CORPORATE ACCOUNT TAKEOVER

Traditional Protection Strategies Not Enough; Multi-Dimensional, Preemptive Strategies Needed

Fraud Could Cost American Companies $1,000,000,000 This Year.

First reported in 2006, Corporate Account Takeover is a form of financial fraud where criminals (aka fraudsters) using electronic means redirect money transfers for legitimate business payments to either their own accounts or the account of "money mules" by adjusting the account and routing numbers of the legitimate payees. Initially, criminals executed Corporate Account Takeover by creating new ACH files; as time has gone by these perpetrators have transitioned to manipulating the content of existing batches. Account information changes can be so innocuous that they go unnoticed until potentially irreparable damage has been done to an organization, its finances, and reputation.

The FBI estimates Corporate Account Takeover could cost American companies as much as $1,000,000,000 in 2011 alone. Originally targeting larger corporations, fraudsters using Corporate Account Takeover methods have redirected their efforts toward small- and medium-sized businesses as well as municipalities and non-profit organizations. These smaller organizations lack the resources to defend against, detect a breach and repair the damage to reputation and finances that larger organizations can protect against.

According to the Ponemon Institute's 2010 *Business Banking Trust* survey, 80 percent of financial institutions were oblivious to fraud until ***after*** funds had been transferred out of the institution. A majority of businesses affected by Corporate Account Takeover, 57 percent, were unable to recover all the resources lost to fraudsters. Each case of Corporate Account Takeover can represent a $100,000 to $200,000 loss for small to midsize businesses; some cases have even gone into the millions of dollars; as a result, 40 percent of businesses victimized by fraud moved their banking activities to another institution.

How Corporate Account Takeover Occurs

Corporate Account Takeover is essentially a five-step process. The fraudsters begin by targeting their victims by using various phishing techniques like mass emails, pop-ups, or faux-friend requests. With these phishing techniques fraudsters hope a victim will expose themselves to malware by responding to the various outreach attempts.

Becoming infected with malware can be as simple as clicking on a bad link and probably invisible to the user of the computer. A computer user can become a victim by opening an attachment on an email, logging on to a legitimate website that has been compromised or responding to a malicious email that has requested personal information.

Once the malware has been downloaded, it will run in the background unnoticed until the computer user logs on to his or her online financial institution account. Once the malware acquires a user's online financial institution credentials; it transmits the information to fraudsters who use the information to initiate unauthorized fund transfers away from the victims account.

Traditional Protection Strategies Are One Dimensional

Education has been the primary preventative prescribed by experts in both government and industry publications. This is essential but this one dimensional approach needs to go further. Teaching users about the risks associated with opening unsolicited attachments, and how clicking on pop-ups and cruising social networking sites on machines is a good place to start. But financial institutions need a more practical and effective preemptive strategy. Trying to train, monitor and discipline every person within an organization to proper online usage is unrealistic; there are simply too many variables and it only takes one mistake to invite malware onto a machine.

Enhanced security measures such as limiting functions computers can perform as well using spam filters have been suggested. Filters and firewalls can be breached and implementing security procedures such as dual payment controls remain cumbersome and time consuming.

Security tokens and use of One Time Password (OTP) technology have been used to hamper the efforts of cyber criminals. Security tokens and OTP work by having a designated password for only a short period of time, for the purpose of authenticating a user attempting to access a financial institution application; however, many malicious software applications and Trojans are now capable of acting autonomously from the end user's personal computer. With the ability to act on their own some Trojans are able to inflict their damage before an OTP clearance expires.

Out of Band Verification (OOB) has become the industry best practice for verifying access. With some 40 percent of personal computers being infected with some form of malware, phone verification is seen as the most secure way to authenticate a user. However, manual user verification by phone adds yet another step in the authentication process, seen by many Originators as another hoop to jump through.

Even following all the prescribed preventative measures for defending against Corporate Account Takeover does not provide air tight protection for organizations using electronic means to transfer funds. Computers cannot always be monitored and even dedicated equipment can fall prey to corrupted site at no fault of a local user. The only way to eliminate the threat from fraudsters is to employ multi-dimensional, preemptive strategies that verify transactions once they arrive at the Originating Depository Financial Institution **and** before they are released to the ACH Operator.

There's A Cure for Corporate Account Takeover

Trying to manage verification of all transactions between an originating organization and the ODFI manually would be a daunting, if not impossible, task for an army of analysts. It would be cost prohibitive for most institutions. But where does the responsibility for online banking security lie? Yes, it is the responsibility of each individual organization to try to protect their own financial interests; but if we are looking for a solution on a systematic level there are just too many variables in this "every-man-for-himself" environment.

While it might be perceived that there may be little legal responsibility on the part of financial institutions to defend against some types of fraud, there is a responsibility to offer "commercially reasonable" solutions to safeguard the resources they have been entrusted with and that they use as a means of generating profits. If financial institutions do not act to provide reasonable protections to protect funds and inspire confidence; legal battles will continue to be fought and the government will begin to legislate how institutions must act.

The reality is financial institutions are in a better position to implement system wide safeguards. They have the ability to isolate equipment, set restrictions and enforce protocols that individual businesses may not. Industry experts have suggested the following technologies be implemented by financial institutions to protect their clients:

- A secure environment that's tamper-proof, portable, and easy to use for all types of commercial financial institution clients
- A secure web browser that isolates banking sessions from the rest of the computer to prevent malware from taking control
- Two-factor authentication to increase the assurance that the user is authorized to access online commercial banking
- Anti-malware to scan the user's computer before launching a secure environment to eliminate as many possible threats as possible
- Automatic updates to keep systems updated with the latest threat protection
- Analytics to provide updates on client usage and the threats observed to drive anti-fraud and risk management decisions

For too long the attention has been given to *individual measures* to try and stop cyber-criminal activity. Use of Dual-factor authentication, OTPs and OOB methods, used simply for verifying users' authorized access to a funds transfer system, have their own vulnerabilities and they do not address manipulation of transactions once access has been granted. Financial institutions should look toward leveraging the strengths of each of these techniques by creating a series of security protocols *within a transaction verification system* to eliminate the threat of Corporate Account Takeover.

An automated solution to transaction verification is greatly needed to stem the tide of unrecoverable monies being lost to fraud. But what will this automation look like. The solution will leverage OOB methods, but OOB should be used to send out-of-band *alert*s to an Originator when a suspect transaction is detected. The Originator contact information must be controlled by the financial institution and be inaccessible by the Originator in order to prevent information from being changed by a fraudster in an effort to re-directed alerts.

Verification of every outgoing credit transaction must be performed. The only reasonable method for validating an out-going credit is to compare it against a pre-approved list of payees, with payees being defined by a routing number/account number combination. To prevent manipulation by a fraudster, the payee list should only be populated by a financial institution and then verified by the Originator. Furthermore, the Originator should never have access to populate or modify the contents of an issuance file.

The Originator's role should be limited to verification of issuance file contents, after receiving an OOB alert, logging in using multi-factor authentication and then, in the last step of verification, entering an OTP. Any approval granted by the Originator, must be followed up with an out-of-band confirmation alert.

Once payees are verified by an Originator, each subsequent live credit entry should be compared against the issuance file to ensure new routing number and account number combinations are not present. If they are introduced, the batch should be suspended and the system should create a random OTP and send an alert via the out-of-band method to the Originator. Because the OTP transmitted can only be used to verify the transaction that has already been received by the financial institution's server and cannot be altered from the outside, this OTP is of no use to a criminal. In theory, sending OTPs by SMS should hence be as effective a fraud prevention measure as a key generator. It should be noted that financial institutions have experienced that the weak point is the mobile phone identification.

Effective fraud prevention is only provided if any change of mobile phone number is performed by the financial institution and only after thorough identity checking.

The technology and techniques to make Corporate Account Takeover a thing of the past exist. The question is: When will financial institutions take advantage of the immediate opportunity to protect their clients, reputations, and ultimately secure confidence in our economic system? Can we continue to tolerate these potentially cataclysmic risks and losses?

References

Chickowski, Ericka. (Oct 5, 2010). *Security Dark Reading.* 'Man in the Mobile' Attacks Highlight Weaknesses in Out-Of Band Authentication. Retrieved from http://www.darkreading.com/authentication/167901072/security/application-security/227700141/index.html.

Consumer Affairs. Financial Fraud Hits 7.5 Percent of Americans in 2008. Retrieved from http://consumeraffairs.com/news04/2009/03/financial_breach.html.

Fraud Advisory for Businesses: Corporate Account Take Over. Retrieved from http://www.ic3.gov/media/2010/corporateaccounttakeover.pdf.

INFORM, Institut Fur Operation Research Und Management GmbH. How Can A Bank Prevent Online Banking Fraud. Retrieved from http://www.internetbankingfraud.com/.

McGlassen, Linda. (July 8, 2010). Bank Info Security. Account Takeover: The New Wrinkle. Retrieved from http://www.bankinfosecurity.com/articles.php?art_id=2728.

Tripier, Dave. *The Ethical Hacker*. Organized Cyber Crime and Corporate Bank Account Takeovers. Retrieved from http://www.ethicalhacker.net/content/view/335/2/.

Vijayan, Jaikumar. (Oct 4, 2010). *Computerworld*. Retrieved from http://www.computerworld.com/s/article/9189201/Money_mule_arrests_highlight_banks_efforts_to_fight_fraud.

Wilson, Tim. (Oct 21, 2010). *Security Dark Reading*. FBI Warns of Corporate Account Takeover Scam. Retrieved from http://www.darkreading.com/smb-security/167901073/security/perimeter-security/227900529/index.html.