Davis Wright Tremaine LLP

FFIEC Releases New Authentication Guidance for Online Banking

By Andrew J. Lorentz and Richard A. Gibbs

July 06, 2011

On June 28, 2011, the Federal Financial Institutions Examination Council (FFIEC) issued a Supplement to the *Authentication in an Internet Banking Environment* guidance first issued in Oct. 2005. The FFIEC considered that further guidance was appropriate due to the continued growth of electronic and mobile banking and greater sophistication of the associated threats, which have increased risks for financial institutions and their customers.

The Supplement reflects the FFIEC's view that the controls in its previous guidance have become less effective over time as criminals have used techniques such as "corporate account takeover" to inflict large losses on banks and their customers for online banking services. The new guidance is expected to spur adoption of enhanced authentication technologies and controls, particularly for smaller financial institutions that may not have invested as heavily in advanced security technology as the largest banks.

Specifically, the Supplement:

- Reiterates the risk-management framework described in the 2005 guidance;
- Identifies customer authentication techniques that are less effective in the current environment and calls for enhanced measures;
- Outlines minimum layered security control elements for online banking activities; and
- Sets forth specific minimum elements that should be part of an institution's customer awareness and education program.

A link to the new Supplement is provided here. The FFIEC member agencies have directed examiners to formally assess financial institutions under the enhanced expectations outlined in the Supplement beginning in Jan. 2012.

Specific supervisory expectations

Risk Assessments. The FFIEC member agencies expect that financial institutions will 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.

Customer Authentication for High Risk Transactions. The FFIEC member agencies expect that financial institutions will implement more robust controls as the risk level of the transaction increases. Financial institutions should implement varying levels of layered security (as discussed briefly below) consistent with the risk level of the transaction. In addition to layered security, the Supplement recommends that financial institutions offer multifactor authentication for their business/commercial banking customers.

In its 2005 guidance, the FFIEC stated that authentication methods that depend on more than one factor of the following authentication factors are more difficult to compromise than single-factor methods:

- Something the user knows (e.g., password, PIN);
- Something the user has (e.g., ATM card, smart card); and
- Something the user is (e.g., biometric characteristic, such as a fingerprint).

The FFIEC clarified its position in its Aug. 15, 2006 FAQ supplement, rejecting such single-factor approaches as challenge/response approach and shared secret images. The FFIEC pronounced that true multifactor authentication requires the use of solutions from two or more of the three categories of factors and that using multiple solutions from the same category would not constitute multifactor authentication. For example, requiring that the user insert a smart card into their PC (something the user has) and enter in a password (something the user knows) would be two-factor authentication. Requiring a valid fingerprint via biometric fingerprint reader would add a third factor.

Ineffective Authentication Techniques. Financial institutions should no longer consider simple device identification (such as cookies placed on a customer's PC, IP addresses, or geo-location information) to be an effective risk mitigation technique. The FFIEC member agencies consider complex device identification to be more secure and preferable to simple device identification. Complex device identification, also known as "digital fingerprinting, incorporates a number of characteristics such as PC configuration, IP address, geo-location, and other factors. Similarly, financial institutions should not rely on challenge questions based only on personal information of the customer, given the amount of such information that is now publicly available. Challenge questions should include information that is not publically available and should include a "red herring" question which the customer (but not the fraudster) will recognize as nonsensical.

Layered Security Program. The FFIEC member agencies expect that financial institutions will implement a layered security program for high-risk Internet-based systems. Essentially, this means using different security or access controls at different points in the transaction process. At a minimum, a financial institution's layered security program should contain the following two elements:

1. Controls and processes designed to detect anomalies and effectively respond to suspicious or anomalous activity related to (i) initial login and authentication of customers to financial institution's systems and (ii) initiation of electronic transactions involving the transfer of funds to other parties. The Supplement notes that a number of fraudulent transactions were plainly anomalous when compared to the normal transaction profile of the associated account and so could have been prevented by more robust and frequent monitoring and controls. Further, the ability to "white list" payees and establish "positive pay" programs that identify the accounts to which funds may be transferred are also recommended.

2. For business accounts, enhanced controls for system administrators who are granted privileges to set up or change system configurations, such as setting access privileges and application configurations and/or limitations.

Some examples to be used in a layered security program include:

- Using one-time password tokens or USB tokens;
- Using out-of-band authentication or verifications;
- Establishing, requiring and periodically reviewing volume and value limitations or parameters and time-of-day restrictions for what activities a business customer in the aggregate, and its enrolled users individually, can functionally accomplish while accessing the online system;
- Establishing individual transaction and aggregate account exposure limits based on expected account activity;
- Using transaction monitoring/anomaly detection software and alerting on exception events;
- Establishing payee whitelisting (e.g., positive pay) and/or blacklisting;

- Requiring every ACH file originating entity to provide a proactive notice of intent to originate a file prior to its submission; and

- Requiring business customers to deploy dual control routines over higher risk functions performed online.

Customer awareness and education

- 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;

- 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;

- A suggestion that commercial online banking customers perform a related risk assessment and controls evaluation periodically;

- A listing of alternative risk control mechanisms that 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 they notice suspicious account activity or experience customer information security-related events.

If you have any comments or would like more information please contact Andrew J. Lorentz, James H. Mann, Randy Gainer, or Richard Gibbs.