

ACH Fraud – Corporate Account Takeovers*

Fraudsters look for online credentials to raid small business accounts

Businesses are being attacked by malicious software in which perpetrators are attempting to obtain their valid online banking credentials. The targets appear primarily to be small business customers that are vulnerable because they do not have or do not use the most current anti-virus software or have adequate dual control over online accounts. Once a business' credentials are stolen, the perpetrator has online access to the business' account and any other funds transfer capabilities associated with the credentials.

Stealing Credentials

There are several methods being employed to steal credentials. One is to mimic the look and feel of legitimate financial institutions' websites. Users provide their credentials to these sites, without knowing that it is the perpetrator behind the website.

A second is malware that infects computer workstations and laptops via infected emails with links or document attachments. In addition, malware can be downloaded to users' workstations and laptops by visiting legitimate websites – especially social networking sites – and clicking on the documents, videos or photos posted there. The malware installs keylogging software on the computer, which allows the perpetrator to capture the user's ID and password as they are entered at the financial institution's website.

Other viruses are more robust. They alert the perpetrator when the legitimate user has logged onto a financial institution's web site, then fools the user into thinking the system is down, or not responding, when the perpetrator is actually sending transactions in the user's name.

Corporate Account Takeover

In a worst-case scenario where robust authentication is not used, once the user's credentials are stolen, the perpetrator can take over the business' account. To the financial institution, the credentials look just like the legitimate user. The perpetrator has access to and can review the account details of the business, including account activity and patterns, and ACH and wire transfer origination parameters. In other words, once an account has been taken over, a perpetrator can do virtually anything the legitimate account owner can do. They usually begin by testing their access, and once they have gained a better comfort level, they begin sending out wire transfers or ACH transactions to other financial institutions. The accounts at the other financial institutions may be newly opened by accomplices or 'mules' who withdraw the entire balances shortly after receiving the money, then send funds overseas via wire transfer or other popular money transfer services.

The perpetrators also have been known to send in "credits" to the small business customer's account, so that the balance can be inflated, offering them more money to send out. These credits coming in are from victims at other banks, adding more layers and identities to the scam.

**Courtesy NACHA*