Morrison Mahoney Partner Daniel S. Marvin Outlines Cybersecurity Regulations for the Alternative Finance Bar Association

By: Daniel S. Marvin

Businesses in the alternative lending space face unique cybersecurity challenges. Whether it be social security numbers, bank account information, debit and credit card data or other personal information, the very information that these businesses collect and maintain in order to conduct their everyday affairs is the exact type that hackers try to steal each day. If a business does fall victim to a breach, the costs can quickly pile up; expenses can include remediation, business interruption, forensic investigation, restoration of network operations, legal fees and of course, reputational harm. With those costs in mind, having a strong cybersecurity program simply makes good business sense. But it is not just good business sense that should be on the mind of companies that engage in alternative lending. There are both federal and state regulatory requirements that these companies must adhere to with respect to data privacy.

For those companies looking to implement, or improve upon a cybersecurity program, understanding the regulatory framework in which they operate is vital. Such a framework should set the floor for these organizations' cybersecurity practices, which can then be improved upon as needed. However, the regulators and legislators have not made it easy. There is currently no single federal or state law regulating the collection and use of personal data, nor is there a single rule governing the notification of consumers if a breach has occurred. Instead, companies must be cognizant of a patchwork of federal and state laws that regulate both data privacy and breach notification. For businesses engaged in alternative lending, awareness of the laws and regulations below is key to the maintenance of cybersecurity and data privacy best practices.

The Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act (GLBA), also known as the Financial Modernization Act of 1999, is federal law that requires financial institutions to protect their customers' private information, including names, social security numbers, addresses, phone numbers, bank account numbers, credit card numbers, income, and credit histories. With respect to most financial institutions, implementation and enforcement of the GLBA is overseen by the Federal Trade Commission (FTC). As part of that implementation, the FTC issued what is known as the Safeguards Rule, which requires financial institutions to have measures in place to keep customer information secure by developing, implementing and maintaining a comprehensive written information security program that addresses administrative, technical, and physical safeguards. The Safeguards Rule applies to all businesses, regardless of size, that are "significantly engaged" in providing financial products or services, including payday lenders and nonbank lenders.

There are 5 basic elements that a lender needs to have in place in order to be GLBA compliant. The first is the designation of one or more employees (such as a Chief Information Security Office) to coordinate an information security program. Next, companies need to iidentify reasonably foreseeable internal and external risks to customer information that could result in an unauthorized

disclosure, and assess the sufficiency of any safeguards in place to control these risks. Third, GLBA compliance requires that companies design and implement information safeguards to control risks, and regularly test or otherwise monitor the effectiveness of those safeguards. Fourth, companies must take reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards, and oversee those service providers. Finally, companies must engage in the ongoing evaluation and adjustment of their information security program based on results of the testing and monitoring, or based on any material changes to operations or business arrangements or circumstances.

The Federal Trade Commission Act

The FTC's authority is not just limited to the Safeguards Rule. Pursuant to Section 5 of the FTC Act, the FTC has broad authority to regulate "unfair" or "deceptive" acts or practices. An act or trade practice is considered "unfair" if it causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and is not outweighed by countervailing benefits to it. A deceptive trade practice consists of a material representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment. So how does this relate to cybersecurity?

The FTC has brought numerous enforcement actions using the "unfairness doctrine" against companies that the FTC accused of failing to install reasonable security measures. For example, according to the FTC, businesses maintaining or storing personal identifying information or other sensitive data are under a duty to undertake reasonable steps to protect such data, and the failure to do so is an unfair practice. Companies in violation of the unfairness doctrine expose themselves to enforcement actions, including the imposition of injunctive relief, financial penalties and government approved third-party monitoring of cybersecurity standards, policies and procedures. Consent agreements, which include mandatory monitoring and data security compliance programs, often extend for a term of twenty years. Thus, companies engaged in alternative lending should be aware that federal regulators are looking at data security practices, even when no breach has occurred, and may use their enforcement powers to remedy cybersecurity measures that do not meet the regulators' view of reasonable or adequate.

The Consumer Financial Protection Bureau

The Consumer Financial Protection Bureau (CFPB) is a federal agency responsible for consumer protection in the financial sector. The CFPB's creation was authorized by the Dodd–Frank Wall Street Reform and Consumer Protection Act, and its jurisdiction includes banks, credit unions, securities firms, payday lenders, and other financial institutions. In March 2016, the CFPB instituted its first data security enforcement action in the form of a consent order against online payment platform Dwolla, Inc. Notably, as with some actions which are brought by the FTC, the Dwolla action was brought by the CFPB without any data breach having occurred or evidence of consumer harm. Instead, Dwolla was accused of overstating the measures it took to protect consumers' personal information between December 2010 and 2014. The CFPB also accused Dwolla of failing to implement a written data-security plan, failing to conduct adequate, regular risk assessments, and not providing adequate training to employees.

What is interesting about the Dwolla action is that it reinforces that some regulators believe that there are baseline standards of what reasonable cybersecurity measures are, despite the fact that no formal regulations have been issued. In fact, this issue was brought front-and-center a few years ago when the FTC brought a lawsuit against Wyndham Worldwide Corporation alleging unfair and deceptive acts and practices (UDAP) based on Wyndham's public representations about its cybersecurity efforts. Wyndham argued to the Court that it lacked fair notice as to the standard to which the FTC was holding it, claiming that there were no rules or statutes explaining what steps organizations must take to safeguard customer data. Wyndham's arguments were rejected, with the Court holding that the company had sufficient notice that its activity could fall within the ambit of the Federal Trade Commission Act's UDAP statute (which is similar to the Consumer Financial Protection Act's UDAP provisions) based upon agency guidance documents, enforcement actions, and settlements, all of which could provide adequate notice as to what cybersecurity measures are reasonable. Thus, companies should be aware that cybersecurity concerns could arise both in the context of routine examinations by regulators, as well as targeted inquiries, even when no breach has occurred. This is especially true in the alternative lending industry, given the sheer amount of sensitive data that is handled.

New York State Department of Financial Services Cybersecurity Requirements

On March 1, 2017, the New York State Department of Financial Services (DFS) enacted first-of-their-kind regulations that require institutions regulated by DFS to establish and maintain a cybersecurity program designed to protect consumers. Depending on the nature of an alternative lender's business, it may be subject to these regulations. Regulated entities include "Licensed Lenders" pursuant to Section 9 of the New York State Banking Law, which are defined as entities that are engaged in the business of making loans in the principal amount of $25,000 or less to any individual for personal, family, household, or investment purposes, or $50,000 or less for business and commercial loans, at a rate of interest greater than 16% a year. For the purposes of the Banking Law, an entity is considered as engaging in the business of making loans in New York, and subject to the licensing and other requirements, if it solicits loans in New York and, in connection with such solicitation, makes loans to individuals who reside in New York.

The DFS regulations are designed to allow each regulated entity the ability to craft a cybersecurity program based upon its own individual risk assessment. In order to be compliant with the Regulations, the DFS requires a covered entity's cybersecurity program to addresses six core cybersecurity functions: 1) to identify and assess internal and external cybersecurity risks; 2) use defensive infrastructure and the implementation of policies and procedures to protect the covered entity's information systems from unauthorized access, use or other malicious acts; 3) detect cybersecurity events; 4) respond to identified or detected cybersecurity events to mitigate any negative effects; 5) recover from cybersecurity events and restore normal operations and services; and 6) fulfill applicable regulatory reporting obligations. These six areas are among those commonly viewed as integral to any cybersecurity program, and sharp parallels can be drawn between the DFS' Regulation and the National Institute of Standards and Technology (NIST) Cybersecurity Framework. The NIST Framework was first published by the United States Department of Commerce in 2014 and revised in December 2017, and is designed to offer private organizations guidance on how to prevent, detect and respond to cybersecurity events by

addressing 5 core categories, (Identify, Protect, Detect, Respond and Recover), which are similar to those core functions set forth by the DFS.

State Consumer Data Privacy Laws

Many states have enacted, or are planning to enact, regulations governing the protection of the personal data of their residents. The California Consumer Privacy Act (CCPA), which takes effect January 1, 2020, creates new data privacy rights for California consumers, including the rights to know, access, have deleted and opt out of the sale of their personal information. The right to know requires Covered Businesses to make both affirmative disclosures to all consumers, and respond to verifiable consumer requests with individualized disclosures about the business's collection, sale, or disclosure of personal information. The CCPA further guarantees consumers the right to access a copy of the "specific pieces of personal information that [a business] has collected about that consumer." Businesses need to be prepared to have an efficient way to timely respond to such demands for access.

Following in the footsteps of the CCPA, New York State Senator Kevin Thomas recently introduced the New York Privacy Act (NYPA), a bill which would enact strict, consumer–oriented rules for the collection, use, control, processing, and transfer of data by companies that conduct business in New York or target products or services at New York residents. The NYPA's stated purpose is to address how online platform/social media firms process personal data, and will require the companies to attain consent from consumers before they share and/or sell their information by acting as fiduciary entities. Among, other things, the bill expands the definition of personal information, and creates a private right of action for consumers to sue companies for violations of the law. Massachusetts is considering a similar bill which would also significantly expand consumer rights and create a private right of action, and other states are moving towards the same types of legislation.

State Breach Notification Laws

If a company does suffer a data breach, a whole new set of laws are implicated. All fifty states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private entities to notify individuals who are residents of those states of security breaches of information involving personally identifiable information. However, each state has its own, and somewhat different set of requirements. For example, various states have different definitions of "Personal Information," with some states including things such as email addresses, social media handles and biometric data within their definitions. Moreover, in some states, breach notification is triggered by a belief that an unauthorized party has simply accessed personal information, while in other states, notification is triggered upon a reasonable belief that there is a risk of harm that could flow from the access. Furthermore, in the event of a breach, some states require notice to the Attorney General, other state agencies, and/or credit monitoring agencies. Other differences among the states' statutes are the timeframes in which notification is required, and whether employees and/or former employees are covered in addition to customers.

Conclusion

While keeping up with the above laws and regulations can seem daunting, it is important to remember that regulatory compliance will be a natural byproduct of a robust and effective cybersecurity program. Given the regulation, it is incumbent on alternative lenders to maintain a comprehensive cybersecurity program, including a written information security plan, employee data security policy, incident response plan and strong third-party vendor contracts that address the safeguarding of data. These steps will not only ensure regulatory compliance, but will save lenders much grief should a data breach occur.

Daniel S. Marvin is a Partner in the New York office of Morrison Mahoney, LLP, where he represents businesses with respect to data privacy, cybersecurity and cyber-insurance matters. He can be reached at dmarvin@morrisonmahoney.com or 646-870-1739. *The information presented in this article is for general information purposes only and should not be relied upon as legal advice.*