KANE RUSSELL COLEMAN LOGAN

One Mission. Your Mission.

Federal Regulators Push Community Banks To Up Cybersecurity

Banking Law / June 30, 2015

At the end of January, federal regulators strongly encouraged small community banks across the country to take measures to bolster their cybersecurity, and specifically asked that community banks take care to monitor the activities of vendors that handle many aspects of the banks' business. Smaller regional banks, which the Independent Community Bankers Association reports makes up nearly 97% of all banks in the United States, rely heavily on outsourcing various business functions to third-party vendors in order to remain competitive with larger national banks. This outsourcing can pose a serious problem if the vendors haven't established adequate precautions to protect the banks' sensitive data.

Vendors As A Weak Link In Security

The threat of cyberattacks on banks continues to increase—but why are federal regulators emphasizing concerns about vendors that provide services to small community banks? In recent years, community banks have begun to branch out and offer more new products and services to customers in order to satisfy customer demand and remain competitive with larger banks. To do this in an economically viable way, smaller banks have outsourced certain products and services to third party vendors.

In connection with the vendors' services, banks provide the vendors with access to customer data as well as bank specific data. Federal regulators are worried that vendors represent a vulnerability in banks' cybersecurity apparatus. This is a logical conclusion in light of the increasing number of cybersecurity breaches at major companies and retailers across the United States—many of which hackers accomplished by using vendor credentials.

Where There Is Complexity, Hackers Thrive

Online and mobile banking, as well as smartphone app development, are technological aspects of banking that small, regional banks often cannot handle in-house. Similarly, community banks commonly outsource a number of business functions, such as fraud monitoring and card issuing. The addition of every new vendor increases the complexity of business operations—potentially creating security loopholes and opportunities for hackers.

As vendors grow and consolidate, they will take on more community bank clients. If there is a security flaw for one of the vendor's customers, there is a high likelihood that a hacker will discover it and exploit the same flaw for all of the vendor's bank customers.

Can Community Banks Rise To The Challenge?

One of the main problems with asking community banks to step up the monitoring of their vendors is the cost associated with constant oversight. While banks are already required to monitor the activities of their vendors, federal regulators are asking for more. Federal regulators would like to see small banks conduct thorough research on their vendors and perform in-depth analysis on the associated cybersecurity risks. Small banks have limited resources to begin with, and holding

them responsible for assessing and monitoring the cybersecurity abilities of their vendors places an added burden on the community banks. But protecting the end-customer, those who patronize the community banks, is of the utmost importance and small community banks will have to rise to the challenge or face the consequences.