RSA SOLUTIONS TO ADDRESS THE FFIEC GUIDANCE

Manage Risk and Reduce Fraud in Online Banking

Solution Brief
RSA has shut down over 450,000 phishing attacks.
RSA has shut down over 80,000 Trojan attacks.
Phishing increased 27% in 2010.
More than 20 million malware strains were developed in 2010.

On June 28, 2011, the Federal Financial Institutions Examination Council (FFIEC) released a supplement memorandum to the “Authentication in an Internet Banking Environment Guidance” letter originally issued in October 2005. The FFIEC has recognized an evolution in the threat landscape and is concerned that customer authentication methods and controls implemented in conformance with the original Guidance have become less effective.

This latest memo to regulated financial institutions reinforces the risk management framework originally described during the boom in Internet banking. It includes certain “supervisory expectations” on how financial institutions should protect online customers and transactions and updates the FFIEC’s expectations regarding customer authentication, layered security, and other controls in the increasingly hostile online environment.

High-Risk Transactions Require More Protection

The FFIEC Guidance recognizes that not every online transaction poses the same level of risk, and therefore recommends that financial institutions should implement more robust controls as the risk level of the transaction increases. The FFIEC Guidance calls for layered security which includes risk-based fraud detection and monitoring systems which enable out-of-band, multi-factor and step-up authentication for high-risk transactions. Layered security should include systems that consider customer history and behavior, out-of-band verification, multi-factor authentication for business customers, and techniques to appropriately limit the transactional use of the account.

RSA Solutions for Protecting High-Risk Transactions

RSA Adaptive Authentication is a risk-based authentication and fraud detection platform that measures over one hundred indicators to identify high-risk and suspicious activities. RSA Adaptive Authentication can detect and understand the patterns and risks associated with individual transactions or activities after a user has logged in and uses this historical data to determine the level of risk associated with a user’s current activity. For high-risk transactions, a number of additional authentication methods can be supported within RSA Adaptive Authentication, including out-of-band phone, email and SMS authentication, knowledge-based authentication (i.e., “out of wallet” questions) and one-time passwords, to ensure multiple security layers for fraud prevention. In addition, RSA Adaptive Authentication allows custom rules and policies to be applied to limit transactional use of accounts.

Security Should Align with Risk

While authentication of the customer with passwords, challenge questions, one-time passwords, and other methods present the first layer of security for users logging in to an account, additional layers of security and controls are necessary to ensure that first layer of authentication has not been compromised. Advanced threats such as keyloggers and malware are capable of capturing the data used to authenticate a user at login – many can do this in real-time. In order to prevent fraud at the transaction level, The FFIEC Guidance recommends financial institutions should implement layered security and other controls that are commensurate with the magnitude of the information security and transaction risk.

RSA Solutions for Risk Management of Bank Transactions

RSA Transaction Monitoring is designed to identify activity in a customer's account that is anomalous to that customer's unique behavior. RSA Transaction Monitoring builds a unique profile of each customer's online and account behavior over time and compares it to current activity to identify accounts that may have been compromised. Examples of patterns of behavior analyzed include: time of day; day of week; geo-location; device
type and characteristics; password resets; check viewing; bill pay, ACH, and wire transfer
set up and origination; transaction amount, payee alteration; changes to email, address,
and phone numbers; and call center inquiries. RSA Transaction Monitoring allows
financial institutions to set custom policies according to their risk threshold.

The RSA Archer Continuous Monitoring solution automatically collects, analyzes, and
manages data across segregated tools and groups such as vulnerability scanners,
configuration agents, directory services, compliance scanners, and from “in-person”
control assessment questionnaires. Risk and controls associated with this monitoring can
be scored and items exceeding assigned risk tolerances can be reported to appropriate
individuals for remediation and monitoring.

The RSA Archer Compliance solution provides a framework to document and monitor
internal controls and can be used to comply with this FFIEC Guidance by regularly
obtaining management’s reaffirmation that applicable controls are operating. Examples
of controls include: management’s monitoring and response to security exceptions;
implementation and operation of customer limits, customer’s use of certain security
devices and procedures, and enforcing customer’s use of dual control based on privilege
level and volume and value of customer information and transactions; and security
reviews of new and materially changed internet services. Combined with the RSA Archer
Risk Management solution, compliance with the FFIEC Guidance can be managed and
demonstrated from the point of risk assessment through compliance.

Simple Challenge Questions and Device Authentication are Not Secure

Simple challenge questions can often be easily answered due to the amount of
information about people that is readily available on the Internet and social networking
sites. Therefore, the FFIEC believes that basic challenge questions as a primary control is
no longer an effective risk mitigation technique and more sophisticated “out of wallet”
questions should be implemented.

The FFIEC Guidance also challenges the effectiveness of simple device identification
as it can be easily impersonated by a cybercriminal. The FFIEC believes complex device
identification to be more secure and preferable to simple device identification.

RSA Solutions to Address Limitations of Challenge
Questions and Simple Device Authentication

RSA Identity Verification is a strong authentication and fraud prevention service that
validates user identities in real-time, thereby reducing the risk associated with identity
theft or impersonation. Utilizing knowledge-based authentication, RSA Identity
Verification challenges users in real-time with a series of top-of- mind questions
generated from information contained within databases containing billions of public and
commercially available records. RSA Identity Verification also performs a variety of checks
to spot patterns indicative of fraud, such as identity velocity checks and IP flagging,
allowing organizations to adjust authentication questions to the level of risk associated
with an identity.

RSA Adaptive Authentication leverages the RSA Risk Engine which performs complex
device identification to meet the requirements of the FFIEC Guidance. The device
identification process looks at a diverse set of data to establish the authenticity of a
device including tracking device characteristics that are a natural part of any device (HTTP
headers, operating system versions browser version, languages, and time zone), the IP
address and enriching it by extracting IP geo-location details and additional information
such as the ISP, IP owner, and connection type, and actively introducing additional
identifiers through the use of a cookie and/or a flash shared object (also referred to as
“flash cookie”) which serve as more unique identifiers of the device.
**Periodic Risk Assessments are Critical**

With the rapid pace in which cybercriminals change their attack methods, periodic risk assessments are necessary to manage risk and fraud levels in response to new threats to online banking. The FFIEC Guidance recommends financial institutions consider multiple factors including changes to the electronic banking environment, changes to the customer base adopting electronic services, or actual incidents of data breaches, identity theft or fraud. In addition, the FFIEC Guidance requires that risk assessments be updated as new information about threats becomes available, prior to implementing new or significantly changed online banking services, or at least every twelve months.

**RSA Solutions for Ongoing Risk Management**

The RSA Archer Risk Management solution provides a framework for information security risk managers to document the information security environment, perform periodic risk assessments as needed, and manage gaps in the control environments. RSA Archer Risk Management can also be used to document and manage the resolution of risks associated with new and materially changed products and services delivered online. This framework integrates with other IT-GRC and eGRC initiatives as well as enabling awareness and consistency with organizational policies, procedures, and controls.

The RSA FFIEC Guidelines Assessment and Strategy Service helps financial institutions comply with the updated guidance regarding securing online financial applications and activities. This service provides seasoned, expert consultants to help define an organization’s FFIEC strategy, build the business case, create the roadmap and gain the organizational consensus necessary to approve, fund and initiate changes as well as educating the end user.

Today, RSA’s Identity Protection and Verification solutions are used by over 8,000 financial institutions to protect more than 350 million end users and have secured more than 20 billion transactions. For more information on the FFIEC Guidance and how RSA can help your institution ensure compliance by the January 2012 deadline, please visit www.rsa.com/bankingsecurity.

**About RSA**

RSA is the premier provider of security, risk and compliance solutions, helping the world’s leading organizations succeed by solving their most complex and sensitive security challenges. These challenges include managing organizational risk, safeguarding mobile access and collaboration, proving compliance, and securing virtual and cloud environments.

Combining business-critical controls in identity assurance, data loss prevention, encryption and tokenization, fraud protection and SIEM with industry leading eGRC capabilities and consulting services, RSA brings trust and visibility to millions of user identities, the transactions that they perform and the data that is generated.