Is Your Bank's Cybersecurity Program Adequate? If Not, Your Bank May be Subject to Negligence Claims

Related Professionals

David M. Aldous

Related Services

Data Strategy, Privacy and Security

Related Industries

Financial Institutions

AUTHORED ARTICLE | Winter 2019

By David M. Aldous
(Published in the Winter 2019 issue of *The Bankers' Statement*)

The Cybersecurity Challenge

Due to the evolving sophistication of criminals, security breaches continue to occur on a regular basis. When such breaches occur, the victims of breaches often look to the law to make them whole. Yet, because any economic losses are rarely able to be recovered from the criminal(s) who caused the breach, the victim whose personal information was compromised will typically seek to recover any losses from the business where such personal information was held. These two "innocent" parties are then left to dispute who bears the burden of the economic loss.

Banks have already been responding to regulator concerns about cybersecurity risks and the potential liabilities and penalties that could result from failure to have a cybersecurity program that is adequate. Bank regulators monitor cybersecurity issues on a regular basis through on-site bank examinations and regulatory reports, and it is important that banks be ready to respond to any inquiries from the regulators regarding their cybersecurity controls. What has been less clear, however, is what kind of duty banks owe to their customers and employees directly to ensure that any personal information held by banks is not disclosed as a result of a cyber-breach.

Of course, the best way for a bank to avoid the potential for any liability claims resulting from data breaches is to avoid data breaches altogether. However, in an age when even the most fortified governments and companies are subject to breach, banks should be ready to defend themselves against lawsuits when a breach occurs. Some recent legal developments in Pennsylvania and Ohio provide guidance to banks regarding (i) whether courts will allow customers and employees to bring negligence claims against banks for failure to prevent disclosure of personal information, and (ii) what banks need to do to defend against such claims.

A Bank's Cybersecurity Duty

A recent 2018 Pennsylvania Supreme Court decision highlights the potential liability for businesses that fail to implement reasonable cybersecurity safeguards. In that case, the Supreme Court of Pennsylvania used traditional common law negligence standards to impose on an employer a duty to use reasonable care to safeguard the personal information of its employees.

This case arose from a 2014 data breach of a hospital's network, which resulted in the theft of tens of thousands of its employees' personal information, such as Social Security numbers, bank account information, salaries, etc. The Supreme Court of Pennsylvania held that where an employer's collection of employee personal information creates a foreseeable risk of data breach, the employer has a duty of reasonable care to secure its employee's personal information.

This decision could have a far reaching impact as other courts throughout the country consider whether a business has a duty to prevent disclosure of personal information in its possession. The court's recognition of a duty to prevent disclosure of personal information will likely not be limited to the employment context. In particular, banks and other financial institutions should make sure they are doing what they reasonably can to prevent the disclosure of their customers' personal information. Failure to do so, could expose the financial institution to significant liability based on negligence claims.

How Can a Bank Protect Confidential Information and Itself?

Although the Supreme Court of Pennsylvania did not specifically address actions that a business or bank must take in order to show that it exercised reasonable care in protecting confidential information, recent legislation in Ohio provides clarity for banks and other businesses in Ohio, and may provide guidance for banks in other states.
Ohio implemented last year a statute entitled the Ohio Data Protection Act, which provides a "safe harbor" from certain legal claims resulting from an electronic data breach. Pursuant to the Data Protection Act, a business that has implemented a qualifying cybersecurity program may raise an affirmative defense to any negligence or invasion of privacy claims alleging that failure to implement reasonable information security controls resulted in a data breach.[1]

In order to invoke the "safe harbor" status in Ohio, a business must "create, maintain, and comply with a written cybersecurity program that contains administrative, technical and physical safeguards" to protect personal information and that "reasonably conforms to an industry recognized cybersecurity framework," examples of which are identified by the law.[2] A business "reasonably conforms" to such a framework if the scale and scope of its cybersecurity program "is appropriate" based on the size and complexity of the business, the nature and scope of the business's activities, the sensitivity of the information, the cost and availability of tools to improve information security and reduce vulnerabilities, and the resources available to the business.

We expect courts in Ohio and other states will follow Pennsylvania's lead by imposing a duty of reasonable care on banks and other businesses that electronically store personal information of its customers and/or employees. Banks should protect themselves by implementing cybersecurity programs that demonstrate that they are taking "reasonable care" of sensitive personal information in their possession. If your bank is located in Ohio, the Data Protection Act outlines the cybersecurity controls that a bank must have in place

to affirmatively defend itself against negligence claims. We recommend that banks in states that have not yet provided any clear guidance regarding what would constitute reasonable care in the safeguarding of personal information use Ohio's Data Protection Act, as well as cybersecurity regulations and guidance from state and federal regulators,[3] as reference points. Ultimately, even if it is not yet clear how robust safeguards must be in order to show that reasonable care has been taken, what is clear is that banks that fail to implement a strong cybersecurity program are leaving themselves more exposed to potentially substantial liability resulting from legal claims brought by their customers and employees.

---

[1] This new law does not protect businesses from liability that may arise from violating contractual obligations, nor does it alter any other obligation that a business may have to report the data breaches as may be required by law or contract.

[2] The Data Protection Act sets forth the following recommended frameworks: NIST SP 800-71; NIST SP 800-53 and 800-53(a); The Federal Risk and Authorization Management Program; Center for Internet Security Critical Security Controls; The ISO 270000 Family; The HIPAA Security Rule; Graham-Leach Bliley Act; The Federal Information Security Modernization Act.

[3] In 2017 the New York State Department of Financial Services implemented cybersecurity regulations affecting certain financial institutions. The New York cybersecurity regulation applies to financial institutions that are required to operate under a license or other similar certification under New York's banking, insurance or financial services laws. Subject to exceptions, state banks chartered outside of New York, but which have branches in New York, are not subject to the requirements of the New York cybersecurity regulations. The New York cybersecurity regulations require regulated financial institutions to have (i) a cybersecurity program in place to protect consumers' private data; (ii) a written cybersecurity policy or policies; (iii) a Chief Information Security Officer to help protect confidential data and systems; and (iv) controls in place to preserve safety and soundness. Yet, it is not adequate for regulated financial institutions to simply put these controls in place. They must also audit and ensure that their cybersecurity program is being properly and effectively implemented. Finally, once nonpublic information is no longer necessary for the business operations of the regulated financial institution, and is not required to be retained by another law or regulation, regulated financial institutions are required to dispose of all nonpublic information that can reasonably be disposed of. In addition to these requirements, the regulated financial institutions are required to report cybersecurity events to the Department of Financial Services within 72 hours from a determination that a reportable cybersecurity event has occurred. Cybersecurity events are required to be reported if (i) the cybersecurity event impacts the financial institution and notice of the cybersecurity event is required to be provided to any government body, self-regulatory agency or any other supervisory body; or (ii) the cybersecurity event has a reasonably likelihood of materially harming any material part of the normal operations of the financial institution.