Electronic Funds Transfer Fraud:
How it affects your customers – and how to prevent it

By Marv Chen, AuditOne, LLC

The number one most significant risk scenario that we have seen in the past year or two is online electronic payment fraud. There has been an extremely high incidence of occurrence of such fraud with banks that allow wire transfer or ACH origination over the Internet. The risk has been so severe that the FFIEC on June 28, 2011 released the Supplemental Guidance and Internet Banking Authentication.

It’s not that banks aren’t doing what they can to prevent or detect this, but rather that criminals are attacking the weakest link in the chain: the customers themselves. Unlike banks, which are required by GLBA law and other regulation to have strong information security controls in place, customers are not forced to implement such controls. For bankers, it’s certainly a challenge to maintain a delicate balance between keeping banking systems secure and yet providing ease-of-use for customers.

In order to better ascertain the risks, we need to understand how it happens. Typically, a customer computer (the one being targeted for fraudulent electronic funds transfers) is compromised via targeted-phishing or similar social engineering techniques. Accidental exposure to malware is also possible. Malicious software (such as rootkits, keystroke loggers, or man-in-the-browser programs) is inserted into the target computer. Once these types of malware are installed, the target computer is effectively compromised. Because of the targeted nature of these attacks, anti-virus software may not yet even have the capability to detect the malware. The customers have absolutely no idea that their computer has been compromised.

In many cases, these attacks are quite sophisticated and often performed by organized criminals outside of the country. Less often, these attacks are performed by insiders with intimate knowledge of the wire transfer application and access to the computers.

To sum up the recent FFIEC guidance, we recommend starting with a risk assessment. A risk assessment is critical because this particular risk may not apply to you. For example, if your bank is not allowing funds transfers through the Internet, it’s certainly not an issue. Or if your bank requires callback on every wire transaction, you already have a very strong mitigating control. The FFIEC also recommends a layered security approach – that is to consider the following: multi-factor authentication, dual authentication, out-of-band notification (telephone callback, text-message wire notification, etc.), fraud detection and monitoring, and enhanced customer education.

Additionally, we recommend strengthening customer identification procedures. In one case we examined, a “low tech” method of pre-text calling was used to change customer contract information. The attacker then proceeded to take the identity of the victim and use the customer’s online account to send a fraudulent wire. Needless to say, as we have been saying for years, mother’s maiden name, date of birth, and even social security number are not
secure. These can be easily obtained. Finally, recently changed customer information and password reset should be monitored. We've seen a lot of recent regulatory findings related to this last issue of monitoring.

Finally, we would like to emphasize again the need to keep customers aware of their need to keep their computers secure and to follow policy and good practices (don’t share logins on a dual authentication system; avoid dual-purpose computers – business and gaming, etc.). As stated above, it’s not an easy task maintaining ease-of-use for the customer while keeping a strong information security stance.

<back to March 2012 Technology & Security Digest>

Marv Chen is technology practice director for AuditOne LLC. He can be reached at Marv.Chen@audit-one.com.