Whistleblower News Review

September 19, 2016

Failure to Report Bank Cybersecurity Breaches or Cyber Inadequacies Next Whistleblower Op

By Allison Watts

Financial institutions who fail to secure computer networks and sensitive customer information from cyber attacks are presenting huge whistleblower opportunities for IT professionals and other bank and investment firm employees. Failure to report weak cybersecurity systems and cyberhacks continue to pose a problem for U.S. banks, and whistleblowers are in prime position to collect big cash awards for their inside knowledge.

CYBERCRIME ESTIMATED TO COST GLOBAL ECONOMY OVER $500 BILLION ANNUALLY

McAfee estimates the annual cost of cybercrime to the global economy could be as much as $575 billion per year and banks remain the top cybercrime targets. Not only do weak cybersecurity systems continue to expose sensitive personal information, but careless employee mishandling of sensitive data poses an equally dire threat. Attaching the wrong file to an email or downloading sensitive information to a personal device is becoming a major security issue.

> "We are concerned that financial institutions will fail to immediately report cybersecurity incidents, especially successful attacks," said leading U.S. whistleblower attorney Brian Mahany. "Banks have a duty to disclose cybersecurity breaches that could endanger sensitive information for tens of thousands of U.S. citizens and affect the integrity of the system."

The slightest vulnerabilities in cybersecurity can lead to massive breaches. In 2014, the JPMorgan Chase mega-breach compromised data associated with more than 83 million accounts, including 76 million households and 7 million small businesses. Despite JPMorgan Chase's complex cybersecurity program, a mere failure to upgrade a network server to require double authentication

Continued on next page

Continued from previous page

led to one of the largest data breaches in history.

SEC RAMPING UP FINANCIAL INSTITUTION CYBERSECURITY AND BREACH REPORTING REQUIREMENTS

The federal government enforces a number of stringent cybersecurity and incident reporting regulations on American banks and financial institutions. Mismanagement of cybersecurity can violate securities laws for companies and agencies regulated by the Securities and Exchange Commission (SEC) and in some cases can amount to securities fraud.

The SEC's Regulation Systems Compliance and Integrity rule requires organizations to incorporate computer networking systems with security levels "adequate to maintain operational capacity and fair and orderly markets," and to "take corrective action" and report incidents following system breaches. In addition, the Dodd-Frank Act commands the SEC and CFTC to require financial institutions to design and execute robust identity theft prevention programs.

"Cybersecurity threats know no boundaries. That's why assessing the readiness of market participants and providing investors with information on how to better protect their online investment accounts from cyber threats has been and will continue to be an important focus of the SEC," said SEC Chair Mary Jo White in a February 2015 press release. "Through our engagement with other government agencies as well as with the industry and educating the investing public, we can all work together to reduce the risk of cyberattacks."

Last year, the SEC fined St. Louis-based investment advisor, R.T. Jones Capital Equities Management Inc., $75,000 for cybersecurity failures, including failure to implement data encryption and firewalls, that resulted in the exposure of over 100,000 customers' personal information.

The SEC's recent $1 million settlement with Morgan Stanley Smith Barney LLC illustrates the SEC's eagerness to take action regarding cybersecurity issues. Alleged cybersecurity deficiencies led to the release of personal information for approximately 730,000 customer accounts. The SEC charged the firm with violating the Safeguards Rule (Rule 30(a) of Regulation S-P).

Enacted in 2000, the Safeguards Rule requires that investment companies, broker-dealers and advisors adopt policies and procedures to implement certain safeguards. The safeguards must be designed to insure the security and confidentiality of customer records and information, protect against anticipated threats or hazards to the security or integrity of customer records and information, and protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.

MILLIONS IN WHISTLEBLOWER AWARDS OFFERED TO IT PROFESSIONALS AND BANK EMPLOYEES

Despite extensive federal regulations, financial institutions continue to fail to report incidents of cyber hacking or security breaches. Recently, an FDIC employee downloaded files onto a personal portable hard drive containing thousands of highly sensitive records, including banking and loan information. She left the agency for a private sector job and took the hard drive with her. FDIC officials failed to report the major leak of personally identifiable information after being aware of it for months.

"We are concerned that financial institutions will fail to immediately report cybersecurity incidents, especially successful attacks," said leading U.S. whistleblower attorney Brian Mahany. "Banks have a duty to disclose cybersecurity breaches that could endanger sensitive information for tens of thousands of U.S. citizens

Continued on next page

Continued from previous page

and affect the integrity of the system."

Any breach in cybersecurity that is not reported could potentially qualify for a whistleblower lawsuit under the SEC whistleblower program. The SEC offers whistleblowers between 10% and 30% of any $1 million-plus recovery arising from settlement or successful lawsuit against the wrongdoer. The potential for a whistleblower award of $1 million or more under the SEC whistleblower program is significant.

CYBERSECURITY WEAKNESSES AT FEDERALLY INSURED BANKS

Whistleblowers reporting cybersecurity weaknesses at federally insured banks are also eligible for percentage awards under the Financial Institutions Reform Recovery and Enforcement Act. Those awards can quickly reach $1.6 million.

Bankers, broker-dealers, financial advisors, IT professionals, and other financial institution employees are in a unique position to detect security breaches or flaws in cybersecurity systems. To qualify for an SEC whistleblower award, the whistleblower must have "original source" information about the failure to comply with regulatory requirements.

With today's nearly complete integration of personal and business banking and investment dealings in computer networking and data systems, the potential for failing to provide adequate levels of security and resulting cyber breaches is substantial. Financial institution employees with knowledge of cybersecurity breaches and weak data security measures play a pivotal role in ensuring that our nation's citizens are safe from cybercrimes, and the SEC awards both cash and anti-retaliation protections for those who choose to blow the whistle.