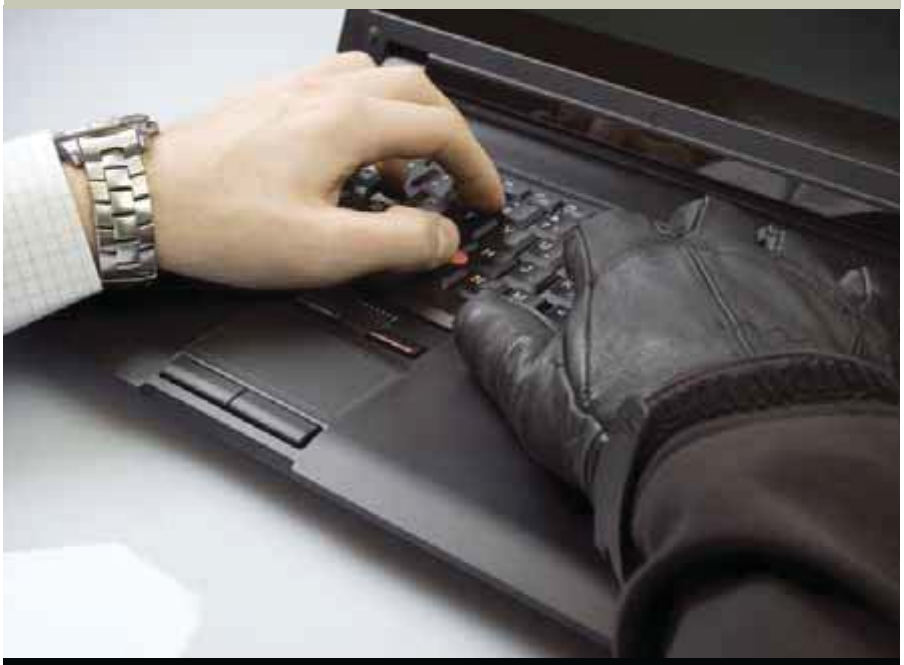
COUNSELOR'S CORNER

2012 Security Measures for Combating Cyber Fraudsters

Jeff Makovicka, Husch Blackwell LLP



Commercial transactions are increasingly conducted online without any face-to-face interaction and without the traditional safeguards used to confirm that a party is who they claim to be.

THIS REALITY HAS CREATED AN OPportunity for criminals to steal online identities and use them for monetary gain. As such, the ability of one party to authenticate the identity of the other party in an online transaction is of key importance, especially in banking.

In response to the increasing threat of fraud in online banking, the Federal Financial Institutions Examination Council (FFIEC) issued a Supplement to Authentication in an Internet Banking Environment on June 28, 2011.[1] The supplement updates the Oct. 12, 2005, FFIEC guidance entitled Authentication in an Internet Banking Environment.[2] Both the guidance and the supplement outline recommended security measures banks may implement to enhance their ability to authenticate the identity of online banking users and prevent fraud. Because "[t]he agencies are concerned that customer authentication methods and controls implemented in conformance with the [guidance] have become less effective," the supplement further reinforces the security framework described in the guidance and updates the supervisory expectations regarding customer authentication, layered security, and other controls in the online environment.

Courts considering the guidance (pre-supplement) suggest that the supplement may establish the new minimum standard against which banks are held legally responsible for claims that a bank has breached its duty to protect customer accounts and information. As a result, banks should review and update their authentication procedures and online banking forms to comply with the guidance as updated by the supplement.[3]

Online Fraud Rising

Banks currently face a growing threat from cyber criminals (or, as the supplement affectionately calls them, "fraudsters") employing sophisticated techniques to perpetrate deposit account "takeovers" and transfer funds, often to criminal accounts overseas. In testimony before a subcommittee of the House Financial Services Committee in September 2011, the assistant director of the FBI's Cyber Division stated the FBI is currently investigating more than 400 reported cases of corporate account takeovers involving in excess of $255 million in attempted theft and approximately $85 million in actual losses.[4]

Supervisory Expectations. The supplement outlines the supervisory expectation that banks should not rely solely on any single control for authenticating online banking transactions, including "high risk transactions" (i.e., electronic transactions involving access to customer information or the movement of funds to other parties),

but rather should institute a system of periodic risk assessments, layered security, and other controls as appropriate. The supplement updates the focus on multifactor 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, or at least every 12 months. Updated risk assessments should consider, among other things: (a) changes in the internal and external threat environment, (b) changes in a bank's electronic banking customer base or electronic banking functionality, and (c) actual incidents of security breaches, identity theft, or fraud experienced by the bank or industry. Banks should document any adjustments made and the reasons for such adjustment.

Customer Authentication for High Risk Transactions. Banks 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 be lower risk as they are less frequent and at lower dollar amounts as compared to commercial transactions (frequent wire transfers with larger dollar amounts). Because of the increased risk, layered security, including multifactor authentication, is recommended for commercial customers.

Layered Security Program. Layered security is characterized as different controls at different points in a transaction process so that a weakness in one is compensated for by the strength in another. The supplement stresses the need for layered security programs to strengthen the overall security of high risk online services to protect sensitive customer information, prevent identity theft, and reduce financial losses.[5] At minimum, layered security should include anomaly detection and response at (a) customer login and (b) initiation of funds transfers to other parties. The FFIEC specifically notes that in many cases of online banking fraud, the fraud could have been prevented because the wire transfers being originated by the fraudsters were anomalous when compared with the customer's established patterns of behavior.

The types of controls noted in the supplement as effective controls in a layered security program include, without limitation:

- fraud detection and monitoring systems that include consideration of customer history and behavior and that enable timely and effective bank response;

■ **Cyber Fraudsters** — continued on page 14

■ Cyber Fraudsters — continued

- dual customer authorization through different access devices;
- use of positive pay, debit blocks, or other services to limit transaction use on accounts;
- enhanced controls over account activities (e.g., transaction value thresholds);
- internet protocol (IP) tools that block connection of bank servers to IP addresses known (or suspected) for fraudulent activity; and,
- enhanced customer education.

For compliance with the supplement beginning in January 2012, banks should engage their respective technology providers to determine what the cyber threats are and what enhanced (layered) security measures are available under each bank's current contract for services.

Effectiveness of Certain Authentication Techniques. In the supplement, the FFIEC provides guidance on the integrity of two types of customer authentication techniques: (a) simple device identification and (b) challenge questions. According to the FFIEC, the following authentication techniques are no longer sufficient:

- simple one-dimensional device authentication (which was implemented by many banks in response to the guidance) relying on the use of cookies loaded onto a customer's personal computer to confirm that the PC attempting access is the one enrolled by the customer.
- simple challenge questions easily answered by anyone that researched the customer through Internet searches and social media.

Examples of stronger, more effective controls identified in the supplement are:

- complex device identification tools such as a "one-time" cookie to create a complex digital "fingerprint" to identify a number of a PC's characteristics, including PC configuration, IP address, geo-location, and other factors.
- a complex challenge question process by use of multiple, more sophisticated, or "out-of-wallet" questions.[6]

Customer Awareness & Education. The supplement also prescribes that customer awareness should be included as a part of the bank's security programs for both commercial and consumer customers. At minimum, these programs should include:

- a description of accountholder protections;
- an explanation of circumstances under which the bank will contact the customer to verify his or her identity;
- suggestions for commercial online banking customers to perform a risk assessment and controls evaluation periodically;
- a listing of alternative risk controls for customers to consider to reduce their online banking risk; and,
- a contact list for customers to use if they notice suspicious account activity or experience a security-related event.

By providing security procedures in writing to new and existing customers, banks can confirm that customers are aware of the types of security available at the bank. As security options change, existing customers should be updated on what is available through links or news on the bank's website.

Court Decisions, the Guidance & the Supplement

After issuance of the guidance, cases arose alleging that use of single factor authentication constitutes unreasonable security. In *Shames-Yeakel v. Citizens Financial Bank*,[7] the court allowed the plaintiffs' negligence claim (arising from an unauthorized transfer obtained from the plaintiffs' account by a fraudster using the plaintiffs' user name and password) to survive by denying a motion for summary judgment, based in part on the guidance. The plaintiffs alleged that the bank had negligently failed to move from single to dual factor authentication per the guidance in time to prevent the unauthorized transfer. The court decided that "[i]n light of Citizens' apparent delay in complying with FFIEC security standards, a reasonable finder of fact could conclude that the bank breached its duty to protect Plaintiffs' account against fraudulent access" and the plaintiffs' claim was allowed to proceed.

Last year, a federal court in Maine delivered a significant decision regarding bank liability for unauthorized withdrawal of funds from a corporate deposit account after a fraudster obtained access to the online credentials of the bank's customer.[8] The main allegation in the suit was that the authentication procedures and other security measures employed by the bank failed to prevent the fraudulent wire transfers and were not commercially reasonable.

The *Patco* court found in favor of the bank by relying in part on the standards set by the guidance concluding that the bank provided commercially reasonable security measures by using not only multifactor authentication but also multiple layers of security. In holding that the bank had implemented commercially reasonable security, the court noted that the bank offered authentication through user identifications and passwords, set transaction limits in connection with challenge questions to those initiating the transactions, and summarized the layered security offered and implemented by the bank at the time of the fraud. Moreover, the court stated that the bank's implementation of the security procedures was a "careful effort at compliance" with the guidance 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."

As discussed above, courts have considered compliance with the guidance in determining whether a bank adopted commercially reasonable methods of providing security against online fraud. Because of this past treatment by the courts, the guidance, as updated by the supplement, may create a new standard of care against which a bank's actions will be measured in litigation involving cyber fraud losses.

What This Means to You

In light of the supplement, banks should assess or reassess customer cyber risk, implement any additional layered security measures currently available under the bank's technology service contracts, and review with vendors or in-house technology departments any needed security upgrades (and costs of upgrades) to current technology contracts to cover the new requirements. Going forward, it is essential that banks review their current controls against the principles outlined in the guidance and the supplement and, if necessary, develop and implement appropriate action plans to strengthen and enhance their controls.

Even if the bank implements the appropriate controls, banks will likely find it difficult convincing all customers to agree to use some form of security. Allowing transactions without the recommended security procedures, however, presents unnecessary risk to the bank. Banks might use the topic of their security measures as a positive market differentiator as customers who use online banking likely choose banks that offer superior security measures. To mitigate any potential risk in the event a customer declines the bank's security measures, the bank should obtain a signed waiver by such customer.

[1] See www.ffiec.gov/pdf/Auth-ITS-Final%206-22-11%20(FFIEC%20Formated).pdf (last visited Dec. 30, 2011).

[2] See www.ffiec.gov/pdf/authentication_guidance.pdf (last visited Dec. 30, 2011).

[3] The FFIEC has directed examiners to formally assess banks under the enhanced expectations outlined in the supplement beginning in January 2012.

[4] "Cyber Security: Threats to the Financial Sector," Testimony before the House Financial Services Committee Subcommittee on Financial Institutions and Consumer Credit by Gordon M. Snow, Federal Bureau of Investigation, Sept. 14, 2011.

[5] Please note that other regulations and guidelines also specifically address banks' responsibilities to protect customer information and prevent identity theft. See Interagency Final Regulation and Guidelines on Identity Theft Red Flags, 12 CFR parts 41, 222, 334, 571, and 717; Interagency Guidelines Establishing Information Security Standards, 12 CFR parts 30, 208, 225, 364, and 570, Appendix B.

[6] "Out-of-wallet" questions are ones that do not rely on information that is often publicly available.

[7] 677 F. Supp. 2d 994 (ND Ill. 2009).

[8] *Patco Construction Company, Inc., v. People's United Bank d/b/a Ocean Bank*, 2011 WL 217450 (D. Maine May 27, 2011), aff'd., No. 09503PH (D. Maine Aug. 4, 2011).

For more information, contact Jeff Makovicka at Husch Blackwell LLP at (402) 964-5000 or jeff.makovicka@huschblackwell.com. Makovicka is a member of Husch Blackwell LLP's Banking & Finance practice where he concentrates on bank regulatory matters.