



ACH Fraud Is Happening To Bankers You Know – NOW

Over the past year, we have seen an ever-increasing number of financial institutions caught off-guard as business customers have been targeted by criminals exploiting weaknesses in the ACH process. Criminals target businesses with computers pre-approved to initiate ACH transfers by developing “spear-phishing” emails directed at specific companies and their employees in an attempt to install malware, which allows criminals to have control of company PCs. Then they initiate funds transfers from the company’s accounts using those compromised PCs. With no other verification steps, the money is gone - usually forever. It is normally deposited into accounts of “money mules,” who, many times, are unsuspecting people that have opened accounts as part of a “work from home” plan or something similar. The criminals then have the “mules” immediately withdraw the money and forward it on to them.

In this scenario, whom do you believe is “at fault” and should be responsible for the lost money? The only real answer right now is, “it depends.” Here are some questions to help you think through this critical problem:

- What does your ACH agreement with the company say about this?
- Is the money being transferred to a location that was “not normal” for the company?
- Should you have noticed and questioned the transaction?

There will be plenty of attorneys, courts, and politicians involved before the new paradigm is established. Until then, be aware of this active fraud channel, alert your ACH clients about the issue, and decide if you need to make changes in how you handle ACH originations until more definitive guidance is finalized.

Fraudulent Automated Clearing House (ACH) Transfers Connected to Malware and Work-at-Home Scams

http://www.fbi.gov/pressrel/pressrel09/ach_110309.htm

FDIC: SA-185-2009: Fraudulent Work-at-Home Funds Transfer Agent Schemes

<http://www.fdic.gov/news/news/SpecialAlert/2009/sa09185.html>

© 2009 Reynolds, Bone & Griesbeck PLC