July 14, 2011

Updated Regulatory Guidance for Authentication in an Internet Banking Environment: A New Standard of Care?

On June 29, 2011, the Federal Financial Institutions Examination Council (the "FFIEC"), a federal interagency body empowered to prescribe uniform standards of supervision for banks and credit unions, issued new guidance (the "FFIEC 2011 Supplement") updating the FFIEC's minimum supervisory expectations "regarding customer authentication, layered security, and other controls in an increasingly hostile online environment."[1] This updated guidance may create a new standard against which financial institutions' actions will be measured when defending claims by customers in connection with alleged losses involving online account takeovers and unauthorized electronic funds transfers. According to the FFIEC, cybercrime complaints have risen substantially each year since 2005, particularly with respect to commercial accounts. In the third quarter of 2009 alone, computer scams targeting commercial deposit accounts cost U.S. companies $120 million.[2] Small businesses and nonprofits have suffered some relatively large losses because commercial deposit accounts do not receive the reimbursement protection that consumer accounts do. As a result, there has been a surge in litigation against financial institutions, in which customers allege their financial institutions should have stopped payments.[3] The updated FFIEC guidance reflects significant changes in the risk landscape. Specifically, banking regulators are concerned that customer authentication methods and controls implemented in conformance with guidance issued several years ago have become less effective. The FFIEC said that "[f]raudsters have continued to develop and deploy more sophisticated, effective, and malicious methods to compromise authentication mechanisms and gain unauthorized access to customers' online accounts. Rapidly growing organized criminal groups have become more specialized in financial fraud and have been successful in compromising an increasing array of controls. Various complicated types of attack tools have been developed and automated into downloadable kits, increasing availability and their use by less experienced fraudsters."[4] The FFIEC 2011 Supplement, which updates the earlier guidance, Authentication in an Internet Banking Environment (the "FFIEC 2005 Guidance"), issued on October 12, 2005,[5] instructs financial institutions to use certain minimum types of "layered security" and fraud monitoring to better protect against cybercrime. It establishes minimum control expectations for certain online banking activities and identifies controls that are less effective in the current environment. It also identifies certain specific minimum elements that should be part of an institution's customer awareness and education program. **Risk Assessment** The FFIEC 2011 Supplement requires financial institutions to review and update existing risk assessments (i) as new information becomes available, (ii) prior to implementing new electronic financial services, and (iii) at least every 12 months. In light of the constantly evolving environment for online banking, financial institution 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;
- 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.

Customer Authentication for "High-Risk Transactions" In its 2005 Guidance, the FFIEC defined "high-risk transactions" as "electronic transactions involving access to customer information or the movement of funds to other parties." Although the FFIEC does not change this definition in the FFIEC 2011 Supplement, it recognizes that "not every online transaction poses the same level of risk." Specifically, the FFIEC notes the risks posed by online consumer transactions (e.g., accessing account information, bill payment, intrabank funds transfers, occasional interbank funds transfers or wire transfers) are generally lower than the risks posed by online business transactions (e.g., ACH file origination, frequent interbank wire transfers), particularly when taking into account the frequency and dollar amounts of these transactions. In light of the varied risks, financial institutions should implement layered security consistent with the risk for covered transactions. For commercial transactions, financial institutions are advised to use controls consistent with the increased level of risk for covered business transactions. According to the FFIEC, effective controls that may be included in a layered security program include, but are not limited to, the following:

- Fraud detection and monitoring systems that include consideration of customer history and behavior and enable a timely and effective institution response;
- Use of dual customer authorization through different access devices;
- Use of out-of-band verification for transactions;
- 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);
- 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;
- 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 they can use to mitigate the risk.

The FFIEC expects an institution's layered security program will contain, at a minimum, (i) manual or automated transaction monitoring or anomaly detection and response processes, to detect and respond to suspicious account activity, and (ii) enhanced controls for customers and system administrators who are granted privileges to set up or change system configurations, such as setting access privileges and application configurations and/or limitations. Importantly, the FFIEC recommends institutions offer to their business customers multifactor authentication systems that may include device authentication and challenge questions. With respect to device authentication, the FFIEC's guidance distinguished between "simple" device identification techniques (such as use of cookies installed on end-user devices) and "more sophisticated" techniques (such as use of digital fingerprints that combine a number of characteristics including PC configuration, Internet protocol address, geo-location, and other factors). The FFIEC noted that it considers *"complex device identification to be more secure and preferable to simple device identification"* [emphasis added]. Further, the FFIEC recognizes the usefulness of challenge questions as an effective component of a layered online security program. In view of the amount of information about people that is readily available on the Internet and that individuals themselves make available on social networking websites, the FFIEC advised that *"institutions should no longer consider such basic challenge questions, as a primary*

control, to be an effective risk mitigation technique" [emphasis added]. Rather, the FFIEC notes, challenge questions can be implemented more effectively using "out of wallet" questions that do not rely on information that is often publicly available. Sophisticated challenge question systems usually require the customer to correctly answer more than one question and often include a "red herring" question designed to trick the fraudster, one?that the legitimate customer will recognize as nonsensical. Finally, the FFIEC stresses the effectiveness of customer awareness and education programs for both retail and commercial account holders. At a minimum, such awareness and education efforts should address the following elements:

- An explanation of protections provided (and those 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;
- An explanation of circumstances (if any) under which and means through which the institution may contact a customer on an unsolicited basis and request the customer's electronic banking credentials;
- A suggestion that commercial online banking customers periodically perform a related risk assessment and controls evaluation;
- A listing of alternative risk control mechanisms customers may consider implementing to mitigate their own risk, or (alternatively) a listing of available resources where such information can be found; and
- A listing of institutional contacts for customers' discretionary use in the event the customer notices suspicious account activity.

Conclusions In the past, plaintiffs' attorneys and the courts have looked to the FFIEC 2005 Guidance as establishing the minimum standard of care for determining whether institutions have adopted commercially reasonable methods of providing security against unauthorized payment orders. Going forward, financial institutions should expect that the FFIEC 2011 Supplement, requiring annual risk assessments and enhanced authentication and monitoring for Internet-based banking transactions, will set a new, higher minimum standard of care for the industry. At Day Pitney, we believe a strong offense is our clients' best defense to minimize the risks of an adverse outcome in a regulatory review or in litigation. In light of the importance of the newly issued FFIEC 2011 Supplement, we recommend each financial institution carefully review the FFIEC's updated guidance and consider undertaking an early risk assessment and internal controls review to be sure the institution complies with the announced minimum supervisory expectations. Further, by working together with appropriate technology experts, financial institutions should develop a plan for implementing enhanced authentication and monitoring consistent with the updated FFIEC guidance. The Day Pitney Compliance and Risk Management team would be pleased to speak with you in more detail about the new FFIEC 2011 Supplement or any related subject matter.

---

[1] Supplement to Authentication in an Internet Banking Environment (June 29, 2011), at 1, http://www.ffiec.gov/pdf/Auth-ITS-Final 6-22-11 %28FFIEC Formated%29.pdf. [2] David M. Nelson, Federal Deposit Insurance Corp., FDIC Cyber Fraud and Financial Crime Report, Presentation at RSA Conference 2010 (March 2010), at 12, https://365.rsaconference.com/docs/DOC-2470. [3] See, e.g., Shames-Yeakel v. Citizens Fin. Bank, 677 F. Supp. 2d 994 (N.D. Ill. 2009), plaintiff's cite to the FFIEC 2005 Guidance to support its contention that the defendant bank was negligent in failing to prevent a fraudulent transfer from a commercial deposit account; see also Patco Constr. Co. v. People's United Bank, 2011 U.S. Dist. LEXIS 58112 (D. Maine May 27, 2011), granting summary judgment in favor of defendant based in part on compliance with the FFIEC 2005 Guidance, and Experi-Metal Inc. v. Comerica, Inc., 2010 U.S. Dist. LEXIS 68149 (E.D. Mich. July 8, 2010). [4] Supplement to Authentication in an Internet Banking Environment (June 29, 2011), at 2,

http://www.ffiec.gov/pdf/Auth-ITS-Final 6-22-11 %28FFIEC Formated%29.pdf. [5] FFIEC, Authentication in an Internet Banking Environment (2005), at 1-2, http://www.ffiec.gov/pdf/authentication_guidance.pdf.