Get the Facts on Identity Theft
According to the Consumer Sentinel Network (CSN), the number of identity theft complaints has doubled over the last five years with more than 279,000 identity theft complaints filed to the Federal Trade Commission (FTC) in 2011.

Consumers are demanding more convenient, real-time, self-service options for account creation, management, and activity. As a result, organizations have implemented online and call center practices. Through these channels, businesses have seen reduced costs, increased efficiency and discovered opportunities to offer new services. These advantages, however, also come with risks, specifically the risk of fraud and identity theft.

RSA® Identity Verification, from LexisNexis, is a strong consumer authentication and fraud prevention service that validates user identities in real-time, thereby reducing the risk associated with identity impersonation. Utilizing Knowledge-Based Authentication (KBA), RSA Identity Verification challenges users with a series of top-of-mind questions generated from information within databases containing billions of public and commercially available records. With industry-leading speed and accuracy, RSA Identity Verification conveniently confirms identities within seconds, without requiring an organization to have a prior relationship with the user.

Figure 1: RSA Identity Verification Balances Business, Solution, & End User Requirements
Key Benefits

By using RSA Identity Verification to authenticate customers, businesses can reduce operational costs and fraud losses, increase efficiency and revenue, meet regulatory standards, and enhance overall user experience. More specifically, RSA Identity Verification:

- **Reduces operational costs** by improving and automating existing manual processes, creating a consistent authentication method across the organization in web, point-of-sale terminal, and call center channels.

- **Increases number of new accounts opened** by providing a faster authentication process in which businesses can approve more account openings and process more transactions.

- **Reduces fraud** with a deeper level of identity authentication thereby preventing those with stolen documents from establishing new accounts and conducting transactions – dramatically reducing the losses associated with fraud and identity theft.

- **Helps meet compliance requirements** in the Bank Secrecy Act and the PATRIOT Act Section 326 for implementing Know Your Customer policies in addition to compliance with FACTA Red Flag guidelines.

- **Enhances the user experience** with real-time, accurate, non-invasive questions providing instant authentication and access to user accounts.

Key Features

Flexible Configurations

RSA Identity Verification is a flexible solution that can be deployed at several touchpoints across the organization – from the web to the point-of-sale terminals to the call center. RSA Identity Verification offers configuration options which can be customized and continuously fine-tuned based on the unique needs of each business, their activities, and the associated sensitivity to the activity. Real-time configuration adjustments include the ability to:

- Determine number of questions presented and score needed to pass

- Modify system behavior based on predetermined triggering events

- Terminate the authentication process or issue warnings based on a multitude of conditions and risk factors

Seamless Integration

Built on a universal ASP platform, RSA Identity Verification can be deployed seamlessly – without integration complexity or costly disruption of client-side information systems. For call centers and retail service agents, there is an easy-to-use web portal that provides turnkey authentication processing. For websites or other external-facing channels, the solution can be seamlessly integrated with RSA Identity Verification viva a SOAP (Simple Object Access Protocol) interface.

Static Challenge Questions vs. Dynamic KBA Questions

Static challenge questions verify an identity by asking one or more personal questions based on information supplied by the end user during account or profile creation. The use of challenge questions may be “good enough” in some cases and tend to be more acceptable for low risk transactions. However, basic consumer supplied data only goes so far and is readily compromised by identity thieves. The increased use of social network sites is providing more access to typical responses to challenge questions such as hometown, high school, university, pets, favorite food, favorite book, favorite music, etc.

Dynamic KBA questions verify an identity by asking top-of-mind questions generated on the fly based on publicly and commercially available data sources, requiring no previous contact or relationship with the end user. To initiate the process, basic identification factors such as name, address and date of birth must be provided, and then questions are generated in real-time from the data records corresponding to the individual identity provided. KBA questions are sometimes referred to as out-of-wallet questions as the knowledge needed to correctly answer the questions is not held in a wallet and therefore very difficult for anyone other than the actual identity to know.
How it Works

The RSA Identity Verification service has several components including Identity Proofing, Fraud Indicator Checks, Risk Assessment, and Authentication.

Identity Proofing

During Identity Proofing, RSA Identity Verification matches data provided by or about the user to data found within public or commercially available records. It can also perform various data checks, such as a check against the Specially Designated Nationals (SDN) list published by the Office of Foreign Asset Control (OFAC) and other global watch lists. If there is no match within the public or commercial records, RSA Identity Verification indicates that the user cannot be located, and the authentication process is terminated. If a match is found and the identity passes other configured data checks, then the authentication process continues.

Identity Fraud Monitoring

An organization can configure RSA Identity Verification to perform a check against velocity or volume of activity associated with an identity within a short timeframe to spot patterns indicative of fraud. Based on the outcome, an alert can be sent, or the authentication process can be terminated.

Authentication

RSA Identity Verification is fueled by Intelligent Questioning technology which is designed to logically develop correct and incorrect, sometimes referred to as “Red Herring,” questions and answers using actual consumer data in real-time. These questions are presented to the end user, and based on the accuracy of their responses they successfully pass or fail the authentication.

FFIEC Guidance: Authentication in an Internet Banking Environment

The FFIEC guidance, Authentication in an Internet Banking Environment, was first released in 2001, and updated in 2005 and again in June 2011. The guidance outlines risk management controls necessary to authenticate retail and consumer customers accessing internet-based financial services. The 2011 supplement calls for continuous risk assessment and layered defense wherein organizations use different controls at different points of the transaction so that a weakness in one control is compensated by the strength of another. One of the controls highlighted includes challenge questions. The FFIEC feels as though institutions should no longer rely on traditional static challenge questions as a primary control. Instead, dynamic KBA or “out of wallet” questions that rely on data that is not easily accessible by the public, and provide multiple questions without exposing all of the questions in one session, are more effective.

Figure 2: RSA Identity Verification in Action
Use Cases

There are a number of use cases to which RSA Identity Verification can be applied. The most common use cases include:

- Call Center Identity Verification
- Account Origination & Enrollment
- Automated Self-Service for Accounts
- Password Resets
- High-Risk Transactions
- Exception Handling
- Authentication for Infrequent Users
- Compliance with KYC (Know Your Customer)
- Compliance with FACTA (Fair and Accurate Credit Transaction Act)
- Compliance with FFIEC Authentication in Online Banking Environment Guidance

Conclusion

Organizations require authentication solutions that are fast, accurate, and secure, conveniently confirming identities while eliminating the risk of fraudulent activity such as account takeover or compromise. The solution must provide strong authentication with little or no impact on the end user; a solution that is too invasive or difficult to use may cause high levels of abandonment and a decrease in user satisfaction. RSA Identity Verification delivers strong authentication that is not only accurate, secure, and user friendly, but also delivers operational and cost reduction benefits to an organization through automation of existing manual processes.