Introduction

The Federal Financial Institutions Examination Council (FFIEC) recently released a Supplement to its 2005 publication entitled Authentication in an Internet Banking Environment (Guidance). The 2005 Guidance provided a risk management framework for financial institutions offering Internet-based products and services to their customers.\(^1\)

The purpose of the recent Supplement is to reinforce the original Guidance’s risk management framework and update the Agencies’ expectations regarding customer authentication, layered security, or other controls in the increasingly hostile online environment.\(^2\)

The Supplement has identified a compliance date of January 1, 2012 at which time bank examiners will be looking for adherence to FFIEC guidelines.

These guidelines from the FFIEC come on the heels of a recent ruling in the U.S. holding a bank responsible for fraudulent losses from a business account. Traditionally, liability for funds stolen online has remained with the business banking customer. However, the court ruled that the bank has a responsibility to protect its customers through the use of fraud detection mechanisms.

The court ruling, coupled with a host of mass data breaches and token compromises, highlight the banks’ need to evaluate their security and risk management plans in the online banking environment.

Accordingly, ACI is providing a response to the FFIEC Supplement to walk readers through the guidelines and to provide options for adhering to the requirements within.

\(^1, 2\) Supplement to Authentication in an Internet Banking Environment, Federal Financial Institutions Examination Council’s Supplement, June 2011
## FFIEC Supervisory Expectations

### Risk Assessments

| Financial Institutions (FI) should perform regular risk assessments | Best practices dictate that organizations should review and update their assessment practices as new information becomes available, or at least every 12 months. The updated assessment should consider:  
| • changes in the customer base adopting electronic banking  
| • changes in the customer functionality offered through electronic banking  
| • changes in the external or internal environment  
| • actual incidents of security breaches, identity theft, or fraud experienced by the institution or industry |

### Layered Security Programs

| Financial institutions should implement a layered approach to security | Best practices recommend employing a prescriptive, layered approach to security – utilizing security tools within your online banking solution (e.g. multi-factor authentication, limit management, etc) with a fraud prevention and detection solution (e.g. profiling, analytics, etc.)

ACI Enterprise Banker provides options for layering security measures, including:
| • Login:
| o Trusteer secure browsing, RSA® Adaptive Authentication (Adaptive Authentication), tokens
| • Transaction Release:
| o ACI’s Proactive Risk Manager for transaction monitoring, fraud prevention and detection, tokens |
Effective controls may be included in a layered security program through a variety of safeguards.

Through Enterprise Banker and Proactive Risk Manager, multiple layers of authentication are available for securing transactions include:
- Adaptive Authentication including out-of-band verification
- Dual approval
- Positive pay
- Transaction limits
- One-time passwords (OTP) at login and/or transaction release (aka tokens or credentials)
- Real-time fraud detection and monitoring

<table>
<thead>
<tr>
<th>Layered Security Programs – Detect and Respond to Suspicious Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detect and respond to suspicious activity at login and at fund transfer</td>
</tr>
</tbody>
</table>
| Enterprise Banker allows for detecting and responding to suspicious activity at login with Adaptive Authentication, and at payment release with Proactive Risk Manager.  

Proactive Risk Manager offers real-time analytics to monitor transactional behavior to determine whether activity is standard or anomalous for that customer. When high-risk activity is detected, action can be taken in real time or near-real time to stop the transfer of funds from the customer’s account. Funds can also be held until customer validation can take place.  

In addition, Proactive Risk Manager employs profiling – including non-financial information (IP address, login activities, and device characteristics) – to build customer profiles which can be stored to monitor ongoing behavior. |

<table>
<thead>
<tr>
<th>Layered Security Programs – Control of Administrative Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enhanced controls over administrative access and functions</td>
</tr>
</tbody>
</table>
| Best practices dictate that end-users with transaction initiation or approval entitlements should not also have administrative rights.  

Enterprise Banker offers robust administrative entitling abilities, in addition to dual approval and transaction limits for enhanced control. |
## Effectiveness of Certain Authentication Techniques – Device Identification

| Institutions should no longer consider simple device identification as a primary control | Cookies, IP address, and geolocation are considered simple device identification and no longer an effective choice, as fraudsters have found ways to work-around around these security measures.  
Enterprise Banker offers Adaptive Authentication at login which employs a complex digital fingerprint by tracking device identification details in addition to IP address and geo-location. |

## Challenge Questions

| Implement sophisticated/complex challenge questions | Adaptive Authentication offers the ability to present “Knowledge Based Authentication” questions at login to Enterprise Banker.  
Adaptive Authentication also offers the ability to authenticate at login via an out-of-band phone call. |

## Customer Awareness and Education

| Increase in customer awareness and education | Financial Institutions are expected to provide:  
• The customer’s protections related to Regulation E  
• Explanation of the circumstances through what means the bank may contact a customer to validate credentials  
• Their need for proactive involvement to ensure transactions are valid through their own risk assessments  
• Information about who to contact when security related events occur  
• Inform the customers about alternative risk control mechanisms that a customer can implement themselves in the |

## Threat Landscape and Compensating Controls
| Identifying the threat landscape and introduce compensating controls to thwart malicious attacks | Man-in-the-Middle and Man-in-the-Browser attacks can be addressed through the use of a secure web browser service, such as Trusteer, as well as one-time-password tokens. Transactions and anomalies can be monitored through Proactive Risk Manager. Rules are designed to evaluate transactions in real-time for validity. Proactive Risk Manager can also compare transactions to a restricted funds transfer list. |


Online Banking Fraud Detection and Prevention

ACI Enterprise Banker™ is the industry-leading online banking system and is used by more large institutions than any other system in the world. The enterprise-wide solution allows financial institutions of all sizes to uniquely package products and services for different markets — or even individual customers — from a single, flexible platform. Enterprise Banker offers a full range of functionality including balance and transaction reporting, ACH and wire transfer origination and reporting, remote check deposit, bill presentment and payment, and cash concentration.

ACI Proactive Risk Manager™ is a complete fraud detection solution which manages risk across a financial institution’s business lines and customer accounts. Proactive Risk Manager combines the power of advanced analytics, custom neural network modeling and intuitive investigative tools for a fast, accurate and flexible response to current and emerging fraud trends.

The ACI Online Banking Fraud Management solution offers a system that leverages and closely monitors all Enterprise Banker customer activity, including log-in, expected usage and likely transactions to identify anomalies in behavior that can indicate suspicious activities. Financial institutions have immediate protection for their online banking activities through monitoring and analysis of log-in and token authentication, browser security, entitlements and other security protocols within the core Enterprise Banker offering. By leveraging these protocols and data points, Proactive Risk Manager can identify suspicious transaction activity in real time and stop fraudulent ACH and wire transfers immediately.

With this solution, financial institutions work with a single vendor to securely manage online banking transactions.

ACI recognizes the importance of security and risk management in the online banking environment and remain committed to our customers in helping them meet their compliance objectives.
## FFIEC Guidance Checklist

<table>
<thead>
<tr>
<th>Guidance</th>
<th>ACI Enterprise Banker</th>
<th>ACI Proactive Risk Manager</th>
<th>FI Best Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layered Security</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Risk Assessments</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Detect &amp; Respond to Suspicious Activity</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Control of Administrative Functions</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Device Identification</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Challenge Questions</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Customer Awareness &amp; Education</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>
ACI Worldwide
Offices in principal cities throughout the world
www.aciworldwide.com

Americas +1 402 390 7600
Asia Pacific +65 6334 4843
Europe, Middle East, Africa +44 (0) 1923 816393

© Copyright ACI Worldwide 2011
All rights reserved. All product names are trademarks or registered trademarks of their respective companies. ACI and the ACI logo are trademarks or registered trademarks of ACI Worldwide or its subsidiaries in the United States, other countries or both.

About ACI Worldwide
ACI Worldwide powers electronic payments for financial institutions, retailers and processors around the world with the broadest, most integrated suite of electronic payment software in the market. More than 75 billion times each year, ACI’s solutions process consumer payments. On an average day, ACI software manages more than US$12 trillion in wholesale payments. And for more than 150 payments organizations worldwide, ACI software ensures people and businesses don’t fall victim to financial crime. We are trusted globally based on our unrivaled understanding of payments and related processes. We have a definitive vision of how electronic payment systems will look in the future and we have the knowledge, scale and resources to deliver it. Since 1975, ACI has provided software solutions to the world’s innovators. We welcome the opportunity to do the same for you.