Knowledge, Prevention, Response: Protecting Customers' Personal Data

By Steven C. Kerbaugh

It seems like you can't turn around these days without hearing about another company that has been subject to a data breach. Rightfully, banks are especially concerned about how to prevent being the next to be attacked, given the amount of our customers' personal data we are entrusted with.

Data breaches are also notoriously expensive. Investigation expenses, legal fees, remediation vendors and services, implementation of new policies and technologies, and so forth can add up to tens of millions of dollars. Moreover, one of the largest financial consequences of a data breach comes in the form of dissatisfied, and often lost, customers. As such, it is important to recognize the risks and take effective steps to manage data breach threats.

Laws Relating to Protection of Personal Data

There is a complex, multi-level assortment of laws and regulations to protect customers' personal data.

- All states, including Minnesota, have laws relating to data breaches. State laws on the protection of personal data often vary significantly and depending on the locations of your bank's customers, the laws of multiple states may apply to you.
- In addition, there are federal laws relating to data privacy that are applicable to the financial services industry, including the Gramm-Leach-Bliley Act (GLBA) that requires financial institutions to explain how they share and protect their customers' private information.
- Agency regulations related to data security, such as those promulgated by the Consumer Financial Protection Bureau, may apply to your bank.
- Foreign laws also may apply. For example, the European Union's General Data Protection Regulation can apply to companies based in the United States that process the personal data of European Union residents.

This patchwork of laws and regulations relating to data security may seem dizzying. And it often is. At their core, though, such laws typically include steps that companies must take if there has been a data breach. They also often include provisions on minimum security that are designed to ensure companies have preventive measures and safeguards in place.

Preventive Measures

When it comes to data breaches, the adage that the best defense is a good offense rings true. Banks should implement preventive safeguards, which may include:

- Bank-wide security policies and protocols on the encryption, access, and use of personal data.
- Employee awareness training on the importance of data security and company policies relating to it, how to identify phishing efforts, the proper use of external storage devices, and so forth.
- Retention of appropriate technology/security personnel, and implementation of appropriate systems to detect and respond to data breaches.
- Insurance that covers expenses related to data breaches.

Having reasonable safeguards in place can help prevent breaches before they happen and ensure company preparedness should they

Nominations for MBA Vice Chair/Treasurer

The Minnesota Bankers Association Nominating Committee invites your suggestions for a nominee for MBA Vice Chair/Treasurer for 2020-2021.

For the 2020-2021 year, the Committee will nominate a banker for the position of Vice Chair/Treasurer, to be elected at the Annual Summit on June 15, 2020. The Vice Chair/Treasurer will succeed to the office of Chair, and then to Past Chair.

Enclosed with the *MBA News* is a form for your use in suggesting a candidate for Vice Chair/Treasurer and the form is also available on our website. We have asked that background information be included concerning bankers under consideration by the Committee. As always, past and current involvement with the Minnesota Bankers Association or our industry is important. The Committee will receive nominee suggestions until March 1, 2020.

We appreciate your careful consideration of qualified future leaders for MBA. Feel free to contact any of the Committee members if you have questions or comments.

Members of this year's Committee are Mark Miedtke, Citizens State Bank, Hayfield (Chair); Mark White, First National Bank, Coleraine; Gail Mikolich, Northeast Bank, Minneapolis; Chuck Johnson, Root River State Bank, Chatfield and Bryan Bruns, Lake Central Bank, Annandale. ■

occur. Such safeguards also can provide a defense to litigation in states such as California and Ohio. It is also noteworthy to consider that under the 2018 California Consumer Privacy Act (CCPA), a California resident whose personal information is involved in a data breach caused by a covered business's failure to maintain reasonable safeguards may recover statutory damages without a showing of actual harm. While some data covered by the GLBA is exempt from the CCPA, keep in mind the GLBA may not be the only bucket into which a bank's data falls, for example employee information would not be exempt.

Responding to Data Breaches

Time is of the essence when a breach occurs. A responding bank should immediately investigate the scope of the breach (potentially through forensic analysis), communicate with appropriate law enforcement agencies, coordinate with insurance carriers, and select appropriate vendors. Ensuring compliance with state and federal customer notification mandates will be necessary. Accordingly, it also will be necessary to immediately develop a communication plan and to set up any appropriate mitigation services such as call centers, credit monitoring, identification theft resolution, and the like. Finally, it may be appropriate to put together a litigation team and strategy to help manage any resulting investigations or lawsuits.

Unfortunately, in today's technological environment, it seems the question is not so much whether a data breach will occur, but when. While banks are being subjected to unprecedented cybersecurity threats, there are steps you can take to protect your customers' personal data now. Knowledge of the law and implementation of appropriate safeguards can help prevent breaches, identify breaches, and mitigate the fallout should they occur. ■

This material is provided for informational purposes only. It is not intended to constitute legal advice, nor does it create a client-lawyer relationship between Jackson Lewis P.C. and any recipient. Recipients should consult with counsel before taking any actions based on the information contained within this material.

Steven C. Kerbaugh
Jackson Lewis P.C.
Steven.Kerbaugh@jacksonlewis.com

MBA ASSOCIATE MEMBER