Easy Solutions News

Six Steps to 2011 FFIEC Authentication Compliance

For the first time since 2005, the FFIEC has released new guidelines for authentication in an Internet banking environment. Compliance assessments begin January 1, 2012. This document outlines the six steps financial institutions should take to conform to the new FFIEC authentication guidance.

STEP 1: Take regulations seriously

It is imperative for financial institutions to start working towards compliance today as full compliance will likely take longer than 180 days. Institutions that demonstrate that they did take the guidance seriously will likely have a much easier time with the regulatory agencies. It is estimated that 80% of the financial institutions in the United States have very weak security and thus have a lot of work to do.

STEP 2: Complete first risk assessment and plan for additional assessments

FFIEC guidance stresses the need for periodic risk assessments. Institutions are expected to reassess their security whenever they offer new electronic banking services, when substantially new threats arise, or at least every 12 months. Complete a risk assessment as soon as possible and then develop an action plan and a timeline as follow-up.

STEP 3: Identify compliance gaps

The FFIEC document is well-written and easy to follow thus there are no excuses for not identifying compliance gaps. After reading the document, institutions must look at their online banking platform honestly and objectively and ask themselves "how many security layers do we have in place."

STEP 4: Evaluate layered security solutions

Institutions should investigate and trial various solutions that address the compliance gaps identified in Step 3. Institutions should pay extra attention to business account solutions as the guidance emphasizes a risk-based approach. Business accounts typically have more money than consumer accounts, and thus the controls must be tighter.

STEP 5: Implement layered security system

The guidance emphasizes that virtually every authentication technique can be compromised, so it's important to have a layered system (if one layer is breached, additional layers provide backup). At a minimum, a layered security program should be designed to detect strange or unusual behavior when the customer is logging in to the system, **AND** when initiating electronic transfers to third parties. See Easy Solutions Three Layers of Security Document for additional information.

STEP 6: Provide customer awareness and education campaigns

Institutions should direct customer awareness and education efforts at both retail and commercial account holders. In particular, discuss the applicability of Regulation E to accounts with Internet access and explain how/when (if at all) electronic banking credentials will be requested. The following is also recommended:

- Suggest commercial online banking customers perform their own risk assessments
- Provide a list of available risk controls that customers may consider implementing
- Provide a list of institutional contacts for customers' use in the event they notice suspicious account activity

For more information please contact:

David Sylvester
Business Development Manager, North America
dsylvester@easysol.net
Main: + 1 (866) 524 4782 Ext. 103
Mobile: + 1 (302) 463 3209

EASYSOLUTIONS
TOTAL FRAUD PROTECTION®