

New Internet-Security Standards for Financial Institutions



NEIL J. SMITH

VIEWPOINT

The Federal Financial Institutions Examination Council (FFIEC) — a group of federal financial regulators empowered to issue uniform standards for most of the financial institutions in the United States — issued new guidelines to the nation's federal credit unions, banks, and other financial institutions. It notified them that they will have to comply with new Internet-security standards.

Credit unions were required to comply with the new standards by Jan. 1, 2011.

The FFIEC laid out these new standards in a supplement that is an update to guidance on Internet security that it had is-

sued in 2005, entitled "Authentication in an Internet Banking Environment."

The original 2005 guidance

The 2005 guidance provided a risk-management framework for financial institutions offering products and services to their customers through the Internet. It required financial institutions to use effective methods to authenticate the identity of customers.

It also required financial institutions to implement Internet-security techniques commensurate with the risks associated with the products and services offered and the importance of the protection of sensitive

consumer information.

The 2005 guidance also provided minimum supervisory expectations for effective authentication controls applicable to high-risk online transactions involving access to consumer information or the movement of funds to other parties (such as automated payments and other electronic-funds transfers).

In addition, the 2005 guidance required financial institutions to perform periodic risk assessments and adjust their Internet-security control mechanisms as appropriate in response to the ever-changing threats from cybercriminals.

New supplement requirements

The purpose of the supplement to the 2005 guidance is to reinforce the guidance's risk-management framework and update financial regulators' expectations regarding customer authentication, layered security, and other controls in the increasingly hostile online environment.

The supplement reiterates the FFIEC's expectations outlined in the 2005 guidance that financial institutions must perform periodic risk assessments that consider new and evolving threats to online accounts and adjust their customer authentication, layered security, and other controls as appropriate in response to identified risks.

The supplement 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 a financial institution's customer awareness and education programs.

Update Internet risk assessments

The first specific expectation for financial institutions in the supplement is that they will be required to renew and update their Internet-security risk assessments whenever new threat information becomes available or whenever they introduce new services.

Even if financial institutions do not introduce any new online services or receive any new threat information, at a minimum they will be required to review their risk assessments at least once a year.

These updated risk assessments should consider changes in the threat environment, changes in the customer base using electronic services, changes in the way banks and credit unions deliver those services, and any actual experiences of security breaches by the financial-services industry.

Provide layered Internet security

In addition, the supplement requires financial institutions to provide layered Internet security. The intent is that the strength of other security barriers can compensate for vulnerable security controls.

It is expected that security programs will, at a minimum, contain processes to detect and effectively respond to suspicious activity when a consumer logs into his/her account or initiates an electronic transfer.

It is expected that there will be enhanced controls for system administrators who are granted privileges to set up or change system applications related to business accounts.

Credit unions and banks will be required to utilize controls to cover both initial account access and subsequent account-transaction processing if they engage in "high risk Internet transactions."

High-risk transactions are defined to include automated-payment services and commercial financial services. Given this broad definition, it is likely that most financial institutions will fall into this category.

Educate consumers

Finally, credit unions and banks will be

See SMITH, page 12

SMITH: They will have to advise consumers about the protections provided

Continued from page 10

required to educate consumers.

First, they will have to advise consumers about the protections provided, as well as the protections *not* provided by Regulation E, the federal regulation governing elec-

tronic fund transfers.

Second, they will have to disclose to consumers that they will be asked to provide their electronic-banking credentials, and that they will contact the authorities when they detect suspicious account activity.

Aside from technical guidance, this new

set of rules for credit unions and banks is a clear reminder that preventing fraud continues to be a significant goal of federal regulators.

It is also a reminder that Internet-security measures will not only have to withstand attacks by hackers, they will also have to with-

stand the scrutiny of federal officials. □

Neil J. Smith is an attorney with Mackenzie Hughes LLP in Syracuse and handles business, bankruptcy, and creditor's rights issues for a variety of clients. Contact him at (315) 233-8226.