



Electronic Fraud Awareness Advisory

Indiana Bankers Association
Fraud Awareness Task Force
February, 2012

Electronic Fraud Awareness Advisory

Purpose/Summary

The Indiana Bankers Association (IBA) was involved in meetings and discussions with the Indiana Dept. of Financial Institutions (DFI) and the Indiana State Board of Accounts (ISBA) during the last quarter of 2011. These meetings were to address recent fraudulent activity occurring within electronic banking activities, including ACH Transactions and Payroll Initiations originated through Municipality and School accounts, from throughout the state of Indiana. After these discussions and interviews with the affected financial institutions, it was determined these fraudulent activities had occurred in various methods including keylogging malware, man-in-the middle (MIM) or man-in-the browser (MIB) attacks, or simple facsimile requests.

It is believed that municipalities and schools were chosen as the victim in these occurrences due to having larger amounts of money flow through their accounts on a regular basis, while often being limited in the area of IT security measures and adequate staffing. This issue can also be the case, many times, with small business deposit clients of banks. Due to these factors, it is often in the best interest of the bank to provide awareness and training in the area of Basic IT Security for their clients.

The IBA formed a task force comprised of bankers throughout the state, along with representation from the DFI and the ISBA to meet and review the issues. During those meetings, it was determined there is not one "fix" for all financial institutions, nor is there one "fix" for all clients. The solution will depend on the size and complexity of the bank client and their transactions, as well as the size and complexity of the bank itself. However, the task force did determine that it would be beneficial to create and distribute an Awareness Reminder document that, (1) highlights the recent FFIEC Guidance on this topic, (2) discusses the threats and potential breakdowns to various methods of control, (3) provides suggestions for customer awareness and education, and (4) reminds banks to Know Your Customer and their "normal" activities.

FFIEC Guidance

The FFIEC issued a guidance supplement on June 28, 2011, updating the initial guidance released in October 2005.

[FFIEC Online Banking Security Guidelines Supplement
www.ffiec.gov/press/pr062811.htm](http://www.ffiec.gov/press/pr062811.htm)

This supplement describes updated supervisory expectations regarding customer authentication, layered security and other controls in an increasingly hostile online environment. Compliance with this supplement was to occur by January 1, 2012. Banks are expected to perform yearly risk assessments, implement layered security controls, and be more active in their customer awareness and education efforts.

Financial institutions should perform periodic risk assessments and adjust their customer authentication controls as appropriate in response to new threats to customers' online accounts. They should also review and update their existing risk assessments periodically, as new information becomes available, and prior to implementing new electronic financial services. These risk assessments should consider the changes in the internal and external threat environment.

Financial institutions should implement layered security controls consistent with the risk associated to the consumer or business transactions. Institutions are also to offer multifactor authentications to their business customers. Layered security programs utilize different controls at different points in a transaction process so that a weakness in one control is generally compensated for by the strength of a different control. Such controls may include: monitoring systems that include consideration of the customer history and behavior, dual customer authorization through different access devices, out-of-band verification, “positive pay” or debit blocks to limit transactional use of account, transactional value or number of transaction thresholds, internet protocol reputation-based tools, and controls over customer account maintenance activities. The layered security program should detect and respond to suspicious activity, as well as provide additional control of administrative functions involving the client’s account.

In the area of customer awareness and education, the financial institution should explain the protections provided, and not provided, to account holders relative to electronic funds transfers and Internet access. The institution should explain when and how, if at all, they will contact a customer on an unsolicited basis requesting the customer’s electronic banking credentials. The bank should suggest that commercial clients perform an internal electronic risk assessment and controls evaluation; and provide the client with a listing of alternative risk control mechanisms. Finally, the bank should provide a list of appropriate bank personnel to contact in the event they notice suspicious activity or security-related events.

Threats and Methods of Compromise to Online Security Controls

Criminal online account takeovers and resulting ACH and wire fraud begin with the compromise of online banking customers’ computers. The compromise of computer operating systems and browser applications leads to total online banking account control – defeating even the most sophisticated security controls, including dual control authorization. There are several off-the-shelf crimeware products available to compromise customer computers, defeat multiple security controls, and transfer funds to money mules that facilitate the movement of those funds beyond the reach of financial institutions and law enforcement.

Many of the security controls that were initially put in place with the implementation of online banking have become too simplistic in their efforts, with the development of the crimeware mentioned above. Often attackers gain access to a PC when a user visits an infected website or clicks on an infected website banner. Below are some of the initial security control methods and what fraudsters are doing to penetrate the security measures.

Security and Challenge Questions – Criminals use keylogging malware to record the keystrokes entered on a PC and transmit a record of those keystrokes to the person controlling the malware over the Internet. With these methods, criminals can automate the mass collection of secret security and challenge questions. Content injection using MIB attacks, placing the fraudster between the customer and the financial institution, can also be used to force security question entry and facilitate harvesting. These methods can also obtain personal information authentication details through the desktop browser.

Authenticated Browser Sessions – After compromising the customer’s computer, criminals are able to maintain an authenticated online banking session even after a user has selected to logout. This attack allows criminals to conduct fraudulent transactions in a fully authenticated environment.

Multi-factor Authentication – After having control of the desktop operating system and browser applications, criminals are able to bypass two factor authentication controls using real-time monitoring and content injection. These methods allow criminals to receive passcode and PINs. Time-bound credentials can be obtained through keylogging, or content injection using MIB methods. Criminals will

often distract users with offline maintenance notices or website unavailability notices and then use the passcodes before they expire. Another method is payment modifications into an authenticated channel using MIM attacks, bypassing one-time passcode tokens.

Dual Account Controls – If the criminal compromises a user's computer, malware easily spreads and often the criminal will have access to, or control over, multiple computers within a network. By doing so, criminals are successfully defeating controls requiring two or more authorizations for ACH and wire transactions.

Detection and Prevention Controls

Financial institutions should research and determine controls that may be more effective in detecting and preventing attacks as part of the institution's layered security program. Based on the information above, it can be seen that none of the controls provide absolute assurance in prevention or detection. Some possibilities include:

Anti-malware software – This is software that is commonly called anti-virus or anti-spyware and is used to prevent, detect, block and remove adware, spyware, and other forms of malware such as keyloggers and MIM/MIB attacks.

Transaction monitoring software - Systems are available to monitor online banking activity for suspicious funds transfers. They can stop a suspicious ACH/wire transfer before completion and alert the bank and/or the customer so the transfer can be further authenticated or dismissed. This software tracks and compares the customer's established patterns of behavior, the size of transaction and the timing of transactions. Another control often used is an approved funds transfer recipient list. This is created by the customer and maintained by the bank to monitor and approve a requested funds transfer against the list of recipients.

Out-of-band authentications – This process involves a transaction that is initiated via one delivery channel, such as the Internet, and then must be re-authenticated or verified via an independent delivery channel, such as the telephone, in order to complete the transaction. In order to raise the level of authentication, many out-of-band authentications or verifications must be provided by a second person, other than the one who initiated the transaction, and completely independent of the initiation function.

Secure browsers for clients, via USB devices – Financial institutions provide their client with a USB device that is plugged into the client's computer. When device is inserted it will enable a secure link between the client's PC and the financial institution, independent of the PC's operating system and application software.

Customer Awareness and Education

As mentioned previously, customer awareness and understanding may be limited in these areas. Financial institutions have a responsibility to educate and inform their customers of potential threats and risks that may be associated with the use of Internet banking alternatives for both the consumer client and the business client. Some possible solutions are: a checklist of discussion points upon completion of the Internet banking application; a customer-signed document discussing what protections are provided and/or included with the Internet banking product; bank sponsored community awareness sessions; or lunch and learn sessions for customers.

If a customer is unable or unwilling to gain the appropriate education or awareness of the risk involved in Internet banking or Internet banking services, it may be in the best interest of all parties involved to not

allow the client to have the Internet banking privileges. This action, while seeming harsh, will protect the client and the bank from the many potential threats and fraudulent activities that may occur with the inappropriate use of Internet banking activities.

Some topics that may be included in a checklist or document discussing Internet banking may include:

- Report to your IT staff, or the Bank, any activity that seems suspicious (last login date is incorrect, you receive challenge questions on a registered computer, you are asked challenge questions for which you are unfamiliar, you receive a message that the system is “unavailable”, you are asked to re-enter token information at odd times.)
- Report to your IT staff, or the Bank, if you experience slow response times during the login process.
- Do not share passwords. Each user should have a unique login ID.
- Notify Bank when an employee with online banking access has left the company.
- Change your passwords frequently and don't give your passwords to anyone, not even the bank. Be sure to create passwords that are difficult for others to guess. Select your password by using random letters, numbers and symbols.
- Ensure that no one is watching when you are entering your online User ID and Password.
- Remain at your computer until your online banking transactions are completed. Log off the online banking product prior to accessing other Internet sites.
- Use virus and spyware protection software and other Internet security software on your computer. Keep these software tools up-to-date with the most recent versions.
- Keep your computer software up-to-date.
- Use a software or hardware firewall to protect your computer from intrusion.
- Make sure your wireless network, if applicable, is secure and utilizes proper encryption tools.
- Be cautious of any email that you receive from people that you do not know. Do not open or download any attachment that may be included with this email.
- Do not send any confidential information through regular email.
- Limit User Administrative Rights including uploads, downloads, installations, etc.– This protects against the inadvertent download of malicious software and viruses.
- Do not access personal email accounts through a business computer.
- Consider a stand-alone PC for online banking.
- Consider a Cyber Insurance Policy to help cover you in the event of fraud.

Know Your Customer

Knowing your customer is always important, in every area of the bank, but it is crucial in the area of Internet banking and ACH transaction activity. Since the client is accessing your bank without being visible to any staff member of the bank, knowing the client's “normal” activities, types of transactions, amount of transactions and destinations for transactions is very important. Based on knowing your customer, at the first hint of something out of the ordinary, always take the extra step and review the matter with fellow bank staff and/or verify the transaction verbally, or in person, with the client.

1) FFIEC - Supplement to Authentication in an Internet Banking Environment
2) Ironkey - Methods to Compromise Online Security controls Using PC-based Crimeware
3) Trusteer - Addressing Customer Concerns from Financial Trojans
4) Banker Online