BANK INFO SECURITY®

FFIEC Authentication Guidance: The Case for Knowledge-Based Authentication
By Monica Pearson, Senior Product Manager, Fraud and Identity Solutions, Experian Decision Analytics
Monica Pearson
October 17, 2011

The latest guidance issued by the Federal Financial Institutions Examination Council draws a line of clear distinction between the **types of knowledge-based authentication available** - from static challenge questions, such as those derived from customer enrollment information, to dynamic KBA sessions that serve as part of more complex out-of-wallet identity verification procedures.

Challenge questions

Acknowledging that many institutions use challenge questions as a backup when the primary logon authentication technique becomes inoperable or when it becomes necessary to reauthenticate for a specific transaction, the FFIEC guidance emphasizes that implementation of challenge questions can greatly impact efficacy.

Of greater importance is that the FFIEC guidelines caution on the use of information that can be easily guessed or obtained from an Internet search, given the amount of information available, particularly on social networks. This does not mean dynamic KBA has been called into question. In fact, if the FFIEC guidelines are read carefully, the opposite is true.

Out-of-wallet identity verification

"Challenge questions can be implemented more effectively using sophisticated questions," the guidance states. "These are commonly referred to as out-of- wallet questions that do not rely on information that is often publicly available."

The FFIEC guidelines call for a move toward more sophisticated question tools rather than the use of static "secret questions." Static challenge questions should no longer be used as a primary control, as they cannot be part of an effective risk-mitigation technique. Again, the FFIEC guidelines call for questions that "do not rely on information that is often publicly available," making reliance on a broad range of data assets to the base questions necessary. This is an area KBA users should review carefully. It is perfectly appropriate to ask, "Does my KBA provider rely on data that is publicly sourced?" If you aren't sure, ask for and review data sources. Look for a broad range of data types: first-party and purchased, as well as both credit and noncredit, where permissible purpose exists.

Sophisticated KBA systems

Finally, the guidance speaks to the use of more sophisticated question tools - those with the ability to pose multiple questions within the question set and that include a "diversionary" question designed to trick the fraudster. However, a **truly sophisticated KBA system** will do even more. It will be designed for customizable delivery of a broad set of questions, with features that enhance the consumer experience while reducing client fraud risk.

To enhance the customer experience, such a KBA system will provide features to allow a customizable question wording feature that formats question text to the target audience and maintains control over question order. Sophisticated KBA systems can control both question presentation and the question process or session flow - so "good" consumers move through the process more quickly, while fraudsters become "outsorts." The customer experience features drive the difference between sales and abandonment rates.

The fraud risk features associated with a sophisticated KBA system typically include the ability to control the questions presented based on multiple criteria, as well as the ability to exclude questions globally or once the question has been presented to a particular consumer. Additionally, they make use of configurable settings designed to control system access. These "velocity checks" and "use limits" create a protection barrier when consumer behavior crosses a predefined risk threshold.

Following a **risk-based approach to authentication**, cross-referencing a customer's question performance with other risk attributes, such as a fraud score or an authentication score, generally will provide the most useful decisioning criteria and enable a more complete view of a specific consumer transaction. "Question weighting" is another method used by more complex KBA systems to focus greater emphasis on more difficult questions. The more difficult the question, and the higher the fraud separation, the higher the weight assigned to the question, where the fraud separation is the difference between the true consumer's ability to answer correctly and a fraud artist's ability to answer correctly.

Experian® consults with clients to find the optimal process points and question session configuration to strike the right balance among the often opposing forces of fraud prevention, customer experience and cost. Any institution should consider, at a minimum, the following best practices when evaluating an out-of-wallet question service provider and implementation:

- Questions founded in as diverse a universe of data categories as possible, including credit and noncredit assets, if permissible purpose exists;
- Consumer question performance as an element among many within an overall risk-based decisioning policy;
- Robust performance monitoring via established key performance indicators associated with individual question performance and overall policy effectiveness;
- An established process to rotate questions and adjust access parameters and velocity limits at the institution and consumer levels.

Providers who offer only static challenge questions will no doubt feel their business is threatened, as will those who rely wholly on publicly sourced data. However, there are providers who meet the test of the new FFIEC guidelines and welcome the opportunity to demonstrate how. When evaluating a provider, consider that the return on investment associated with out-of-wallet questions is often most compelling when the evaluation includes not only fraud prevention, but also customer experience and cost savings (in lieu of more manual customer management processes). Some of these values may be considered soft costs or less quantifiable, but they are quite real.

Monica Pearson is a Product Manager accountable for identifying and evaluating new market

opportunities as well as developing and executing long-term product strategy. She currently manages the Experian knowledge-based authentication practice, including Knowledge IQSMSM and the Authentication Services level 3 product as well as the Fraud and Identity Solutions' consortium database strategy, including the National Fraud Database. Pearson enjoys public speaking and has presented at Experian's Vision conference in addition to industry events, such as the Merchant Risk Council "eCommerce and Payments and Risk Conference" and other partner advisory forums. She's a published poet and enjoys kayaking and stand-up paddle boarding.

Pearson holds a Master of Business Administration with an emphasis in marketing from California Lutheran University.

Close Window
