

Fraudsters Bank on Commercial Customers

Market Update

As we know, business accounts are no less susceptible to cybercrime than consumer fraud victims – and in many ways are more at risk. Small business banking is particularly vulnerable in the current economic climate and is a prime target for cyber thieves who know commercial banking customers are often too small to have information technology staffs able to stay current on today's security threats. Regulation E of the Federal Electronic Funds Transfer Act requires banks to reimburse consumer victims within ten days of a reported fraud, but it does not protect businesses in a similar fashion. In an alarming but not unexpected trend, some small businesses have started to sue their bankers if not made whole to their satisfaction.

In a single month this past August, no less than the FDIC, NACHA, the Financial Services Information Sharing and Analysis Center (FS-ISAC) and IT advisory firm **Gartner Inc.** all published alerts about rising Internet threats to business banking. The following month, the Senate Committee on Homeland Security and Governmental Affairs held a **special hearing** to discuss cybercriminals targeting small- and medium- sized businesses. In October, The **FBI recently reported** \$85M in attempted fraud leading to \$40M in actual losses across 205 cases reviewed and the **FDIC** released yet another alert.

Meanwhile, it's getting ugly out there. The Washington Post reported in September about a **construction firm in Maine** that is suing its local bank after cyber thieves stole more than \$500,000 from the customer in a sophisticated online bank heist. The lawsuit alleges that the bank didn't do enough to prevent the series of transfers to dozens of co-conspirators over an eight-day period in a single month. The construction firm's attorney maintains that the contract his client signed with the bank does not absolve the institution of its responsibility to protect customers from fraud under the Uniform Commercial Code.

Fraud Scheme Details

Guardian Analytics has been tracking an alarming sophistication in the schemes and methods employed by fraudsters to extract both data and dollars from online business accounts. Business banking is being targeted more frequently because criminals know that these transactions typically involve larger dollar transfers from larger balances than from individual accounts. The thieves steal in amounts under \$10,000 to avoid triggering traditional transaction alerts. The malware is sometimes so well written that the connection comes from an authorized and authenticated computer – a legitimate computer and session that has been hijacked, circumventing even token-based authentication. The fraudsters understand the intricacies of the online business banking platforms and the money is then transferred to "money mules" recruited over Internet job boards who unwittingly think they work for a legitimate company.

-The Washington Post reported that recent victims include:

- a school district near Pittsburgh that lost \$700,000
- a chemical manufacturing firm that lost \$437,000
- a Texas manufacturing firm that lost \$1.2 million.

One Guardian Analytics customer recently intercepted an attempted Automated Clearing House (ACH) transfer of \$800,000 for a business banking customer in a scheme involving more than 80 smaller transactions all set up to be sent to unwitting mules.

Aggressive and adaptable cyber criminals have elevated online fraud to be a significant risk to business customers from revenue, legal and public relations perspectives. For your institution, the threat of lost customers or worse – business victims that have filed suit against their banks – should give pause to reexamine your fraud prevention strategy.

Prevention Tips

Here are some tips for online business banking fraud prevention:

Educate management and employees on the threat. Distribute the latest fraud attack reports cross-functionally beyond the fraud team, so more stakeholders can become educated about questionable transactions as well as understand the risks to the institution should a business customer fall victim.

Be proactive. Don't let your institution wait for the law to catch up with it. At worst, avoid being sued. Meet with legal counsel to discuss procedures following a business banking fraud discovery. Know your rights should a customer ever decide to sue. At best, avoid losing lucrative customers by assuring them that you have the most effective fraud prevention solutions in place.

Strengthen your online fraud defenses. Would your current fraud system recognize online fraud like the ones detailed above? If not, it's time to bolster your security before it's too late. Security should be commensurate to the risks, which is the essence of the FFIEC authentication guidance.

Educate customers on the threat. Initiate programs to educate financial managers within small business customer organizations – forwarding the latest fraud advisories and stressing distribution to heavy online users such as the CEO, CFO and Accounting. Aim to increase general customer awareness of optional security features of your online banking platform such as dual control of transfers, and advocate use of the latest anti-malware software and security firewalls.

Review customer policies. Terms of use for ACH transactions in particular should be reviewed to ensure bank and customer obligations are clear and consistent with security policies as well as legal and regulatory requirements.

Assume that customer machines have been compromised and react accordingly. Forward-looking banks already do this by implementing sophisticated back-end fraud prevention solutions (going beyond multi-factor authentication) that look for anomalies in individual customer behavior that reveal account compromises. Don't be one of the ones still lagging behind.

For more information, please visit www.guardiananalytics.com/fraud_informer/



About Guardian Analytics

Guardian Analytics is the technology leader in the prevention of online account fraud, providing real-time risk management solutions that protect online channels. The company supports the end-to-end online risk management process with rich analytics and behavior-based modeling. We offer an analytics-based software solution that addresses the entire risk management lifecycle.