AUTHENTICATION IN AN INTERNET BANKING ENVIRONMENT

TWHC | Turner, Warren, Hwang & Conrad AC
Certified Public Accountants & Consultants

An Independent Member of BDO SEIDMAN ALLIANCE

What You Will Gain From This Presentation

Understanding of :

- The background of the Guidance.
- The Guidance's approach to risk assessments.
- How long the Guidance has been discussing the need to perform risk assessments.
- Consumer Awareness Program and what is required.

Questions

- How many of you have implemented Mobile Banking since 2001?
- How many of you have implemented Online Banking since 2001?
- How many of you are familiar with the term Authentication in an *Electronic* Banking Environment?

Questions

- How many of you are aware of what a Consumer Awareness Program is?
- Has anyone in the room been audited on this by your regulator?

Authentication in an Internet Banking Environment

- The concept of risk assessing a product or service before it is launched is not new, although recent guidance makes it appear so.

Authentication in an Internet Banking Environment

Background

- On August 8, 2001, the FFIEC issued guidance entitled "*Authentication in an Electronic Banking Environment*" (the Guidance).
- The Guidance focused on risks and risk management controls related to authentication in an electronic banking environment.

Authentication in an Internet Banking Environment

Background

- Noted that the implementation of appropriate authentication methodologies starts with *an assessment of the risk* posed by the institution's electronic banking systems.

Authentication in an Internet Banking Environment

Background

- Risk evaluation
  - Institution's customer base (consumer or commercial).
  - The institution's electronic delivery capabilities such as bill pay programs, electronic funds transfer products (wire transfer and ACH).
  - The sensitivity and value of the stored information to both the institution and the customer.

Authentication in an Internet Banking Environment

Background

- Risk evaluation (cont'd)
- The ease of using the method.
- The size and volume of transactions.

Authentication in an Internet Banking Environment

Background

- On October 12, 2005, the FFIEC issued updated guidance. The title of the 2005 guidance was changed to "*Authentication in an Internet Banking Environment*."

Authentication in an Internet Banking Environment

Background

- Significant legal and technological changes in the Financial Services Industry since the issuance of the 2001 guidance.
- Most of the changes addressed:
  - Management of consumer information.
  - Control and protection of consumer information.

Authentication in an Internet Banking Environment

Background

- Changes (cont'd)
  - Increasing incidents of fraud, including identity theft.
  - The introduction of improved authentication technologies.

Authentication in an Internet Banking Environment

Background

- Specific components of the 2005 guidance for FIs regulated by the:
  - OCC
  - OTS
  - Federal Reserve
  - FDIC
  - NCUA

Authentication in an Internet Banking Environment

Background

- Included:

  Conduct risk-based assessments.
  - Evaluate customer awareness programs.
  - Develop security measures to reliably authenticate customers remotely accessing their Internet-based financial services.

Authentication in an Internet Banking Environment

Background

- The 2005 guidance did several things:
  - Provided a risk management framework for financial institutions offering Internet-based products and services to their customers.
  - Told institutions to use effective methods of authenticating the identity of customers and that the techniques employed should be commensurate with the risks associated with the products and services offered and the protection of sensitive customer information.

Authentication in an Internet Banking Environment

Background

- The 2005 guidance (cont'd):
  - It provided minimal supervisory expectations for effective authentication controls applicable to high-risk online transactions involving access to customer information or the movement of funds.

Authentication in an Internet Banking Environment

Background

- The 2005 guidance (cont'd):
  - It addressed the fact that institutions should perform periodic risk assessments and adjust their control considerations as appropriate in response to changing internal and external threats.

Authentication in an Internet Banking Environment

Background

NCUA Letter 05-CU-18 (November 2005)

"Credit unions are expected to have achieved conformance with the guidance by year-end 2006."

And also

Authentication in an Internet Banking Environment

Background

- "NCUA Letter 06-CU-13 (August 2006)

"NCUA issued Letter to Credit Unions 05-CU-18 Guidance on Authentication in Internet Banking in November 2005. The letter directs credit unions which provide Internet-based service to determine if appropriate authentication methodologies and technologies are in place to authenticate members. Credit unions should be in compliance with this letter by yearend 2006."

and also

Authentication in an Internet Banking Environment

Background

- "Credit unions which provide Internet based products and services to members need to complete a risk assessment, determine if the authentication methodology is adequate based on the risk assessment, implement additional controls if high- risk Internet based products and services are provided and single factor authentication is the only control mechanism to authenticate members, implement monitoring systems to determine if unauthorized access occurs, and evaluate member educations program by yearend 2006."

Authentication in an Internet Banking Environment

Background

- On June 22, 2011, the FFIEC issued "*Supplement to Authentication in an Internet Banking Environment*"

Authentication in an Internet Banking Environment

General Supervisory Expectations

- "Since virtually every authentication technique can be compromised, financial institutions should not rely solely on any single control for authorizing high risk transactions, but rather institute a system of layered security."

Authentication in an Internet Banking Environment

Specific Supervisory Expectations

Risk Assessments

- The Agencies reiterate and stress the expectation described in the 2005 Guidance:
  - FIs should perform periodic risk assessments and
  - Adjust their customer authentication controls as appropriate in response to new threats to customers' online accounts.
- FIs should review and update their existing risk assessments:
  - As new information becomes available, prior to implementing new electronic financial services, or
  - At least every twelve months.

Authentication in an Internet Banking Environment

Specific Supervisory Expectations

Risk Assessments

- Updated risk assessments should consider, but not be limited to, the following factors:
  - Changes in the internal and external threat environment;
  - Changes in the customer base adopting electronic banking;

Authentication in an Internet Banking Environment

Specific Supervisory Expectations

Risk Assessments

- Updated risk assessments should consider, but not be limited to, the following factors (cont'd):
  - Changes in the customer functionality offered through electronic banking; and
  - Actual incidents of security breaches, identity theft, or fraud experienced by the institution or industry.

Authentication in an Internet Banking Environment

Customer Authentication for High Risk Transactions

- Definition of "high-risk transactions" remains unchanged from the 2005 guidance:
  - "Electronic transactions involving access to customer information or the movement of funds to other parties."
  - Since 2005, more customers (both consumers and businesses) are conducting online transactions.

Authentication in an Internet Banking Environment

Customer Authentication for High Risk Transactions

- Not all online transactions pose the same level of risk.
- More robust controls need to be implemented as the risk level of the transactions increases.

Authentication in an Internet Banking Environment

Layered Security Programs

- Layered security:
  - Uses different controls at different points in a transaction process so that a weakness in one control is generally compensated for by the strength of a different control.
  - Can substantially strengthen the overall security of Internet-based services.

Authentication in an Internet Banking Environment

Layered Security Programs

- Layered security (cont'd):
  - Is effective in protecting sensitive customer information.
  - Prevents identity theft, and reduces account takeovers and the resulting financial losses.

Authentication in an Internet Banking Environment

Layered Security Controls

- In the "Supplement" the Agencies discuss a number of Layered Security control mechanisms, some of which include:
  - Positive Pay
  - Number of transactions per day on an account
  - Fraud detection and monitoring systems that include consideration of customer history and behavior and enable a timely and effective institution response;
  - The use of dual customer authorization through different access devices;

Authentication in an Internet Banking Environment

Layered Security Controls

- Security control mechanisms cont'd:
  - The use of out-of-band verification for transactions;
  - The use of "positive pay," debit blocks, and other techniques to appropriately limit the transactional use of the account;
  - Enhanced controls over account activities; such as transaction value thresholds, payment recipients, number of transactions allowed per day, and allowable payment windows (e.g., days and times);

Authentication in an Internet Banking Environment

Layered Security Controls

- Security control mechanisms cont'd:
  - The use of out-of-band verification for transactions;
  - Internet protocol (IP) reputation-based tools to block connection to banking servers from IP addresses known or suspected to be associated with fraudulent activities;
  - Policies and practices for addressing customer devices identified as potentially compromised and customers who may be facilitating fraud;

Authentication in an Internet Banking Environment

Layered Security Controls

- Security control mechanisms cont'd:
  - Enhanced control over changes to account maintenance activities performed by customers either online or through customer service channels; and
  - Enhanced customer education to increase awareness of the fraud risk and effective techniques customers can use to mitigate the risk.

Authentication in an Internet Banking Environment

Layered Security Controls

- There is an expectation from the Agencies that the layered security contain "two elements, at minimum," and these include:

Authentication in an Internet Banking Environment

Detect and Respond to Suspicious Activity

- Processes designed to detect anomalies and effectively respond to suspicious or anomalous activity related to:
- Initial login and authentication of customers requesting access to the institution's electronic banking system; and
- Initiation of electronic transactions involving the transfer of funds to other parties.

Authentication in an Internet Banking Environment

Consumer Awareness Program Elements

- "A financial institution's customer awareness and educational efforts should address both retail and commercial account holders and, at a minimum, include the following elements:
  - An explanation of protections provided, and not provided, to account holders relative to electronic funds transfers under Regulation E, and a related explanation of the applicability of Regulation E to the types of accounts with Internet access;

Authentication in an Internet Banking Environment

Consumer Awareness Program Elements

- An explanation of under what, if any, circumstances and through what means the institution may contact a customer on an unsolicited basis and request the customer's provision of electronic banking credentials;

Authentication in an Internet Banking Environment

Consumer Awareness Program Elements

- A suggestion that commercial online banking customers perform a related risk assessment and controls evaluation periodically;
- A list of alternative risk control mechanisms that customers may consider implementing to mitigate their own risk or, alternatively, a list of available resources where such information can be found; and

Authentication in an Internet Banking Environment

Consumer Awareness Program Elements

- A list of institutional contacts for customers' discretionary use in the event they notice suspicious account activity or experience customer information security-related events."

Authentication in an Internet Banking Environment

NCUA Letter 11-CU-09 (June 2011)

- "Federally insured credit unions will be expected to adapt appropriate strategies from the supplement to strengthen and enhance controls by January 2012. Beginning in 2012, at credit unions offering electronic services, NCUA examiners will evaluate these controls under the enhanced expectations outlined in the supplement."

Authentication in an Internet Banking Environment

Conclusion

Risk assessments are here to stay. If you are not doing them, you need to start.

Authentication in an Internet Banking Environment

What TWHC Is Finding

- No risk assessments having been performed.
- Initial risk assessments were performed, but no subsequent risk assessments were completed.
- New electronic services being added, and no risk assessment was completed.

Authentication in an Internet Banking Environment

What TWHC IS Finding

- Business accounts not included in the risk assessment.
- No Consumer Awareness Program has been developed.
- Weak security question being used, (i.e., mothers maiden name, date of birth) instead of out-of-wallet questions.

Authentication in an Internet Banking Environment

What TWHC IS Finding

- No system for monitoring anomalous activity on online accounts.

Green Dot Engagements

Questions?

Terry L. Nabors, CRCM
Principal
Terryn@twhc.com

Kian Moshirzadeh, CPA
Partner
Kianm@twhc.com