SAFETY STEPS

Five Best Practices to Minimize Vendor-Information Security Risks

by
Tyler J. Bexley, Attorney,
Reese Gordon Marketos LLP,
Dallas, Texas

reprinted with permission from **IB**, *a publication of Independent Community Bankers of America*

BD FEATURE

With data breaches dominating front-page headlines and regulators increasingly focused on data protection, cybersecurity is one of the most important issues confronting community banks today. For example, the Consumer Financial Protection Bureau (CFPB) filed its first enforcement action related to data security, entering into a consent order with an online payment processor related to the company's data security practices.

...the OCC...cautions that "a bank's failure to have an effective third-party risk management process...may be an unsafe and unsound banking practice."

Although this enforcement action did not directly involve a bank, it serves as a reminder that banks must closely monitor their vendors to ensure compliance with applicable laws and regulations. In fact, the Office of the Comptroller of the Currency (OCC), in its Bulletin 2013-29, cautions that "a bank's failure to have an effective third-party risk management process that is commensurate with the risk, complexity of third-party relationships, and organizational structure of the bank may be an unsafe and unsound banking practice."

Because of the serious consequences that come with data breaches, banks must scrutinize potential vendors and ensure that every vendor meets minimum regulatory requirements for data security. These are some best practices for banks to follow to minimize vendor data security risks:

• **Have a written plan** relating to vendor management and designate an employee (preferably someone in senior management) to be responsible for vendor oversight. For vendors involved with "critical activities," the regulators expect board involvement in approval and monitoring. All employees and directors who have responsibility for vendor selection and management should have up-to-date training in data security issues.

• **Ensure that IT and software vendors** are familiar with the Federal Financial Institution Examinations Council (FFIEC) guidelines on information security, the *Gramm-Leach Bliley Act*, and other applicable laws and regulatory guidance. Consider using only vendors with extensive experience working with regulated financial institutions.

• **Put prospective vendors** through a thorough vetting process. This should include an on-site assessment of the vendor's facilities, a review of any prior customer or regulatory complaints, and an interview of the vendor's management team.

• **Have written agreements with all vendors** that establish detailed minimum performance standards for information security. The agreement should mandate that vendors stay current on data security issues and regularly update their software to address new vulnerabilities in their

(*continued on Page* 12)

BANKERS DIGEST
P. O. Box 743006
Dallas, Texas 75374-3006
(USPS 041180)

PERIODICAL

ADDRESS CHANGE - When writing to us about your subscription, enclose the address label from your copy of Bankers Digest. You can also change your address or other information at *www.bankersdigest.com* under subscriptions.

FEATURE (*continued from Page 3*)

systems. The agreement also should require vendors to pass on the same minimum standards to any subcontractors.

• **Ensure that vendors** can meet any security-related claims in bank marketing material. For example, if a bank advertises that it protects customer data using certain encryption standards, the bank should ensure that its vendors (as well as their subscontractors) use the same encryption standards.

In the worst-case scenario of a data breach or adverse regulatory action, the bank should be prepared to hold vendors accountable where appropriate. To that end, banks should ensure that their contracts with vendors contain strong indemnification provisions to protect the bank. The indemnity language should protect the bank from losses and legal fees associated with customer litigation, shareholder litigation, legal compliance, and any regulatory enforcement action.

In the end, there is nothing a bank can do to completely prevent a data breach. But banks can minimize their cybersecurity risks by staying current on the latest risks and regulatory requirements, thoroughly vetting their vendors on the front end, and closely monitoring vendor performance. In the event of a data breach, banks should have procedures in place to quickly address the breach, and, if appropriate, seek reimbursement from responsible vendors 🏛

About the author: **Tyler Bexley** is a commercial litigation attorney at Reese Gordon Marketos LLP in Dallas, TX. He represents community banks and their officers and directors in litigation and enforcement proceedings. He has authored a previous article in Bankers Digest on "Understanding and Avoiding Unsafe and Unsound Banking Practice." (See *Bankers Digest*, May 2, 2016, Volume 148, No. 17)

Bexley also authors a blog that follows recent trends in banking litigation, regulation, and enforcement at *www.communitybankblog.com*. He may be contacted at 214.382.9805.

Picking Protocols

In a member poll, the Independent Community Bankers of America asked members: "What standard, framework or assessment does your community bank use to implement its cybersecurity controls?"

The following member poll results are from ICBA NewsWatch Today, March 2016:

• Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool: 41%
• FFIEC IT Handbook: 22%

• Vendor-Provided Controls: 19%

• National Institute of Standards and Technology Cybersecurity Framework: 2%

• Other: 2%

• All of the above: 16%