



ADI Adviser

## **FFIEC- Authentication in an Internet Banking Environment**

The Federal Financial Institutions Examination Council, FFIEC, has updated guidance regarding risks and controls associated with customer authentication when accessing internet based products and services in order to secure confidential customer information. That guidance, Authentication in an Internet Banking Environment published October 12, 2005, stipulates that all Financial Institutions regulated by one of the FFIEC member agencies and offering retail and/or commercial customers internet based access to financial products and/or services must conduct a risk-assessment of their Information Security Program regarding Internet Banking. Further, the guidance stipulates that controls must be designed and implemented by the end of 2006 that address the identified risks. The type and amount of controls to manage risk will vary based on the outcome of each institution's risk assessment.

The guidance requires the risk assessment be completed and adequate and appropriate controls be in place regarding Internet Banking by the end of 2006. In addition to noncompliance with this regulatory guidance, there are several other risks from having a weak Internet Banking Program. They include but are not limited to:

- Financial loss
- Reputation damage
- Fraudulent data
- Unenforceable/unbinding legal documents and contracts

While the guidance specifically calls attention to Internet Banking, it does not include coverage over the retail use of credit or debit cards used via the internet. It does state financial institutions will no longer be able to rely on single-factor authentication controls, such as a password or identification code, for moderate to high risk products/ services. Rather, institutions will have to implement multi-factor controls, such as a password in addition to a physical device, like an ATM card, and a possible third element like a, a fingerprint.

The concept is that authentication involves three elements:

- Information Known: password, personal identification number, etc.
- Information Has: ATM card, other physical device; and

- Information Is: biometric characteristic, like a fingerprint.

### Risk Assessment

The guidance calls for financial institutions to conduct a thorough risk assessment on existing Internet Banking systems and associated controls. Financial Institutions must evaluate the level of risk associated with their products and services, including all transactions and levels of access. Based on the outcome, appropriate and effective controls should be designed and implemented. Once in place, the system of controls must be evaluated for their effectiveness.

This type of risk assessment is similar to the elements of a BSA/AML and Privacy risk assessment that is most likely already in place and that may be a good place to start. As with any good risk assessment, a thorough Internet Banking risk assessment should not only identify the risks but also the mitigating controls.

#### Identify existing characteristics and the associated risk of:

- Customer base
- Products and services offered
- On-line transactional capabilities
  - Information only;
    - no banking or transaction capability – potentially lower



625 North Washington Street  
Suite 303  
Alexandria, VA 22314  
703-836-1517  
info@adiconsulting.com

- Full transactional internet banking - potentially higher risk

- Sensitivity of customer information being communicated with customer or Financial Institution
- Ease of using communication method
- Volume of transactions

Identify existing controls:

- Consider and evaluate the controls or mitigating factors of the Bank's Information Security (IS) program to individually address each existing characteristic and its associated risks
- Similar existing controls for BSA/AML and Privacy (section 505 of GLBA) may also serve to address risks associated with Internet Banking.

Identify Residual Risk:

- Weigh the effectiveness of the controls against the level of risk associated with the identified characteristics.
  - Are there any gaps in the controls
  - Are the controls identified appropriate and adequate to support the level of risk in the identified characteristics

**Control Characteristics**

Controls are designed and implemented to mitigate risk and

strengthen a process. The type and level of controls necessary to mitigate risk from internet banking processes vary depending on the outcome of each financial institution's risk assessment. When assessing or designing appropriate and adequate controls for an internet banking compliance program, financial institutions should consider:

- Authentication techniques: These should be appropriate and consistent with the level of risk associated with the customer base, products/services, on-line banking capabilities and overall results from a risk-assessment
  - (single-factor authentication is not deemed effective in many instances).
- Authentication controls should incorporate:
  - Customer acceptance: codes or passwords, etc. that are customer specific
  - Reliable performance: consistent controls that have a proven effectiveness
  - Scalability to accommodate growth: controls sufficient to handle growth in products and services
  - Applicability with existing systems and future plans: consistent with strategic plan for internet banking (Changes and updates should occur as often as needed to maintain strong controls).
  - Multi-factor authentication, layered security, etc. should be



625 North Washington Street  
 Suite 303  
 Alexandria, VA 22314  
 703-836-1517  
 info@adiconsulting.com

used in order to be in compliance with the Standards for Safeguarding of Customer Information (Graham Leach Bliley Act), to prevent money laundering and or terrorist financing (USA PATRIOT Act), to reduce fraud, stop identity theft, and promote legal enforceability of electronic agreements and or transactions (multiple layers of controls in general)

- Examples: PINs, passwords, digital certificates (PKI), physical devices, one-time passwords (OTP), plug-ins/tokens, transaction profile scripts, biometric id, etc. (Remember the questions: What a customer Knows, Has, and Is)?
- More factors are more effective if their accompanying policies, procedures, and other controls are successful

Each financial institution should start by looking at their own strategic plan regarding Information Security and Internet Banking. From their, a top down approach should be used to assess the make-up of the business and the applicable controls like policies, procedures, etc. to complete a thorough risk assessment. The end goal is to ensure that appropriate and adequate controls are in place to

mitigate risk and achieve the goals of the strategic plan.

### Internet Banking Compliance Program

The existing systems and controls should be part of larger Internet Banking compliance program. That larger Internet Banking Compliance Program should also include :

- **Verification of new customers:** Section 326 of the USA PATRIOT Act requires Financial Institutions to use reliable identification methods to verify all new customers via internet
- **Customer Awareness:** Financial Institutions should educate their customers about crimes such as, fraud and identity theft. An educated customer is the key defense and a powerful control against these common crimes. A customer awareness program can be implemented by using such tools as, statement stuffers, a bank's web-site, direct mail, etc. to communicate useful information on fraud and identity theft. However, keep in mind, that sending or providing communication is not the only step in a customer awareness program; it is also necessary to measure and evaluate its effectiveness.
- **Monitoring:** Financial Institutions must conduct on-



625 North Washington Street  
Suite 303  
Alexandria, VA 22314  
703-836-1517  
info@adiconsulting.com

going monitoring to help detect/identify any unauthorized access. Monitoring is essential in identifying any gaps or weaknesses in controls and can aid in identifying when adjustments are required due to technological changes and external or internal threats, etc.

- **Reporting:** Financial Institutions must promptly report suspicious or unauthorized access or activity in order to suspend an account or take other appropriate action. Independent audits of these reports should take place in order to ensure that adequate and appropriate controls are in place.