The Banking Law Journal

VOLUME 128 NUMBER 9 OCTOBER 2011

THE BANKING LAW JOURNAL (ISSN 0005 5506) (USPS 003-160) is published ten times a year by A.S. Pratt & Sons, 805 Fifteenth Street, NW., Third Floor, Washington, DC 20005-2207. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices.
POSTMASTER: Send address changes to THE BANKING LAW JOURNAL, A.S. Pratt & Sons, 805 Fifteenth Street, NW., Third Floor, Washington, DC 20005-2207.

The FFIEC's Supplement to Authentication in an Internet Banking Environment: The New Minimum Legal Standard?

SCOTT FRYZEL

In this article the author provides a brief overview and examination of the recent FFIEC Internet banking security guidance supplement, includes compliance considerations for bankers on addressing some specific requirements in the Supplement, and reviews the question of whether courts will hold financial institutions liable for failing to comply with its more rigorous layered security standard.

In response to the increasing threat of fraud in Internet banking and to update what is expected of financial institutions by federal regulatory agencies, the Federal Financial Institutions Examination Council ("FFIEC") issued its *Supplement to Authentication in an Internet Banking Environment* on June 28, 2011 (the "Supplement"). The Supplement updates the FFIEC's guidance from October 12, 2005 entitled *Authentication in an Internet Banking Environment* ("Guidance"). Based on recent court decisions that have relied on the Guidance, the Supplement may also establish the new minimum standard against which banks are held legally responsible for claims that a bank has breached its duty to protect client accounts and information.

Scott Fryzel is a partner in the Banking Department of Chapman and Cutler LLP. He may be reached at fryzel@chapman.com.

Published by A.S. Pratt in the October 2011 issue of *The Banking Law Journal*.

SPECIFIC SUPERVISORY EXPECTATIONS

The Supplement outlines the supervisory expectation that financial institutions should not rely solely on any single control for authenticating Internet banking transactions, including "high risk transactions" (*i.e.*, electronic transactions involving access to customer information or the movement of funds to other parties), but should employ a system of periodic risk assessments, layered security, and other controls as appropriate. This Supplement updates the focus on multi-factor authentication methods emphasizing a layered security program that is commensurate with the risk associated with the products and services offered.

Risk Assessments

The Supplement stresses the need to perform periodic risk assessments and adjust customer authentication controls in response to new threats to customers' online accounts. The type of risk assessments should be updated as new information becomes available and when new electronic financial services are implemented, but no less frequently than every 12 months. Updated risk assessments should consider, among other things, changes in the internal and external threat environment, changes in an institution's electronic banking customer base or electronic banking functionality, and actual incidents of security breaches, identity theft, or fraud experienced by the institution or industry.

Customer Authentication for High Risk Transactions

Financial institutions are directed to assess the risk in the types of electronic banking transactions offered and implement more robust controls as the risk level of the transaction increases. Consumer transactions are considered by the FFIEC to present a lower level of risk because they are executed less frequently and at lower dollar amounts (primarily for bill payment, interbank funds transfers, and infrequent transfers to another bank) as compared to commercial transactions (more frequent ACH origination and wire transfers with larger dollar amounts). Layered security, including multi-factor authentication, is recommended for commercial clients.

Layered Security Program

Layered security is characterized by the use of different controls at different points in a transaction process so that a weakness in one control is generally compensated for by the strength of another control.[1] The Supplement stresses the need for layered security programs to strengthen the overall security of high risk Internet-based services to protect confidential client information, prevent identity theft, and reduce losses. The types of controls noted in the Supplement as effective controls in a layered security program include, but are not limited to:

- Fraud detection that includes consideration of client history and behavior and enables timely and effective institution response;
- Dual authorization through different access devices;
- Use of positive pay, debit blocks, or other services to limit transaction use on accounts;
- Enhanced controls on deposit accounts (*e.g.*, transaction value thresholds);
- Internet protocols that block connection of bank servers to Internet sites known for fraudulent activity; and
- Enhanced client education.

Compliance Consideration

Institutions should contact and consult with their Internet banking service providers to determine what types of layered security functions are available under its current contract for services but may not currently be utilized. Service provider contracts should be reviewed to determine what upgrades are available and at what cost to the institution.

MINIMUM ELEMENTS OF LAYERED SECURITY

Of those programs mentioned, the Supplement expressly states that a layered security program will contain, at a minimum, the following: (i) processes

designed to detect anomalies and effectively respond to such occurrences in client electronic banking transactions, and (ii) enhanced control of administrative functions that establish a client's electronic banking configurations that exceed those for routine business clients (*e.g.*, a transaction verification notice after implementing changes).

The Appendix to the Supplement provides a discussion of the threat landscape and compensating controls that can be implemented by a banking institution. The types of threats that are identified and explained include keylogging malware, man-in-the middle ("MIM"), or man-in-the browser ("MIB") attacks. Financial institutions are directed to investigate which controls may be most effective in preventing attacks and losses as part of an institution's layered security program. Anti-malware software, transaction monitoring/anomaly detection software, and one-time password tokens are each suggested by the Supplement as strong authentication methods to control MIM/MIB attacks. "Out-of-band" authentication requires a transaction delivered via one delivery channel to be verified through a second delivery channel, including a different person to confirm the transaction (*i.e.*, someone other than the person initiating the transaction) and is also included as an effective control to reduce fraudulent funds transfers.

Traditional business control procedures are also encouraged including:

- Periodic review of volume and value limits (individual and aggregate), monitor and alert on exception events, establish individual and aggregate exposure limits;
- Use of positive pay;
- Notice of intent to originate ACH transaction prior to origination; and
- Dual control procedures for higher risk functions performed online.

Compliance Consideration

Institutions can immediately evaluate the use of volume and value limits recommended in the Supplement above as part of its risk assessment and implementation of layered security. Internet transaction services typically offer the ability to limit the value or volume of transactions (either single transactions or in the

aggregate) — but establishing these limits is often left to the client during implementation. Institutions should: (i) evaluate the limits in place for current clients; (ii) implement limits for those clients as appropriate; and (iii) implement default limits for new clients. Transactions initiated above those limits should require client action (through response to a challenge question or other communication with the bank) to increase limits or approve transactions in excess of limits. As noted in the court decisions below the use of transaction limits was one consideration in the determination that a bank acted in a commercially reasonable manner in implementing a layered security program.

EFFECTIVENESS OF CERTAIN AUTHENTICATION TECHNIQUES

The Supplement provides information on the integrity of two types of client authentication techniques: (i) device identification and (ii) challenge questions. Device authentication was implemented by many banks in response to the Guidance. The Supplement encourages the use of complex device authentication through use of a "one-time" cookie to create a digital "fingerprint" to identify a number of a PC's characteristics (*e.g.*, PC configuration, Internet protocol address, geo-location) as opposed to simple device authentication (use of a less sophisticated cookie installed on the user's computer). Challenge questions are also encouraged for use if the primary logon presents unexpected transaction characteristics. The use of multiple, more sophisticated and "out of wallet" questions is promoted as an effective component of a layered security program.

CUSTOMER AWARENESS AND EDUCATION

Financial institutions are on notice that customer awareness should be included as a part of the financial institution's security programs for both commercial and consumer clients. Without specifying how customer awareness and education programs should be structured, the FFIEC set forth that minimum efforts should include:

- An explanation of protections provided and not provided and the applicability of Regulation E;

- An explanation of what, if any, circumstances and through what means an institution might contact the client regarding electronic banking credentials;
- A suggestion to commercial clients to perform their own periodic risk assessment and controls evaluation;
- A list of alternative risk controls that clients might implement; and
- A list of contacts at the institution for the client to contact in the event of suspicious or other information security related events.

Compliance Consideration

Institutions should confirm that clients are educated regarding the types of security available at the institution by providing its documented security procedures to new and existing clients. Existing clients should be updated on what is available as security options change and no less than annually. As part of ongoing awareness institutions should develop links or a click-through that pop up on the institution's Internet banking site that highlights the most recent fraud alerts or schemes; and include links to government sponsored web sites that contain regulatory information and guidance, the types of security procedures offered by the institution and institution's client contact lists.

COURT DECISIONS AND FFIEC GUIDANCE: A NEW MINIMUM LEGAL STANDARD?

Financial institutions are advised to follow the direction provided by the Supplement, not only to maintain regulatory compliance, but also to demonstrate that its security procedures comply with the terms of their own service agreements and meet commercially reasonable standards in case of a client loss and potential litigation.

In the recent decision of *Patco Construction Company, Inc., v. People's United Bank d/b/a Ocean Bank*, the federal magistrate found in favor of Ocean Bank by relying in part on the standards set by the Guidance in deciding that the bank provided commercially reasonable security measures by using not only multi-factor authentication but multiple layers of security.[2]

The opinion detailed how Ocean Bank offered authentication through User IDs and passwords, set transaction limits in connection with challenge questions to those initiating the transactions and summarized the layered security offered and implemented by Ocean Bank at the time of the fraud, including sending email alerts and anti-phishing controls; while acknowledging that tokens were not used by the plaintiff client. The opinion stated that the bank's implementation of the security procedures offered by its service provider was a careful effort to comply with the Guidance;[3] and that "when measured against the Guidance yardstick that both parties have treated as a critical factor in this case, is commercially reasonable, incorporating not only at least two factors but also 'multiple layers' of security."[4]

In a similar instance of fraud on a customer's account, in a Bench Opinion issued in *Experi-Metal, Inc. v. Comerica Bank*, the court found that the bank had not acted in good faith in implementing its security procedures and fraud monitoring for its client Experi-Metal.[5] The Experi-Metal ruling was based in part on the court's conclusion that Comerica failed to meet its burden to show that it accepted payment orders in good faith and in compliance with reasonable commercial standards of fair dealing for a client such as Experi-Metal. As part of its opinion, the court noted that although the FFIEC guidance is not mandatory, it was a consideration by the court in determining whether the bank dealt fairly with its customer; the court determined that fraud monitoring as recommended by the FFIEC should have been used under these circumstances.

These recent cases were not the first time a court has cited or relied in part on the Guidance as a benchmark. In the 2009 decision of *Shames-Yeakel v. Citizens Financial Bank*, the federal court in the Northern District of Illinois allowed a plaintiff's negligence claim to proceed by denying a motion for summary judgment, based on the Guidance.[6] In this instance, an unauthorized transaction was allowed on a home equity line of credit using Citizens Financial's Internet banking service. The court noted that the Guidance stated that single-factor authentication is inadequate for high risk transactions including funds transfers. Citizens Financial had failed to provide multi-factor authentication security, issuing only user names and passwords, to a business customer that experienced an unauthorized access to its line of credit even though the bank was in the process of implementing multi-factor

authentication. The Citizens Financial court decided that due to the bank's failure to comply with the Guidance, a finder of fact could conclude that the defendant bank breached its duty to sufficiently secure its online banking system to protect a client's account against fraudulent access and the plaintiff's claim shall proceed.

In light of this judicial reliance, financial institutions should assess their Internet banking authentication and monitoring security procedures to verify compliance with the Supplement as a minimum standard for security procedures for high risk transactions. In the instances above, courts have decided in favor of the bank that complied with the Guidance and decided against the banks that did not comply with the Guidance, even though it was not mandatory. However, compliance with the Guidance and the Supplement may not establish an absolute safe harbor. Financial institutions must continue to provide the levels and layers of security, monitoring, and communication as available and appropriate for high risk transactions of its electronic banking customer base to meet commercially reasonable and good faith standards.

Compliance Consideration

While the Supplement and court decisions focus on implementing and requiring layered security procedures to meet the legally required commercially reasonable standard, banks struggle to have all clients agree to use some form of security. Clients are either constrained by a limited number of employees to implement the procedures typically required or consider them burdensome. Continuing to allow transactions without the recommended security procedures presents unnecessary legal and financial risk to the institution. Clients without security procedures should be presented with the options recommended by the institution in writing and if the client chooses to proceed without such procedures, the institution should obtain a written waiver signed by an authorized representative of the client as required by applicable law. Oftentimes a strongly worded waiver can convince a client that using the security procedures may be a better alternative.

SUMMARY AND CONCLUSION

The Supplement outlines minimum requirements to implement a layered security program and imposes obligations to perform periodic risk assessments to continuously update and improve a system of layered security for Internet banking transactions. While consistent with the earlier Guidance, the Supplement may be relied upon by courts as establishing a new higher standard by which to measure a bank's performance and allocate legal liability when providing Internet banking services to its clients. Institutions are advised to undertake a client risk assessment, implement the layered security options currently available if not previously required, review compliance and security upgrades with their vendors or in-house systems and assess client controls, process, and agreements.

NOTES

[1] Federal Financial Institution Examination Council, Supplement to Authentication in an Internet Banking Environment, June 28, 2011, at 4.

[2] No. 2:09-CR-503-DBH, WL 217450 (D. Maine May 27, 2011), *aff'd.*, No. 09-503-P-H (D. Maine Aug. 4, 2011).

[3] *Id.* at *32.

[4] *Id.* at *33.

[5] No. 09-14890, WL 2433383, (E.D. Mich. June 13, 2011).

[6] *Shames-Yeakel v. Citizens Financial Bank*, 677 F. Supp. 2d 994 (N.D. III. 2009).