The Role of Knowledge Based Authentication (KBA) In Identity Proofing

Knowledge Based Authentication [KBA] is not just for onboarding new customers

December 2013
Best Practices for maximizing affordable, low-friction KBA to help prevent fraud in virtually every industry

Several generations ago families routinely left their front doors unlocked and their car keys in the glove box. But today it’s not uncommon for homeowners to live in gated communities and subscribe to home security services that monitor break-ins in real time.

At a considerably elevated level, businesses have been forced to travel a similar road regarding cyber security. The difference is that companies are faced with far higher financial stakes, a dizzying array of identity proofing options and the need to balance privacy, security and convenience. (Customers value all three attributes but, all too often, convenience trumps everything else.)

In general, identity proofing—the process of vetting an identity to confirm its validity and ownership claim—is critical for businesses to combat fraud and improper payments. Knowledge based authentication (KBA), as a component of a comprehensive identity proofing process, has great utility as a crucial layer of an organization’s identity management solution. While KBA is already recognized as a potential first line of defense against fraudsters, we will explore how businesses can continue to harness this cost-effective, low-friction tool throughout the customer lifecycle to drive better compliance, improve risk and ensure a more profitable, secure relationship.
Identity Proofing 101

When opening a new customer account or creating new user credentials, companies typically use a combination of approaches to understand who an applicant really is. Different types of identity proofing solutions are leveraged based on the risk tolerance of the transaction, but there are a few key components that are universally employed.

For many companies, the first layer of identity vetting consists of some sort of Fraud Risk Decisioning (Step 1). This can include looking at where the transaction originated, identification of the access device and IP geolocation to determine a risk profile. The company then begins an Identity Proofing process (Step 2), which uses various components to resolve to a unique identity with the identity attributes collected based on the identified risk profile of the transaction. Finally, the identity attributes could be checked among internal or external databases to verify the relationship between the individual data components – does the name and address or name and phone number belong together or was the correct date of birth provided?

This multi-faceted process benefits from additional layers of security that can be independently leveraged or combined together in order to provide the customized level of security and user-friendliness needed in any particular situation. When implemented correctly, solutions such as knowledge based authentication can provide a higher level of assurance that those identity attributes collected actually belong to the individual asserting or claiming the identity.
The Role of KBA In Identity Proofing

KBA is an indispensable tool in a multi-layered Identity Proofing solution

KBA is offered in many formats, making it a valuable, flexible weapon in the cybersecurity arsenal. The different authentication protocols involve “static questions” where the user sets up an account by supplying a fixed answer; e.g. “In what city were you born?”. This is in opposition to “dynamic” authentication, which generates a multi-variable prompt such as: “Which of the following streets have you NEVER lived or used as your address?” These dynamic questions provide randomized right and wrong answer choices based on data found for the subject by the KBA solution.

Dynamic KBA can be made more effective because of the depth and breadth of questions which reference both current and historical information. The data used to generate these questions should include sources that are generated through non-traditional or “alternative” data in order to capture customers who may not have traditional credit profiles. Sophisticated challenge question systems usually require that the customer correctly answer multiple questions and could include a diversionary question that is designed to trick the fraudster.

Identity proofing solutions are often deployed as a stand-alone in a business process, but these solutions are most effective when paired together. When dynamic KBA is paired with identity verification, an organization can first determine if the identity elements exist together and if there are any mismatches of data elements. Depending on the individual risk profile generated by a verification failure, the system could be signaled to not generate a KBA quiz and instead have the customer go through an alternate process to provide further documentary evidence. This balance between ease of access and security should be automatically adjusted, allowing verified customers to pass through uninhibited while stopping fraudsters in their tracks.

What to look for in a KBA solution

The most effective KBA solutions use a wide-ranging set of data sources to create a unique set of dynamic questions about an identity to verify that the individual on the other side of an online, mobile, or phone-based transaction is not an imposter. These data sources need to take into account populations that may not have typical credit profiles, referred to as thin credit customers, such as those in younger demographics.

Solutions that can incorporate proprietary customer information that you may already have into quiz questions provide a more secure authentication process. These types of questions can be based around when you last accessed an account and other account type information. Some solutions also provide the ability to correlate a consumer’s KBA activity with recently accessed public record information that could assist them in taking a KBA quiz, as well as built-in security features such as velocity checking to ensure the quiz cannot be taken more than a certain number of times.
KBA is used virtually everywhere

How KBA is Used Across Industries

Government
- Before providing disaster, unemployment or other financial assistance benefits.
- Before issuing tax refunds and in protecting sensitive documents, such as a copy of a birth certificate.

E-commerce
- Online retailers use KBA during account signup, password resets, adjusting account settings, or when conducting high-value transactions.
- Cable and utility companies authenticate identities prior to changing account information in order to ferret out users who attempt to assume new identities to avoid paying late fees or reconnection fees.

Financial services
- Used during remote account opening, re-opening or to authorize major account changes.
- Prior to processing high-risk transactions, either by policy (e.g., all balance transfers over $1000 and all password resets), or by predictive risk assessment.
- Prior to processing loan applications to avoid the costly and time-consuming loan process on a fraudulent applicant.

Healthcare
- With the growth of online portals, the ability to confirm patient and provider identities with KBA while accessing health information is an important part of protecting personal health information in compliance with HIPAA.
- It is also crucial for authenticating consumers prior to granting remote access to medical records or approving a medication refill.

Insurance
- Before issuing a policy, making changes to a policy, as well as allowing vetting of a policyholder when they apply for online access to view or modify a policy.
- During a high-risk transaction, such as the password-reset process or adding supplemental coverage.
KBA: A crucial layer to your Identity Proofing solution

KBA is a cost-effective solution for identity proofing: Best-of-breed automated KBA solutions provide a significant savings over manual identity verification processes. For example, many retail pharmacies use the technology to securely handle online prescription management. To date, some 10 million patients have participated in online prescription services, saving countless hours for pharmacy staff and allowing them to focus on their core business.

KBA is reliable for identity proofing: KBA quizzes try to provide questions that can be easily answered by the person being authenticated. However, because of the diverse information presented in KBA quizzes, sometimes good customers don’t get all the answers right because they forgot the answer to a question. The good news is that fraudsters are up to seven (7) times more likely to fail a quiz than honest customers with poor memory. For example, in the retail pharmacy space, where pharmacists are faced with the tasks of enhancing convenience while protecting access to the sensitive medical information of their customers, the use of KBA has shown very high pass rates (nearly 85%), with a very low percentage of customers failing the KBA quiz or abandoning/opting out of the proofing process altogether. Companies can continue to improve this rate with configuration changes, but it is important to balance the issue of making a quiz too difficult for honest customers while keeping fraudsters at bay.

Strong configuration setups for KBA are essential to stop fraud: There are many best practices in place to prevent fraudsters from getting through a quiz. Features such as stringent timeouts, velocity checking and diversionary questions help ensure that fraudsters aren’t able to defeat the quiz, or are routed into even more secure authentication methods. How you set up the quiz is just as important—making sure customers answer enough questions and not just one or two to pass, not including more than one diversionary question, having different types of diversionary questions, making sure historical questions are asked and not just current questions, etc. KBA solutions that provide strong professional services can consult with you to ensure best practices and deliver a strong KBA program without causing customer friction.

Easy-to-implement KBA does not cause customer friction: KBA provides convenient services online on a mobile device, in an IVR, or over the phone in a call center that many consumers would otherwise have to pursue in person. Users may opt out of taking the quiz and use alternative authentication methods, but on average 5% or fewer choose to do so. KBA can be easily implemented and flexible to accommodate customers’ on-boarding business processes as a component of a layered approach to identity authentication.

Strong, efficient identity proofing solutions are at your command when KBA is part of the toolkit.
KBA as part of a layered security approach helps prevent fraud

No identity management system should exist in a vacuum. To deliver the flexible, robust identity proofing solutions needed by companies across the business spectrum, a layered approach must be implemented. KBA solutions from LexisNexis can provide another layer to your current solution in order to provide a user-friendly interface paired with an indispensable, robust fraud-blocking tool.

Authoritative boards, such as the Federal Financial Institutions Examination Council [FFIEC] for the financial services industry, have issued guidance advocating the use of dynamic KBA as part of a layered approach for authentication. This agency, like many others, believes the use of sophisticated KBA technology can be an effective component of a security program.

The right KBA solution can be part of a highly effective layered security program that meets your business needs while reducing customer friction. Call LexisNexis today to learn more about the powerful benefits of implementing KBA in your organization.
For more information
Call 866.887.8343, visit lexisnexis.com/risk/identity
or email us at idmanagement@lexisnexis.com.

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, we provide products and services that address evolving client needs in the risk sector while upholding the highest standards of security and privacy. LexisNexis Risk Solutions is part of Reed Elsevier, a leading publisher and information provider that serves customers in more than 100 countries with more than 30,000 employees worldwide.

Our retail solutions assist organizations with protecting revenue, maximizing operational efficiencies, and predicting and preventing retail fraud.