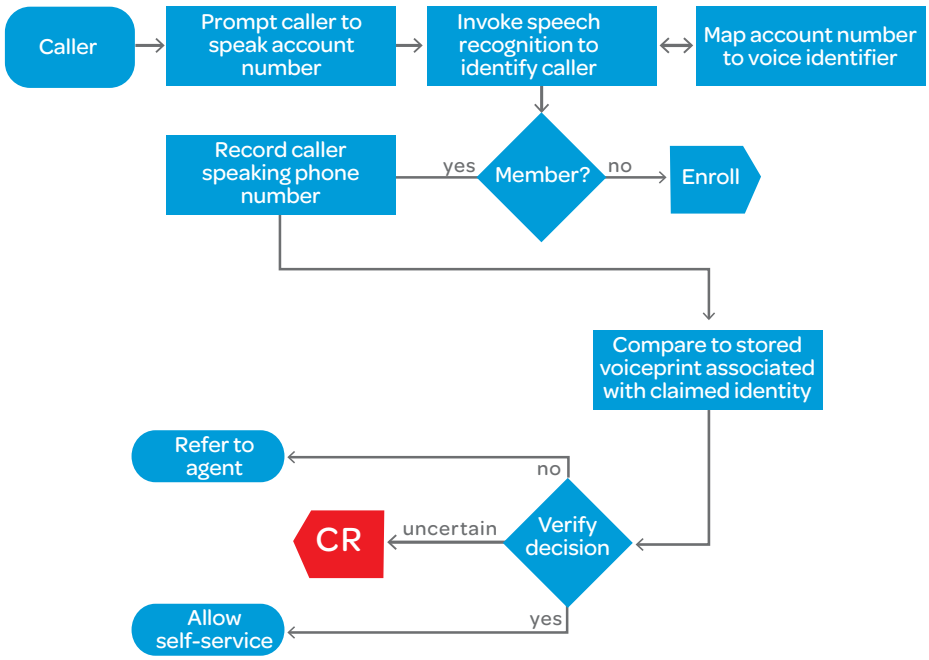
Or consider how a federal agency is managing the identities of pilots who routinely need to pass through checkpoints to reach their gates.

Low-friction process for pilots. Security is paramount, of course, for everyone entering airport gates, yet it is extremely inefficient for pilots, who often pass through security areas several times a day, to be subjected to standard screening processes. Instead, pilot access is streamlined and controlled by an identity management 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 pilots pass through the security area, they present their employee badge and submit their 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 delays.

In addition, much of the necessary security can be invisible to the user. Analytics operating in the background can spot links between customer/constituent data and suspicious entities or recognize suspicious patterns of verification failure.

You can also use analytics to determine if the current transactional pattern of behavior is usual or unusual for the customer/constituent, and interact with your business rules to adjust the security level and trigger the appropriate treatments.

Increasing Volume & Importance of Identity-Reliant Transactions



Reacting to customer/constituent responses in real time, and based on your rules and thresholds for different product lines, channels and types of transactions, an identity management service can make dynamic decisions about when to invoke additional and/or stronger measures.

For example:

An online retailer uses identity management to clear more orders and increase customer satisfaction while reducing risk for both fraud and late deliveries. When Jeff purchases a laptop PC at the retailer's site, he pays extra for expedited shipping and enters a delivery address he's never used before, which is different from his billing address. There's no delay in sending out his order, however, because it's not held up for manual review. The identity management service scores the transaction as low for fraud risk because it knows that the device from which he is ordering has been used by Jeff in the past and that the delivery address is a location where he lived until five years ago. (Jeff's mother, intended recipient of the birthday present, still lives there.)

A telecommunications company uses identity management to provide its mobile voice/data customers with superior service. While attending a conference in Mexico City, Rita accesses her mobile phone 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 challenge via secure SMS (her preferred form of communication) in order 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.

In the next section, we discuss the technology fundamentals necessary to achieve this kind of powerful, flexible identity management.

Four technology fundamentals

The identity management capabilities we've described in this paper can be added to existing operational systems as callable services. You can implement them on-site or through a hosted, managed service.

We find that an increasing number of organizations are choosing the managed service. One reason is that businesses are becoming wary of storing personally identifiable information on their customers. They're also aware of the challenges of keeping identity management solutions up-to-date in consumer markets where attitudes, technology adoption, competitive strategies and business models change frequently.

Whether installed or hosted, customer/constituent identity management solutions should encompass the following technologies:

1. Real-time access to vast, diverse data sources
The accuracy with which an identity management solution verifies that customers/constituents are who they say they are—and the percentage of the population it can accurately verify—depends partly on the amount and variety of data it 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 with access to such an expanse of data sources provide more information about each individual. Plentiful "out-of-wallet" data points (information not usually carried in a customer/constituent's wallet), including time-sensitive data (e.g., the model of a car the consumer owned between 1995-97) can be used in generating a changing set of challenge-response questions for dynamic knowledge-based authentication.

Fraudsters, of course, are increasingly sophisticated in their methods and use the internet to collect information they can use to answer such challenge questions. Still, best-in-class identity management services can form a far more complete and nuanced picture of a customer/constituent identity than would be worthwhile, from a return on investment perspective, for a fraudster to try to construct. The combinatorial possibilities make it extremely difficult for fraudsters to pass challenges that are trivial for legitimate customers.

This approach also enables you to use the least intrusive form of authentication required in each instance to achieve your desired level of identity assurance. Because you can achieve a high level of identity assurance by requesting inconsequential information, you can avoid asking for sensitive information. (Most of us have had the discomforting experience as consumers of being required to supply personally sensitive information, such as our social security number, when it's not clear why.)

To further expand your identity solution's vision, consider participating in a consortium for aggregate-level data sharing (no individual customer data) with other companies in your industry or market ecosystem. Advantages include:

- Reaching beyond your own data and that available from third-party sources.
- Being forewarned about fraudsters and schemes other companies have experienced which haven't yet hit your organization.
- Improving fraud detection by analyzing additional identity characteristics, such as the velocity with which variations of an identity appear across consortium member data.

If you're interested in this added protection, make sure that you can opt-in as it makes sense for your business. You may want to participate across the board or just for identity management implementations for certain lines of business or products.

As you expand the range and richness of customer/constituent identity data, especially if you're participating in consortium, you need a powerful, flexible system to take advantage of it.

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.

For example, a best-in-class solution can not only verify the identity of an individual seeking a copy of their birth certificate, but the identity of that individual's mother as well. Many state public records agencies are restricted by law to issuing authorized copies only to those individuals.

Extended verification of this kind depends 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 instance.

Success Story:

Healthcare remote prescription management

Objective

- Improve accuracy of identity management and ease of use for patients

Solution

- Multifactor authentication
- Something you have: filled prescription RX#
- Something you know: answers to dynamic knowledge based quiz

Results

- 500,000 patients — identification and generation of knowledge based questions for 99.5%
- Of patients who were offered the quiz:
- 90% passed
- 5% failed
- 5% opted out

In general, your identity management solution should be able to instantly perform these functions:

- **Locate data relevant to the identity** being presented by your customer/constituent.
- **Match it with current customer/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 management 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 customer/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 are mathematical algorithms that examine data and complex data relationships (including the multifaceted views constructed through data linking). Their job is often to detect patterns of behavior, such as suspicious patterns of identity verification failure indicative of fraud or data integrity problems.

In customer/constituent identity management, 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.

> " Risk managers measure the risk reward ratios to determine how tightly or loosely the identity verification system should be configured. Therefore, risk managers need a solution that is easily adjusted to meet changing business needs, risk tolerance and new threats."
>
> – **Barbarians at the Gate: Identity Proofing and Assurance**
> Burton Group, May 2010

Rules you configure within the identity management solution enable it to make intelligent dynamic decisions about when it needs more information or higher levels of authentication to arrive at your specified level of assurance. In the case of borderline scores, for example, the system can challenge the customer/constituent with an additional question and/or access an additional data source.

4. 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, in identity management industry lingo, "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).

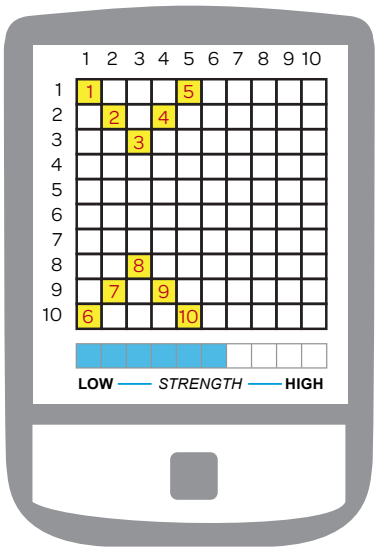
This is the kind of flexibility that is enabling a leading online stock trading and investing company to make a commitment that has become a competitive advantage. This company vows to support any access methods its clients want to use. Period.

Supporting different customer/constituent needs and preferences, you also need flexible deployment. Today's best-in-class solutions can provide identity management services simultaneously to operational systems across any number of channels and interact with customer/constituent 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.

This device 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 the grid.

Later, at transaction time, this passline pattern enables them to respond correctly to a dynamically generated identity verification challenge.



Five Best Practices for Finding Your Answer

Here are some quick takeways on the steps our consulting teams use to help clients answer the question: "What do we need to know?"

- Analyze your objectives and degree of risk tolerance
- Analyze your customers
- Analyze your business processes
- Analyze your market ecosystems
- Revisit and reassess your decisions frequently

Conclusion

The number of identity-reliant transactions is multiplying rapidly, and these transactions are becoming ever more critical to the success of many businesses and government agencies. That makes it essential for these organizations to ask themselves the fundamental question: What do we need to know?

This question is the starting place for all other questions in identity management. The right answer is the key to making identity management an enabler of great services accessed with ease by customers/constituents and delivered with low cost and fraud risk.

For More Information:

Call 800.869.0751 or visit www.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 all industries and government assess, predict and manage risk. Combining cutting-edge technology, unique data and advanced analytics, LexisNexis 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 world leading provider of professional information solutions.

Our identity management solutions assist states with ensuring appropriate access to public benefits, enhance program integrity and operational efficiency, reduce the impact of identity theft and fraud, and proactively combat fraud, waste and abuse throughout government programs. 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. The NAC is in the unique position to benefit by overlaying state data with the complex analytics of LexisNexis's solutions.

LexisNexis® | Health Care