White Paper

Financial Services Identity Management in an era of tell-all and technology overload

Protect your most priceless assets under management: Your customers.

June 4, 2012

LexisNexis®

Risk Solutions

Few industries have benefitted from the Internet evolution to the degree financial services has. The antiquated term "bankers hours" is lost on a new generation of consumers who enjoy access to their money, and information about it, whenever and wherever it's needed. Whether they're looking to splurge on a must-have item or just fill the gas tank, consumers now routinely check account balances, transfer funds, deposit checks and pay bills straight from laptops, smartphones and ATMs. They may have even established their accounts online in the first place, and never actually been face to face with your institution at any point in the relationship.

Online banking has made its way to more than 72 million American households[1]. The benefits to the customer are obvious and many consumers have come to expect, and rely on, these alternate banking channels. Meanwhile, financial institutions have been able to dramatically lower the cost of servicing these customers, who no longer need a physical branch location to perform the most typical transactions. Transactions that used to cost a few dollars in staff time and overhead can now be completed faster — and more conveniently — at a much lower cost.

But what sounds like a no-brainer to the product development and marketing teams can create headaches for the IT and customer service departments. To deliver the ultimate in ease and efficiency through remote, "faceless" channels, institutions must not only consider the impact on security but also the compliance requirements associated with implementing these technologies. IT professionals need to ensure accounts are impenetrable without impeding the speed and convenience customers demand. It's a delicate balance, but one that can be solved with a comprehensive identity management strategy that:

1) Ensures compliance with federal banking authentication guidelines;

2) Promotes efficient banking processes and customer satisfaction; and

3) Reduces fraud without compromising #2.

Financial institutions of all types and sizes — from the community credit union to the national megabank — are deploying robust identity management systems to address one or more of these business drivers. Before we talk about specific strategies, let's review how identity management aligns with each of these goals.

"With the advent of social media, Web 2.0 and mashups, customers expect products to be delivered via non-traditional channels, including mobile devices, voicemail, email, web and chat."

Bank Systems & Technology, February 2011

[1]Fiserv 2010 Consumer Billing and Payment Trends Survey

Identity Management Driver 1:

FFIEC updates compliance requirements to fit the times

In October 2005, when the Federal Financial Institutions Examination Council (FFIEC) B introduced its "Authentication in an Internet Banking Environment" guidelines, electronic banking was largely done from a household or office computer. At that time, nobody could have predicted the proliferation of mobile devices with their rich "app for that" financial capabilities. Now it's expected that the number of Internet-enabled devices carried by the average consumer will double in the next few years. Thus, the simple device identification methods adopted by financial institutions in response to the 2005 guidelines have been rendered incomplete, as the customer may access services from a personal laptop, a work computer, a smartphone and/or a tablet.

Not only that, the Facebook phenomenon has been nothing short of extraordinary. Even formerly "private" people have been caught up in the excitement of sharing every detail of their lives with the world. As a result, the use of basic challenge questions, highlighted as a strategy in 2005 guidelines, is now discouraged in favor of more dynamic knowledge-based authentication (KBA).

Other key changes center on the use of layered security, whereby different controls are used at different points in a transaction process, compensating for the "weakest link." In particular, layered security controls should be designed to detect and respond to suspicious activity or anomalies related to:

- initial login and authentication of customers requesting access to the institution's electronic banking system; and
- initiation of electronic transactions involving the transfer of funds to other parties.

Javelin Strategy & Research's 7th Annual Banking Identity Safety Scorecard found that many top U.S. banks and credit unions continue to rely on outdated authentication practices. According to the FFIEC, it is recommended that financial institutions perform risk assessments at least every 12 months, and adjust their customer authentication programs accordingly to keep up with ever-changing technology and fraud mechanisms.

2011 FFIEC Guidelines	The LexisNexis Approach
Perform periodic risk assessments of your customer authentication controls based on threats.	Identification of gaps in your existing authentication processes.
Implement layered security techniques to strengthen the security of high-risk transactions.	Layered security can be implemented based on risk levels using multi-factor authentication technologies.
Detect fraud related to initial login, re-authentication, or electronic transactions.	Intelligence for more robust enrollment services.
Leverage more robust controls for assessing business transactions.	Business and consumer identity verification services – and fraud analytical capabilities to assess identity fraud risks.
Deploy more sophisticated challenge questions as an effective component to your program.	More effective controls – industry leading dynamic challenge based questions.

The Federal Financial Institutions Examination Council is responsible for developing uniform reporting systems for federally supervised financial institutions, their holding companies, and non-financial institution subsidiaries.

The cost of noncompliance

Financial organizations understand the need to remain compliant—but how do they achieve it? One of the keys to compliance is layered security – using different controls at different points in a transaction process so that a weakness in one control is offset by the strength of a different control. But any system is only as strong as those who use it. It is critical to involve your customers in your identity management program – successful financial organizations place emphasis on educating their customers to the potential risks posed by fraudsters, helping them understand the importance of the organization's fraud safeguards and arming them with the information they need to help protect themselves.

However, in today's rapidly changing business and regulatory landscape one of the most crucial elements to staying compliant and maintaining an appropriate level of security is to perform periodic risk assessments that take into account new and evolving threats to online accounts. Your organization should review and assess your solution frequently to identify security gaps, and refine those processes as needed.

Identity Management Driver 2:

Process Efficiency and Customer Delight

It's not surprising that bank customers quickly become frustrated by processes designed to prevent unauthorized account access and provide more streamlined service across departments. Instead of having customers fax over proof-of-address documents or endure long telephone hold times or voice-response systems, institutions will do well to automate manual or inefficient tasks that hinder the customer experience.

A robust identity management strategy should be scaled to cover a wide range of account management tasks, not just high-dollar online transactions. Consider any type of interaction that requires verification of a customer: new account origination, password resets, change of address requests, fund transfers, gift card reloading, accessing an account from a new or unrecognized device, check reorders, and the myriad other reasons a customer would access your institution on a regular basis. Think about the level of risk associated with each type of activity, and use controls consistent with that risk level.

> For example, customer George, who wants to access online banking to check his balances and verify that transactions have cleared, does not want to be subjected to the same amount of security rigor as Sally, who's opening a new account, or Fred, who is transferring money to his grandson's savings account. Yet, you owe it to George to have effective controls in place to protect his identity should someone else try to access his account and, you are obligated to meet regulatory obligations. At the same time, the controls need to be "friendly" enough that George can easily pass through the system, get the information he needs and be on his way without hassle.

It is important to implement proofing technology that makes the customer authentication process easier and more convenient. Not only will it improve the customer's experience and attitudes toward security controls, it will also reduce calls to the customer care center from frustrated account holders. There's no sense in implementing a technology to help reduce transaction costs to pennies on the dollar if it requires costly hand-holding (or causes you to lose the customer altogether).

Which method(s) of authentication should your institution use? It depends on your level of customer adoption, risk assessments and access channels. Ask yourself:

- What methods are my customers willing to adopt?
- What am I trying to protect?
- What do I consider to be high risk or high value transactions?
- What channels do my customers access?

Identity Management Driver 3:

Preventing Unauthorized Access and Fraud

According to a McKinsey & Company report[3], financial institutions lose an estimated $5-7 billion annually due to fraudulent access to demand deposit accounts. A poor economy reinforces the will of a clever fraudster, but the consumers' appetite for technology has only bolstered the ability for dubious activity to occur. Some sobering points:

- **There are currently more than 5 billion Internet-connected devices in use worldwide[4].** That's a massive number of PCs, smartphones and tablets carrying personal information. And a huge number of doorways for fraudsters to hack through, especially when handheld devices are stolen or left behind on a bench or subway.

- **As of March 2012, there are 900 million active Facebook users[5].** Consider the volume of personal information that can be uncovered by monitoring a Facebook user's page: Birthdate. Pet's names. Schools attended, with mascots and graduation dates identified. Relatives' names. Anniversary dates. Any of this information can be used to piece together an account holder's password or to set up a new account.

- **The bad guys are getting smarter.** Downloadable kits feature complicated attack tools that even the novice fraudster can negotiate with minimal effort. Malware can be surreptitiously installed on an unsuspecting user's PC, monitoring their every keystroke including login credentials.

Improved layered security can reduce the incidents and subsequent dollar loss associated with account takeover fraud. The objective of fraud teams should be to reduce not just individual incidents but the overall rate of incidents. This requires measuring the success of a particular authentication technique.

> Let's say you require a telephonic password reset when the consumer fails five password attempts to log on to her account. Out of the total number of telephonic password resets that occurred in a year across your online account base, how many resulted in a fraud incident within two months of the authentication? This gives you an incident rate. Calculate the rate in a similar fashion across all channels.

Of course, as pointed out earlier, fraud experts are under enormous pressure to mitigate losses without sacrificing customer convenience. Benchmarks that measure things like customer abandonment rates help paint the picture of how balanced the solution is in minimizing the frustration of security. For example, when a financial institution first puts a new system or technology in place, 20% may be an acceptable abandonment rate for them. (Meaning that for every 100 customers who attempt a transaction, 20 of them will give up prior to completion.) However, over time that organization will want to see the abandonment rate decline as the system gets better and customers become more familiar with it. If they are not seeing an improvement in their abandonment rate, they may need to reassess the system and make adjustments to optimize it for their business needs and the way their customers interact. Teams that track these kinds of statistics are better able to hone their systems and processes and have the added benefit of proving the solution's ROI and the value of more automated authentication processes.

Keep in mind that peace of mind is also a valid business goal. Even if your firm has the ability to cover a monetary loss, the customer's trust in your institution will evaporate the minute their account is hacked. Vigilance is never too costly.

---

[3] "Risk, Loss and Mitigation Survey," McKinsey & Company
[4] IMS Research, Press release: "Internet Connected Devices About to Pass the 5 Billion Milestone," August 2010
[5] Facebook Company Info, cited June 2012, newsroom.fb.com/content

Use Cases

Financial institutions have numerous options for identity proofing and authentication. Many financial organizations are familiar with knowledge-based authentication and have used it for years. However, as discussed previously, there is a movement away from static KBA (prompting a user to recall information they provided upon account set-up) in favor of more dynamic KBA that requires a user to answer "out of wallet' questions that would not typically be publicly available. Often, dynamic KBA also includes a "red herring" question that stumps would-be fraudsters, but which the legitimate customer will recognize as nonsensical.

Some organizations are also beginning to explore biometrics. While still in the early stages of adoption, biometrics—such as voice biometrics, fingerprint and keystroke tracking—are proving a useful tool in their identity proofing system. By their very nature, as "something you are", they are immediately accessible to the customer and are harder to fake than other authentication methods.

In the end, the specific methods you choose depend heavily on your business processes, your customer interaction channels and the types of transactions performed. Here are some examples of strategies being employed today.

Voice biometrics has been around for decades, and has been used by financial services institutions elsewhere in the world. However, it's relatively new to U.S. institutions.

Voice Biometrics

A $2.8 billion, 337,000-member credit union in Phoenix evaluates its service channels and concludes that they need a new solution to quickly and efficiently help process their high call volume. They choose a sophisticated voice biometrics system in their call center to authenticate customer identity at four stages:

- Final approval when establishing a new account;
- Account access for routine inquiries;
- High-risk ACH transactions and wire transfers by business members; and
- Password reset.

Prior to even creating a voice print, the customer's identity is first verified through other means to ensure the person creating the voice print is the specific person they say they are. To establish the voice print, the credit union member calls the system and leaves a scripted voice mail that takes less than a minute to complete. During this process, the unique characteristics of the individual's voice are then extracted mathematically and put into a voice template. The member then gets a call back and a brief verification process takes place.

After that, everything is good to go and subsequent phone transactions can be completed with fewer barriers to the customer, and lower costs and call times for the credit union's call center.

Dynamic KBA

A large bank provides mobile access for all its customers including banking, credit and mortgage customers. A customer calls in to make a change on his mortgage account and is prompted by the system to provide his name, last four of his SSN, address, DOB and either the exact mortgage amount, or the full mortgage account number. The customer is away from home and does not have the necessary mortgage information required, so then has to wait for a Customer Service Representative.

The first rep he speaks to handles general banking customers and since the bank doesn't have a single view of the customer across all his accounts, he must be transferred to a representative in the mortgage area. The rep transfers him to a mortgage customer service rep, who then tells him she can't help unless he has one of those pieces of information. Frustrated, the man hangs up and has to delay his business until another time when he has the required information on hand.

Now imagine this scenario if the bank had a more robust authentication solution on-hand. If he could not supply the specific mortgage information required, after providing his name and DOB, he could be given a series of dynamic challenge questions. If he answers them all correctly, he could be passed through the system without additional live assistance, or subsequent callbacks to resolve the issue. This would not only reduce frustration and improve satisfaction for the customer, but also increases same call resolution and decreases operating costs.

Out-of-Band Authentication with One Time Password

An increasingly popular anti-fraud measure for online banking is out-of-band authentication implemented with a one time password. Let's say Kathryn wants to transfer funds to her retirement account. When she initiates the request online, a text message or phone call is sent to her mobile phone number (on file with the bank). Through that call or text, Kathryn receives a one time password that must be provided on her bank's website to complete the transaction.

The same process could be used to add an authorized user, to complete a wire transfer, or for any number of other sensitive transactions. Pairing a one time password with the customer's existing log-in info (user name and password) layers the security and enables the organization to protect the transaction while providing very little to no additional friction to the process.

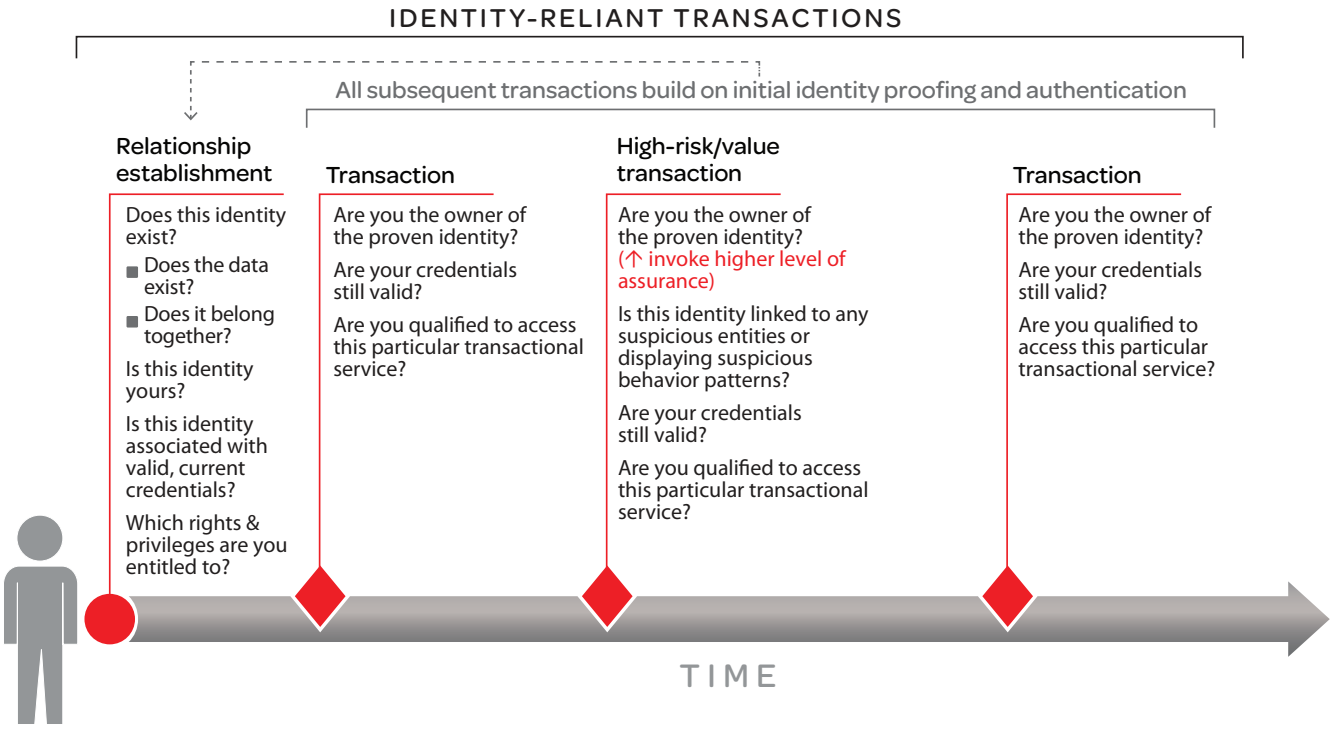
Identity management is an ecosystem...not a quick fix

Robust identity management is not a matter of having one specific piece of information or foolproof challenging question. It's about having access to different types of information and putting them together to authenticate a person's credentials. The ability to "link" these different pieces of information to a single identity assures the customer's identity in ways that a SSN or other single piece of ID cannot.

Going from strangers to a lifelong relationship, in real time

The "secret sauce" of a robust Identity management system is the accumulation, in real-time, of 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 a high degree of 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 and regulations that govern data sharing and retention.

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. (Remember our customer George above.)



This might cause some heartburn among security personnel who aim to reduce risk by restricting access. But with the sophisticated, flexible solutions available today, you can appropriately manage the different types of transactions that occur at various points in customer lifecycles.

Identity Proofing Fundamentals: An introduction

The identity proofing capabilities we've described in this paper can be integrated to existing financial services 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 institution from having to keep up with changing technologies.

Whether installed or hosted, 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 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 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 consumer'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 management functions. It's the key to turning raw data into information relevant to a particular transaction. And because data linking provides a more robust insight into the identity 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 a high degree of 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.

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 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 to help you make high volumes of complex decisions.

Rules that you configure within the identity proofing solution enable you to quickly determine 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, you can configure the system to challenge the person 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, financial institutions 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 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 frameworks and methodologies, such as OpenID Exchange and Microsoft's Open Identity Trust Framework.

Financial service institutions can't afford another blow to the bottom line.

As cases of identity theft rise and regulations continue evolve, now is the time to examine and strengthen your identity management protocol. Forward-thinking financial institutions have realized that a robust, dynamic knowledge-based strategy is the most effective approach for addressing customer convenience while managing transactional risk and maintaining compliance.

Call us today to see how LexisNexis can help you create a layered security solution that enables your business processes and protects your customers—and your reputation and bottom line.

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

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, 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 leading publisher and information provider that serves customers in more than 100 countries with more than 30,000 employees worldwide.

LexisNexis®