

Fraud Alerts

ACH BATCH FRAUD INCREASING

Arkansas Bankers are reporting a recent upsurge in ACH batch fraud and we wanted to take this opportunity to be sure it's on your scope of carefully-watched items. We think this merits your attention.

This scam starts with a customer (usually corporate) who gets a keylogger virus on their computer, causing every keystroke to go unencrypted to an unintended source. The fraudsters collect data such as account numbers and passwords, then use this to initiate an ACH batch from that customer to banks across the U.S. It will be dumped into accounts where they have already hooked someone into believing they are "working-at-home." The customer receiving the funds has already given their account information out in the hope of getting rich redistributing funds for a company overseas. In reality, they are instructed to wire or MoneyGram the funds as soon as it is received, keeping a small percentage for their "work." The funds will then be in the hands of fraudsters who are out of our country and cannot be easily investigated and prosecuted. The trail of money is difficult to trace when funds are wired through Western Union.

Losses before detection of the fraudulent ACH batch often rise to the \$150,000 to \$200,000 range. We have recently seen them starting with lower amounts (\$35,000 to \$50,000) and then trying multiple attempts in that range. If you or your customers detect the fraud immediately after funds are wired, you have a good chance of recovering the funds. If, however, it has been as long as even a day or two, there can be substantial unrecoverable losses. These losses are usually taken by the customer, but some bankers have opted to take the losses themselves rather than have the bad publicity that could accompany a large loss to a customer. It is common to see school districts targeted this way and their budgets are usually strained anyway without this type of loss.

What can our banks do to limit exposure to ACH batch fraud? It requires a three-pronged approach. First, since the initial point of compromise resides with your customer (malware or virus on their computer), the first step should be education of your customers who make ACH batch payments. They need to be aware of the hazards of clicking on hyperlinks in e-mails

from unknown sources and of pop-up boxes purporting to be from your financial institution. For this reason, staff should never open e-mails from anyone they do not know and have a reason to trust. Antivirus software alone is no protection in many instances. Many of our banks are now doing training at the retail customer level to acquaint them with frauds of which they need to be aware. They should also understand that these crimes are not a rarity and are occurring with regularity right here in Arkansas.

Second, your bank (as the originating deposit financial institution) should make every effort to protect your ACH batches. Implementing a higher level of multi-factor authentication is a positive step. Explore with your software vendors reports that would show activity out of the norm for ACH customers (customer usually has batches on first and 15th and you receive one on the eighth). Increase communication and verification with those customers regarding batches, creating your own version of positive pay on these transactions. It's all complemented with an enhanced version of Know Your Customer.

Third, on the flip side of this scam, if you are the receiving bank on this type of transaction, education once again is a large part of the response. Your customers think they have landed the perfect Internet job and may not be inclined to be suspicious. Education could include customer/community education events like the ones OBA is helping to host across the state, statement stuffers, on hold messages and brochures in the bank regarding work-at-home scams. If your customer receives a large wire that is out of the norm (usually just under \$10,000) and asks to withdraw funds immediately in cash, be politely nosy. If they mention working at home, wiring through Western Union or MoneyGram, or sending the funds out of the country, you should inform them that there is a probability that they are involved in a scam. There is also a possibility they could be prosecuted as a principal to a money laundering fraud since that is already happening in many states. Share with them Web sites where these types of scams are detailed. The links below can be helpful for this.

How can ABA help you? As mentioned earlier, we continue to provide education to both your customers and retailers. We also hope that through these fraud alerts, we can help you to be more informed and protected. If you find that you have been hit with this and funds have gone out to banks across the U.S, you will also learn that the fraudsters have become sophisticated enough to focus the transactions in large banks. This may make it more difficult to find that person who can help to recover the funds. If this is the case, contact the ABA and we can help you with networking contacts. If you want more details on how this fraud works, here are several links to articles currently on the web that more fully detail the ACH batch scam:

- * http://www.bankinfosecurity.com/articles.php?art_id=1469&opg=1
- * http://www_networkworld_com-news-2009-080609-cyber-attackers-empty-business-accounts.htm
- * www.fbi.gov/pressrel/pressrel09/ach_110309.htm
- * http://download.entrust.com/resources/download_page.cfm/24002/WP_MITB_March2010.pdf
- * www.entrust.com/news/index.php?

As you are looking to protect your banks against fraud, please also pay attention to your wire processes. Hackers in many countries overseas have become more sophisticated and pose a threat to your bank daily. Just be sure that all necessary precautions are in place, that those policies are being followed, and that you constantly train and retrain your employees. Losses in this arena can also be huge.