

JOURNAL

OF EQUIPMENT LEASE FINANCING

VOLUME 35 • NUMBER 3 • FALL 2017

Thriving Millennials: The Next Generation of Industry Leaders

By Scott A. Wheeler

The Millennial generation — consisting of individuals born between the early 1980s and the mid-to-late 1990s — is changing the work environment, the processes, and the level of services offered by the financial sector. They are investing in themselves, their employers, and the industry to better serve the next generation of stakeholders: vendors, end-users, and investors.

Is Competition Dying in the Canadian Equipment Finance Market?

By Hugh Swandel

Canada's banking system is one of the strongest in the world. But domestic and international regulations that helped preserve the strength of Canadian banks during the financial crisis of 2008 and 2009 have since worked to create an alarming dominance by a handful of banks. Will this work against Canada's equipment leasing and finance industry?

Cybersecurity: The Increasing Obligations and Exposure in the Age of State Regulation

By Frank Peretore, Robert L. Hornby, Michelle A. Schaap and Brigitte M. Gladis

In response to the ever-increasing number of high-profile data breaches, the federal government and the states are turning to regulations and legislation through which businesses must implement cybersecurity safeguards to protect customer information. Many of these measures also make private businesses responsible for monitoring affiliates and third-party vendors. Failure to comply may lead not only to a state enforcement action but also private lawsuits.



Articles in the Journal of Equipment Lease Financing are intended to offer responsible, timely, in-depth analysis of market segments, finance sourcing, marketing and sales opportunities, liability management, tax laws regulatory issues, and current research in the field. Controversy is not shunned. If you have something important to say and would like to be published in the industry's most valuable educational journal, call 202.238.3400.

The Equipment Leasing & Finance Foundation

1625 Eye St NW,
Suite 850
Washington, DC 20006
202.238.3400
www.leasefoundation.org

Cybersecurity: The Increasing Obligations and Exposure in the Age of State Regulation

By Frank Peretore, Robert L. Hornby, Michelle A. Schaap and Brigitte M. Gladis

In response to the ever-increasing number of high-profile data breaches, the federal government and the states are turning to regulations and legislation through which businesses must implement cybersecurity safeguards to protect customer information.

Many of these measures also make private businesses responsible for monitoring affiliates and third-party vendors. Failure to comply may lead not only to a state enforcement action but also private lawsuits.

Recent years have witnessed an alarming upswing in massive data breaches and cyberattacks infiltrating all industries. In response, states have begun to take the initiative by implementing laws and regulations designed to impose affirmative obligations and restrictions on individuals and entities that come into possession of certain personal information, sometimes with severe penalties for noncompliance.

The correlation between large-scale data breaches and increased regulation is not surprising. As more and more everyday activities and interactions take place online, hackers and others with nefarious intentions are afforded a myriad of opportunities to access and exploit personal data. While regulations concerning cybersecurity — and thus the obligations imposed on those in

possession of certain personal information — have existed for years, recent enactments have demonstrated a distinct trend: state governments are increasingly mandating that those who come into possession of personal information *proactively* ensure that such information remains secured, or face the consequences.

Given the unfortunate likelihood that a company may be subject to a cyber-attack at any time — the Insurance Information Institute noted that cyberattacks were in the top five largest threats to businesses worldwide¹ — all companies, regardless of size, should prepare for the worst. Due to the personal and financial nature of the information routinely collected in the equipment financing industry, this industry is in the crosshairs of the new laws. Those in the

industry must keep abreast of the newly imposed obligations at both the state and federal level as well as realize the potentially devastating implications and possible legal ramifications of their failure to do so.

This article highlights the importance for businesses of ensuring the security of personal and financial information in their possession by discussing some recent large-scale data breaches and cyberattacks and the resultant ramifications and liability incurred by the businesses involved in those breaches. The article briefly outlines the most recent legislative efforts to mandate cybersecurity — namely, the recent regulations enacted by Massachusetts, New York, and Delaware — as well as preceding federal laws.

Finally, the article closes by

providing some insight as to how those within the equipment financing industry may better equip themselves to not only comply with newly enacted state regulations but also to enable them to make informed business decisions in connection with their cybersecurity programs.

RECENT HIGH-PROFILE LIABILITY CASES

The numbers do not lie: data breaches increased 40% in 2016.² This is likely because, as Verizon noted in its 2016 Data Breach Investigations Report, a company's information security team can "to a very small degree, be compared to the lot of a hapless soldier," in that he "is told to guard a certain hill and to keep it all costs," but he "is not told who his enemy

may be, what they look like, where they are coming from, or when (or how) they are likely to strike.”³

The nature of personal information in the possession of companies in the financial services and equipment finance industries makes those companies particularly attractive to a cyberattack.

The reality is that a threat to an entity’s cybersecurity may come from anywhere at any time — as the recent spread of the ransomware WannaCry demonstrated — and unfortunately, countless numbers of companies are blindsided by data breaches and cyberattacks each year. The nature of personal information in the possession of companies in the financial services and equipment finance industries makes those companies particularly attractive to a cyberattack. Indeed, in its 2016 Data Breach Investigation Report, Verizon concluded that 89% of

breaches had a “financial or espionage motive.”⁴

These data breaches and cyberattacks are not cheap: a June 2016 report released by the independent research organization Ponemon Institute estimates that the average cost to a U.S. company for a data breach is approximately \$7 million.⁵ Perhaps most importantly, recent disclosures involving large-scale data breaches demonstrate that the sophistication or reputation of a company does not change its vulnerability to a breach or its potential for liability as a result of that breach. Accordingly, companies of all sizes must be vigilant to secure personal information in their possession.

Equifax

Consider the recent Equifax breach. Many if not all readers of this article rely on third-party providers including Equifax to undertake credit checks before entering into a financing transaction. Had the Equifax breach not occurred until June 2019, and had a lender then failed to demonstrate that it adequately vetted Equifax’s security policies and procedures, the lender would potentially face exposure under the recent New

York Cybersecurity Regulations. (These regulations are discussed below. Portions of them are not effective until March 2019.)

Regardless of the applicability of these new regulations, all parties that may have previously relied on Equifax for credit checks are now on notice that Equifax’s data security procedures were insufficient to prevent a breach. Whether or not Equifax’s policies were reasonable will be determined by the courts in the ever-mounting class action lawsuits filed against Equifax (not to mention the investigations pending with various states’ attorneys general, Congress, the FBI, and the FTC). However, as companies selecting vendors for these types of services, those in the equipment finance industry are unquestionably on notice that due inquiry going forward is critical as to any and all third-party vendors.

Further, to the extent that a company provided personally identifiable information of a customer (or potential customer) to Equifax, that company now likely has an obligation to provide timely notice to its impacted customers. Different states’ breach notification stat-

utes provide different procedures, depending on the number of persons impacted.

Ideally, a company’s contracts with its vendors should already (1) require any vendor to provide it with notice of a breach and (2) indemnify the company against resulting liability. Given the enormous volume of impacted persons, Equifax’s notice was made through a very public, nationwide notification. At a minimum, each lessor should consider its use of Equifax for its credit checks and confer with its cybersecurity legal advisors as to its notification obligations.

Even assuming that Equifax is found to have acted “reasonably” in its security efforts, the sheer cost of providing credit watch services to those impacted by the Equifax breach is likely to be a staggering figure.

Government Fines and Penalties

Importantly, companies that experience a data breach may ultimately be on the receiving end of substantial fines and other penalties imposed by the government. In 2013, two laptops were stolen from Hori-

zon Blue Cross Blue Shield’s New Jersey office. Following an investigation, the state Division of Consumer Affairs concluded that Horizon had failed to encrypt policyholders’ personal information, such as names, addresses, birth dates, and Social Security numbers. The stolen laptops and the data exposed affected an estimated 690,000 people.

Horizon reached a settlement with the New Jersey Division of Consumer Affairs that required Horizon to pay a \$1.7 million fine as well as submit to a corrective action plan to regularly assess security risks with respect to policyholders’ personal information.⁶

In 2015, approximately 36 million registered users of the website AshleyMadison.com had their personal information exposed due to a breach of the website’s systems. Following a Federal Trade Commission (FTC) investigation, Ashley Madison reached a settlement with the FTC and state governments, under which it agreed to pay a \$1.6 million fine and to implement more stringent security policies concerning users’ personal information.⁷

Then there is the notorious 2013 data breach involving Target Corporation, in which more than 41 million customers' credit card and 60 million customers' contact information were exposed as a result of a third-party vendor's theft of credentials. Following subsequent investigations, Target settled with 47 states and the District of Columbia, and agreed to pay \$18.5 million, as well as to develop a comprehensive security program with an independent, qualified monitor to conduct a security assessment.⁸

Personal customer information may also be obtained by sophisticated hackers launching cyberattacks. For instance, in 2014, JPMorgan Chase's computer system — along with those of several other well-known banks — was hacked. The hackers were able to obtain personal information of approximately 83 million of JPMorgan Chase's customers, including customers' names, addresses, phone numbers, and email addresses.

The perpetrators were eventually criminally charged, in part for their use of stolen personal information to perpetrate a massive stock fraud scheme; however,

the incident served to demonstrate the potential systemic weaknesses that exist even in the financial services industry.⁹

Private Litigation

In addition to settling with federal and state authorities, companies that have suffered a data breach are also potentially susceptible to private litigation brought by those whose information has been compromised. For instance, Neiman Marcus recently agreed to pay \$1.6 million in a class action lawsuit filed as a result of a data breach disclosing the credit card data of 350,000 customers.¹⁰

While class action lawsuits may present certain difficulties for plaintiffs, their specter remains a threat for companies that have been involved in significant data breaches or cyberattacks and provides an incentive to ensure that they have effective cybersecurity programs and policies in place.¹¹

Importantly, these cases and resulting settlements involve costs incurred *after* a data breach has occurred. They do not take into consideration the additional liabilities a company may face

under regulations which impose *prebreach* requirements. As shown below, government regulations at the state level, including in Massachusetts, New York, and Delaware, implement enforcement mechanisms pursuant to which regulators are attempting to ensure cybersecurity compliance.

FEDERAL INFORMATION SECURITY LAWS

The United States has a long-standing history of privacy regulation and litigation, which in recent years has expanded to address increased concerns regarding cybersecurity and the overall security of personal information. Indeed, for more than two decades, the federal government has regulated the conduct of healthcare organizations, financial institutions, and federal agencies through the 1996 Health Insurance Portability and Accountability Act (HIPAA), the 1999 Gramm-Leach-Bliley Act, and the Federal Information Security Management Act of 2002. Broadly, these laws contain provisions requiring certain businesses that come into the possession of the personal information of others to

safeguard that information from exposure.

For example, consider the Gramm-Leach-Bliley Act (GLBA), also known as the Financial Services Modernization Act, which pertains to financial institutions. It makes clear that "each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."¹²

In pursuit of this goal, the regulations promulgated under the GLBA mandate that "financial institutions" (generally businesses that are "engaging in financial activities," such as, for example, lending, exchanging, transferring, or safeguarding money or securities¹³) must develop a written information security plan that describes their program to protect customer information.¹⁴

The FTC has advised that the plan requirements "are designed to be flexible," and that safeguards should be implemented that are appropriate to the circumstances of the financial institution at issue.¹⁵ Suggested safeguards include background

and reference checks of newly hired employees who will access customer information; limiting access to customer information; developing policies for the appropriate use of devices such as laptops, cellphones, or other mobile devices; and imposing disciplinary measures for security policy violations.¹⁶

The United States has a long-standing history of privacy regulation and litigation, which in recent years has expanded to address increased concerns regarding cybersecurity and the overall security of personal information.

In addition, the GLBA provides guidelines for financial institutions in connection with their collection and disclosure of personal financial information. The Financial Privacy Rule of GLBA requires financial institutions to notify "customers" about their privacy practices, and, under certain circumstances, to also notify "consumers"¹⁷ about such practices, including provid-

ing notices regarding (1) the types of information collected, (2) whether that information is ever disclosed and to whom, and (3) information concerning the institution's policies and practices with respect to protecting confidentiality and security of the "nonpublic personal information."¹⁸

Such requirements may have the practical effect of requiring companies to reassess those with whom they do business, in the event those service providers do not have the ability to maintain "appropriate" security measures.

Federal legislation such as the GLBA, which historically tended to be more flexible in its approach, has set the stage for more recent efforts on the part of the states to enact protections geared toward addressing the security of personal information prior to a cyberattack or a data breach. Although nearly every state has enacted laws related

to notification requirements following a data breach,¹⁹ several states are now implementing regulations containing affirmative obligations to secure customer personal information. In several cases, the mandates are much more specific in their requirements than existing federal requirements.

MASSACHUSETTS – THE BEGINNING OF PROACTIVE REGULATORY REQUIREMENTS

In 2010, Massachusetts enacted what was at the time considered the most comprehensive state cybersecurity regulation in the country.²⁰ The regulation, titled "Standards for Protection of Personal Information of Residents of the Commonwealth," was promulgated with the laudable goals of ensuring

... the security and confidentiality of customer information in a manner fully consistent with industry standards; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that may result in substantial

harm or inconvenience to any consumer."²¹

Importantly, the regulation applies to "all persons that own or license personal information²² about a resident of" Massachusetts — an overwhelming number of both people and entities, as the regulation defines "persons" to include not only natural persons but also corporations, associations, partnerships, or other legal entities.²³

The regulation imposes an obligation on owners and licensees of "personal information" to "develop, implement, and maintain a comprehensive information security program," and demands that those programs contain particularized "administrative, technical, and physical safeguards" to ensure that the personal information in their possession remains protected.²⁴

The Massachusetts regulation further provides particular features that these security programs must possess, including, among others, the identification and assessment of "reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal

information"; the development of security policies for employees as to the storage and handling of personal information; the overseeing of service providers who have access to personal information; and the imposition of appropriate discipline for violations of the security program.²⁵

Certain of these requirements have the potential to be onerous for regulated entities. For example, with respect to service providers, the regulation requires a regulated entity to take "reasonable steps" in selecting "third-party service providers that are capable of maintaining appropriate security measures" to protect personal customer information.²⁶ Accordingly, such requirements may have the practical effect of requiring companies to reassess those with whom they do business, in the event those service providers do not have the ability to maintain "appropriate" security measures.

Although providing leeway to specifically tailor a security program to the particular industry or company at issue, the regulation does not explicitly mandate what each regulated

individual or entity must specifically do in order to comply with the regulation. Instead, the Massachusetts regulation mandates that the regulated "persons" develop programs that take into consideration "the size, scope and type of business" involved, "the amount of resources available" to the regulated person, "the amount of stored data" at issue, and "the need for security and confidentiality of both consumer and employee information."²⁷ Thus, an entity is left to grapple with the question of whether its particular security program meets the somewhat vague standards set by the regulation.

In recent years, the Massachusetts attorney general has relied on the regulation to bring actions against entities — even non-Massachusetts-based entities — that have failed to comply with the terms of the regulation. For instance, in July 2014, the attorney general entered into a consent judgment for \$150,000 to settle claims against the Women & Infants Hospital of Rhode Island, following allegations that the hospital failed to secure backup tapes containing sensitive personal information of several thousand Massachusetts

residents.²⁸ The state attorney general's office emphasized that it is "focused on ensuring that health care practices and their business associates abide by the state's data security laws" and other federal requirements.²⁹

NEW YORK – THE NEW GOLD STANDARD

The Massachusetts regulation was unquestionably an important step in the direction of minimizing the potential for cyberattacks. In imposing more stringent obligations on those who come into possession of personal information, the Massachusetts regulation can no longer be touted as the most comprehensive law to have been enacted by the states in this arena. New York — the self-proclaimed epicenter of the financial services industry — has recently enacted cybersecurity regulations with far-reaching implications.³⁰

Effective March 1, 2017, New York's Superintendent of Financial Services (NYDFS) promulgated a series of "Cybersecurity Requirements for Financial Services Companies," regulations codified at 23 NYCRR

Part 500. The introduction to the New York regulations makes clear that they arose as a result of the NYDFS' close "monitoring [of] the evergrowing threat posed to information and financial systems by nation-states, terrorist organizations and independent criminal actors," and the resultant desire to impose "certain regulatory minimum standards" that are "designed to promote the protection of customer information as well as the information technology systems of regulated entities."³¹

The entities covered by the New York regulations are those that are "operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization" under New York's banking law, insurance law, or financial services law.³² Accordingly, the regulations are designed to apply to banks, holding companies, lenders, and finance agencies.

Moreover, many of the requirements set forth in the regulations extend indirectly to "affiliates" and "third-party service providers" of covered entities, that is, persons controlled by or providing services to those entities

are also subject to a number of obligations set forth in the regulations. As such, covered entities must monitor and assess both their own cybersecurity policies and those of affiliates and third-party service providers with which they do business.

In this regard, vendors to covered entities gathering personal information for financing applications will be subject to the obligations imposed by the New York regulation, even if those vendors are out of state and are not required to be licensed under New York law.

The New York regulations concern the protection of "nonpublic information," which is broadly defined to include business-related information that, if tampered with, would cause a material adverse impact to the business, operations, or security of the covered entity as well as personal information concerning an individual, such as one's name used in connection with his or her Social Security number, driver's license number, or any account number.³³

These broad definitions mean that covered entities must implement programs and policies to

ensure the security of a wide range of data in their possession concerning individuals and entities. For example, not only do the regulations prescribe that covered entities maintain cybersecurity programs, they also specify particular core functions that must be performed by the cybersecurity programs. Those core functions include, similar to the Massachusetts regulation, that the program "identify and assess internal and external cybersecurity risks that may threaten the security or integrity of" the personal information in the entities' possession.³⁴

Moreover, even small companies³⁵ must now be prepared to implement wide-ranging cybersecurity programs to ensure that personal data remains safe from breach. Even if a company falls within one of the limited exemptions provided for under the New York regulations, such companies are still required to comply with certain requirements.

For example, exempt entities are still required to develop a cybersecurity program and cybersecurity policies, perform a risk assessment, maintain a third-party service provider secu-

rity policy, impose limitations on data retention, and provide certain notices to the superintendent. A failure to do so may subject those businesses to state enforcement actions.³⁶ Accordingly, the New York regulations have wide-ranging implications for businesses regardless of size.³⁷

Not only do the regulations prescribe that covered entities maintain cybersecurity programs, they also specify particular core functions that must be performed by the cybersecurity programs.

DELAWARE AND OTHER STATES

On the heels of New York's regulation, Delaware became the latest state to enact a statute imposing affirmative obligations on those in possession of personal information. Delaware's statute, which amends its data breach notification statute, becomes effective on April 14, 2018. It requires that "[a]ny

person who conducts business" in the state of Delaware and "owns, licenses, or maintains personal information *shall implement and maintain reasonable procedures and practices* to prevent the unauthorized acquisition, use, modification, disclosure, or destruction of personal information collected or maintained in the regular course of business."³⁸

These recent legislative measures undertaken by a number of states indicate that the trend will be for states to proactively ensure that personal information remains protected from disclosure.

The statute further specifies that the state attorney general "may bring an action in law or equity to address the violations of this chapter and for other relief that may be appropriate to ensure proper compliance with this chapter or to recover direct economic damages resulting from a violation, or both."³⁹

Given that this statute is not yet in effect, it is unclear to what extent the Delaware attorney general may rely on enforcement actions to ensure that Delaware businesses (and out-of-state companies doing business in Delaware) are actually implementing "reasonable procedures and practices" with respect to safeguarding personal information.

Massachusetts, New York, and Delaware are not alone in assuming the mantle of cybersecurity regulation. Indeed, other states have enacted legislation that would create some affirmative obligations on the part of businesses to ensure certain cybersecurity policies and procedures are in place.

For instance, Rhode Island recently enacted a statute that requires a "person" who "stores, collects, processes, maintains, acquires, uses, owns or licenses personal information about a Rhode Island resident" to "implement and maintain a risk-based information security program that contains reasonable security procedures and practices appropriate to the size and scope of the organization; the nature of the information; and the purpose

for which the information was collected" to ensure the security of the information.⁴⁰

Similarly, California recently enacted a statute requiring a business that "owns, licenses, or maintains personal information about a California resident" to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."⁴¹

In addition, Colorado and Vermont each also recently adopted regulations requiring broker-dealers and investment advisors to adopt written procedures that are "reasonably designed to ensure cybersecurity," as well as mandating annual risk assessments of those advisors' data security practices.⁴²

These recent legislative measures undertaken by a number of states indicate that the trend will be for states to proactively ensure that personal information remains protected from disclosure by imposing obligations on businesses to

protect that information on receipt, rather than to impose obligations solely in the event of a disclosure of the personal information.

HOW SHOULD EQUIPMENT FINANCE COMPANIES ADDRESS THESE REGULATIONS?

Massachusetts, New York, and Delaware are among the first in what will undoubtedly be a deluge of state regulation imposing affirmative cybersecurity requirements in the coming years. While it is impossible to determine what each state will require, it is evident that companies can proactively take certain steps now, both to aid in compliance with the growing body of legislation and to reduce the chance of a cybersecurity breach.

A Written Policy

First and foremost, it is essential that all companies, but especially those that regularly deal with customers' personal information (such as those in the equipment finance industry), develop written policies for identifying potential threats to secured information as well as create incident response plans

for what the company will do in the event of a breach, including specific notification protocols.

As set forth above, virtually every state has enacted statutory requirements with which companies must comply upon discovery of a data security breach. As such, it is prudent, and required by the leading states, for all companies to be prepared to comply with those requirements by creating written policies and procedures in accordance with the statutory mandate.

However, in order for these written policies to be compliant with many of the newest state regulations, they must go beyond simply setting forth a postbreach triage. In this regard, companies should first assess what types of data they handle and store, as well as how that data is currently being stored and who has access to that data. Taking this information into consideration, companies should then assess their current security measures, consider where weaknesses exist that may be exploited by those looking to do so, and implement strategies to mitigate or remediate those weaknesses.

Significantly, companies must look beyond their own systems to identify and assess security issues arising with third-party vendors and other service providers. The goal is to have a written plan, which must be reviewed and revised periodically,⁴³ that safeguards customers' personal information and otherwise complies with notification and reporting requirements of various state and federal laws — a gantlet that will not prove easy to navigate.

Encryption

To that end, one measure that businesses should strongly consider implementing is encryption of all records being stored or transmitted. Encryption is a way to protect secured content by converting plain text into cipher text and securing that text with a unique password in order to prevent unauthorized third parties from accessing the data. Current encryption products can be implemented in any business setting and can protect individual files and folders as well as full disks of data (laptops, desktop computers, and mobile devices).

Encryption is particularly helpful to the extent that a company

regularly stores or transmits personal information on laptops or in the cloud. Perhaps most importantly, encryption can provide a safe harbor under a number of state data breach notification laws. In other words, if exposed data was encrypted and the encryption keys were not themselves compromised, the company employing the encryption may be shielded from financial liability (as well as notification requirements) for the "breach."⁴⁴

While not inexpensive, encryption may prove to be well worth the initial investment, both in terms of protecting customer information and in helping to avoid running afoul of ever-increasing state regulations.

Crisis Management Team

Recent data security breaches, such as Equifax's, have raised another important consideration in planning for a security breach and the appropriate response to that breach: crisis management and communication. Meeting your company's mandatory minimum notice obligation is a far cry from ensuring that the *tone* of the notice is appropriate. If not handled properly, a company's notice following a breach

will compound the negative impact on that company's reputation.

The Equifax breach is instructive as an example of relaying the wrong message. At first glance, it seemed that Equifax was being proactive, offering "free" credit monitoring services to all impacted persons for one year. Initially, the message received was positive. However, the fine print of the initial offer disclosed that recipients of the credit monitoring services were being asked to relinquish and waive the right to participate in any class action initiated for losses incurred as a result of the breach, and instead were contractually bound to arbitrate.

As if this was not enough to sour the initial positive response to the offer of "free credit watch" services, it was then disclosed that the credit watch services offered were from *Equifax*: the very company that already demonstrated an inability to protect customers' personal information from unauthorized access. To even further compound the inept response by the company, several days after the breach, but more than a month before the public

announcement of the breach, key senior executives at Equifax sold enormous volumes of shares of their Equifax stock.

Indeed, since the initial public announcement, Equifax has further disclosed that a breach occurred earlier in the year, one which was never publicly disclosed, and it has since come to light that other senior executives sold Equifax stock before the recent disclosure.

Needless to say, any good will created by the proactive offering of free credit monitoring services has been substantially squandered by the subsequent and continuing disclosures. In doing so, the company effectively negated any good will created by the proactive offering of free credit monitoring services.

In addition to managing the public message, companies that experience data incidents and security breaches will likely face employee fears: whether as to job stability, company stability and/or the security of their own personal information held by the company as their employer. Clearly, the distraction of media coverage and public perception can affect productivity within an organization.

Encryption is a way to protect secured content by converting plain text into cipher text and securing that text with a unique password in order to prevent unauthorized third parties from accessing the data.

Given the foregoing considerations — related to both external and internal concerns — it is critical to engage an outside firm that specializes in data breach crisis management and communication, and such engagement should not be an afterthought. Indeed, while many insurance policies cover the costs associated with hiring such a firm, a company should ensure that the firm ultimately retained is competent to handle the requisite messaging and crisis management that emanates from almost every significant data breach.

Cybersecurity Insurance

Finally, companies of all sizes should purchase cybersecurity insurance. Such insurance will help ensure certain coverage in

the event of a breach — coverage for losses that are generally not otherwise covered under standard property and casualty policies.

At a minimum, cybersecurity insurance should cover not only all costs of a data breach — including those associated with customer notifications, crisis management, and attorneys' fees.

The cost for this insurance is actually decreasing, while at the same time it is evolving to provide greater coverage for the increased exposure in the marketplace.⁴⁵ Every company should scrutinize the coverage offered, as such policies widely vary as to coverage and exclusions.

At a minimum, cybersecurity insurance should cover not only all costs of a data breach — including those associated with customer notifications, crisis management, and attorneys' fees — but should also provide

coverage for fines associated with the breach and the potential failure to comply with various government regulations. This latter requirement is critical because, as shown above, the trend at the state level is toward more regulations that require proactive actions — inevitably leading to more fines.

In any event, cybersecurity insurance must be considered a cost of doing business for any company dealing with customers' personal information. Given the uncertainty as to whether (and when) an attack or breach will occur, and the potential magnitude of that attack or breach, a company may find some measure of security in knowing that it has a cybersecurity policy to help mitigate that risk.

Of course, each business must take into consideration its own potential liability exposure and budgetary constraints to determine whether a cybersecurity insurance policy is appropriate for that business, while being mindful of recent regulatory and private actions resulting from data breaches — breaches for which a company may not have planned.

CONCLUSION

Recent years have demonstrated the necessity of effective cybersecurity programs for every company, but especially those that are regularly in the position of collecting and securing customers' personal information, not only because of the practical aspect of such programs but also because of the recent state government focus on proactive cybersecurity compliance.

In order to navigate the possibly confusing waters of various government regulations, all companies — especially those in the equipment financing industry — would be well served to seek out professional advice to assist in ensuring compliance. This should include not only cybersecurity experts but also knowledgeable insurance brokers that can recommend appropriate policies to meet the needs of the business, as well as other professionals who can assist in training both senior management and other personnel as to the requirements of these new regulations.

Moreover, legal counsel can provide invaluable assistance in navigating the law and ensuring

that the company complies with the requirements now mandated by various government agencies. As discussed above, the ramifications for failing to ensure compliance can be financially ruinous.

In today's era of state regulation, it is essential that all companies, regardless of their size, assess the types and amounts of personal information being received and stored, and implement appropriate security programs and policies with respect to protecting that information.

Endnotes

1. Insurance Information Institute, "Cyber Risk: Threat and Opportunity," at 5 (October 2015).
2. Identity Theft Resource Center, "Data Breaches Increase 40 Percent in 2016, Finds New Report from Identity Theft Resource Center and Cyberscout" (Jan. 19, 2017), available at <http://www.idtheftcenter.org/2016databreaches.html>.
3. Verizon, "2016 Data Breach Investigations Report," at 6.
4. Verizon, "2016 Data Breach Investigations Report."
5. See Ponemon Institute LLC, "2016 Cost of Data Breach Study: Global Analysis," at 2 (June 2016), available at <https://public.dhe.ibm.com/common/ssi/ecm/se/en/sel03094wwen/SEL03094WWEN.PDF>.
6. See New Jersey Division of Consumer Affairs, news release, "Horizon Blue Cross/Blue Shield of New Jersey Agrees

to Pay \$1.1 Million, Tighten Data Security to Settle Allegations of Privacy Lapses Concerning Personal Information of Policyholders" (Feb. 17, 2017), available at <http://www.njconsumeraffairs.gov/News/Pages/02172017.aspx>.

7. See Federal Trade Commission, news release, "Operators of AshleyMadison.com Settle FTC, State Charges Resulting from 2015 Data Breach that Exposed 36 Million Users' Profile Information" (Dec. 16, 2016), available at <https://www.ftc.gov/news-events/press-releases/2016/12/operators-ashleymadisoncom-settle-ftc-state-charges-resulting>.

8. See New York State Office of the Attorney General, news release, "A.G. Schneiderman Announces \$18.5 Million Multi-State Settlement With Target Corporation Over 2013 Data Breach" (May 23, 2017), available at <https://ag.ny.gov/press-release/ag-schneiderman-announces-185-million-multi-state-settlement-target-corporation-over>.

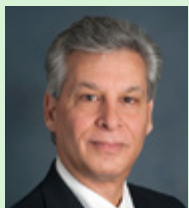
9. See Liz Moyer, "Prosecutors Announce More Charges in Hacking of JP Morgan Chase," *New York Times*, Nov. 10, 2015, available at <https://www.nytimes.com/2015/11/11/business/dealbook/prosecutors-announce-more-charges-in-jpmorgan-cyber-attack.html>.

10. See *Remijas v. The Neiman Marcus Group, LLC*, No. 14 Civ. 1735 (N.D. Ill.).

11. Further, beyond fines and litigation, a data breach could have a significant impact on business transactions the company is involved in. For instance, following the notorious data breach of Yahoo's user information, Yahoo was forced to reduce the price that Verizon would pay to purchase Yahoo's business by \$350 million. See Vinu Goel, "Verizon Will Pay \$350 Million Less for Yahoo," *New York Times*, Feb. 21, 2017, available at <https://www.nytimes.com/2017/02/21/technology/verizon-will-pay-350-million-less-for-yahoo.html>.

12. 15 U.S.C. § 6801(a).

13. 15 U.S.C. § 6809(3); 12 U.S.C. § 1843(k)(4).
14. Federal Trade Commission, "Financial Institutions and Customer Information: Complying with the Safeguards Rule" (last updated April 2006), available at <https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying>.
15. *Id.*
16. *Id.*
17. A "consumer" is an "individual" who obtains "a financial product or service" from a financial institution "that is to be used primarily for personal, family, or household purposes." See 16 C.F.R. § 313.3(e). "Customers" are simply consumers who have a continuing consumer relationship with a financial institution and obtain services such as a credit or investment account, a loan, an insurance product, or financial or economic services. 16 C.F.R. § 313.3(i)(1)(2). Importantly, because "consumers" are defined as "individuals," the term does not apply to commercial clients, such as sole proprietorships, and thus the Financial Privacy Rule also does not apply to those clients. See Federal Trade Commission, "How to Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act" (last updated July 2002), available at <https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm>.
18. See 16 C.F.R. § 313.4 through § 313.9.
19. See Alaska Stat. § 45.48.010 *et seq.*; Ariz. Rev. Stat. § 18-545; Ark. Code §§ 4-110-101 *et seq.*; Cal. Civ. Code §§ 1798.29, 1798.82; Colo. Rev. Stat. § 6-1-716; Conn. Gen. Stat. §§ 36a-701b, 4e-70; Del. Code tit. 6, § 12B-101 *et seq.*; Fla. Stat. §§ 501.171, 282.0041, 282.318(2)(i); Ga. Code §§ 10-1-910, -911, -912, § 46-5-214; Haw. Rev. Stat. § 487N-1 *et seq.*; Idaho Stat. §§ 28-51-104 to -107; 815 ILCS §§ 530/1 to 530/50; Ind. Code §§ 4-1-11 *et seq.*, 24-4-9 *et seq.*; Iowa Code §§ 715C.1, 715C.2; Kan. Stat. § 50-7a01 *et seq.*; KRS § 365.732, KRS §§ 61.931 to 61.934; La. Rev. Stat. §§ 51.3071 *et seq.*; Me. Rev. Stat. tit. 10 § 1346 *et seq.*; Md. Code Com. Law §§ 14-3501 *et seq.*, Md. State Gov't Code §§ 10-1301; Mass. Gen. Laws § 93H-1 *et seq.*; Mich. Comp. Laws §§ 445.63, 445.72; Minn. Stat. §§ 325E.61, 325E.64; Miss. Code § 75-24-29; Mo. Rev. Stat. § 407.1500; Mont. Code §§ 2-6-1501 to -1503, 30-14-1701 *et seq.*, 33-19-321; Neb. Rev. Stat. §§ 87-801 *et seq.*, 242.183; Nev. Rev. Stat. §§ 603A.010 *et seq.*; N.H. Rev. Stat. §§ 359-C:19 *et seq.*; N.J. Stat. § 56:8-161 *et seq.*; H.B. 15, 53rd Leg., 1st Sess. (N.M. 2017); N.Y. Gen. Bus. Law § 899-AA, N.Y. State Tech. Law 208; N.C. Gen. Stat. §§ 75-61, 75-65; N.D. Cent. Code §§ 51-30-01 *et seq.*; Ohio Rev. Code §§ 1347.12, 1349.19, 1349.191; 1349.192; Okla. Stat. §§ 74-3113.1, 24-161 to -166; Oregon Rev. Stat. §§ 646A.600 to .628; 73 Pa. Stat. §§ 2301 *et seq.*; R.I. Gen. Laws §§ 11-49.3-1 *et seq.*; S.C. Code § 39-1-90; Tenn. Code §§ 47-18-2107; 8-4-119; Tex. Bus. & Com. Code §§ 521.002, 521.053; Utah Code §§ 13-44-101 *et seq.*; Vt. Stat. tit. 9 §§ 2430, 2435; Va. Code §§ 18.2-186.6, 32.1-127.1:05; Wash. Rev. Code §§ 19.255.010, 42.56.590; W.V. Code §§ 46A-2A-101 *et seq.*; Wis. Stat. § 134.98; Wyo. Stat. §§ 40-12-501 *et seq.*; D.C. Code §§ 28-3851 *et seq.*
20. Note that, by 2010, HIPAA and the FTC Act (Section 5 being applied as to companies' unfair and/or deceptive practices as to their stated privacy policies) predated the Massachusetts statutory framework, and a number of states had enacted legislation that mandated the protection of personal information. However, the regulation issued by Massachusetts was at the time considered the most onerous state data security regulation and was often considered a gold standard for a more proactive state approach.
21. 201 CMR 17.01(1).
22. The regulation defines "personal information" to include "a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of" certain "data elements," which include Social Security Number, driver's license number, or state-issued identification card number, or "financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account." 201 CMR 17.02. "Personal information" does not include "information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public." *Id.*
23. 201 CMR 17.01(2) (emphasis added); 201 CMR 17.02.
24. 201 CMR 17.03(1).
25. 201 CMR 17.03(2)(a)-(j).
26. 201 CMR 17.03(f)(1)(2).
27. 201 CMR 17.03(1)(a)-(d).
28. See Attorney General of Massachusetts, news release, "Women & Infants Hospital to Pay \$150,000 to Settle Data Breach Allegations Involving Massachusetts Patients" (July 23, 2014), available at <http://www.mass.gov/ago/news-and-updates/press-releases/2014/2014-07-23-women-in-fants-hospital.html>.
29. *Id.*
30. Again, even though state data breach and privacy laws, including those of Massachusetts, predated the New York regulations, the governor lauded the regulations as the "first in the nation." See New York Department of Financial Services, news release, "Governor Cuomo Announces First-in-the-Nation Cybersecurity Regulation Protecting Consumers and Financial Institutions from Cyberattacks to Take Effect March 1" (Feb. 16, 2017), available at <http://www.dfs.ny.gov/about/press/pr1702161.htm>.
31. 23 NYCRR 500.00.
32. 23 NYCRR 500.01(c).
33. 23 NYCRR 500.01(g).
34. 23 NYCRR 500.02(b).
35. The New York regulations do provide certain exemptions from the requirements stated therein for smaller businesses. For example, an entity is exempt from certain requirements under the regulations if it has fewer than 10 employees, earned less than \$5 million in gross annual revenue in each of the last three fiscal years, or has less than \$10 million in year-end total assets. See 23 NYCRR 500.19.
36. See 23 NYCRR 500.20.
37. Companies subject to the New York regulations must also be aware that pursuant to the regulations, a "Senior Officer" must approve the entity's cybersecurity policy and is responsible for "the management, operations, security, information systems, compliance and/or risk" of the covered entity. 23 NYCRR 500.01(m); 23 NYCRR 500.03. Moreover, covered entities are also required to designate an individual as the "Chief Information Security Officer" (CISO), who is responsible for overseeing and implementing the covered entity's cybersecurity program, enforcing the cybersecurity policy, and annually reporting to the covered entity's board of directors. The CISO may be employed by either the covered entity itself or by an affiliate or third-party service provider; to the extent the CISO is employed by an affiliate or third-party service provider, the covered entity still retains responsibility for compliance with the regulations, and must designate a senior member of the covered entity to oversee the third-party service provider. See 23 NYCRR 500.04.
38. House Substitute No. 1 for H.B. 180, 149th Gen. Assem. (Del. 2017) (emphasis added).
39. *Id.*
40. R.I. Gen. Laws § 11-49.3-2(a).
41. Cal. Civ. Code § 1798.81.5(b).
42. See 3 CCR 704-1, Rule 51-4.8 and Rule 51-4.14; V.S.R. § 8-4.
43. For example, the New York regulations require that covered entities conduct a periodic risk assessment to determine whether the entities' cybersecurity programs are sufficient to handle possible threats. Specifically, the regulations state that the risk assessment "shall allow for revision of controls to respond to technological developments and evolving threats and shall consider the particular risks of the Covered Entity's business operations related to cybersecurity, Nonpublic Information collected or stored, Information Systems utilized and the availability and effectiveness of controls to protect Nonpublic Information and Information Systems." 23 NYCRR 500.09(a).
44. See e.g., N.J. Stat. § 56:8-161 (defining "breach of security" as "unauthorized access to electronic files, media or data containing personal information that compromises the security, confidentiality or integrity of personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable") (emphasis added).
45. For instance, cybersecurity policies may be customized to the particular business and may include a variety of coverage, such as liability for security or privacy breaches, costs associated with privacy breaches, business interruption related to a security or privacy breach, and/or expenses related to cyber extortion or cyberterrorism. See National Association of Insurance Commissioners & the Center for Insurance Policy and Research, "Cybersecurity" (last updated April 3, 2017), available at http://www.naic.org/cipr_topics/topic_cyber_risk.htm. However, while cyber insurance often covers governmental fines and penalties, these new state regulations contemplate prebreach penalties that may not be covered. In this regard, it is critical to check your policies to ensure that you understand the coverage provided.



Frank Peretore

fperetore@csglaw.com

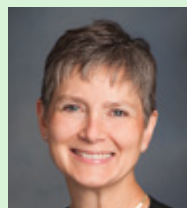
Frank Peretore is a member and co-chair of the Equipment Leasing and Finance Group of the law firm Chiesa Shahinian & Giantomasi PC, based in West Orange, New Jersey. With more than 30 years' experience representing equipment lessors and asset-based lenders, he represents national and regional finance companies and banks, ranging from closely held companies to Fortune 100 members. Mr. Peretore's expertise includes the drafting and negotiation of loan/lease documentation and the purchase/sale of individual transactions and full portfolios, as well as the enforcement of lessors' and secured creditors' rights in thousands of matters in the state, federal, and bankruptcy courts. He has published two books, *Workouts and Enforcement for the Secured Creditor and Equipment Lessor* (Lexis/Nexis 2015 edition) and *Secured Transactions for the Practitioner* (2018 edition).



Robert L. Hornby

rhornby@csglaw.com

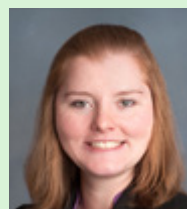
Robert L. Hornby is co-chair of Chiesa Shahinian & Giantomasi's Equipment Leasing and Financing Group. An experienced litigator, he represents national and regional banks and finance companies in all aspects of equipment leasing, asset based lending, and civil litigation in New York and New Jersey state and federal courts. He regularly counsels clients on a wide range of matters unique to the equipment leasing and finance industry, including drafting master documentation, enforcement of secured creditors' rights, and lien priority. Mr. Hornby also counsels clients regarding their compliance with state and federal cybersecurity laws and regulations. He recently co-authored the 2018 edition of *Secured Transactions for the Practitioner: How to Properly Perfect Your Personal Property Lien and Assure Priority*. Mr. Hornby served as a judicial law clerk for the Hon. David S. Baime, PJAD (ret.) in the New Jersey Appellate Division. He received his law degree cum laude from Seton Hall University School of Law, and his undergraduate degree cum laude from the University of Arizona, Tucson.



Michelle A. Schaap

mschaap@csglaw.com

Michelle A. Schaap, member of Chiesa Shahinian & Giantomasi, practices primarily in cybersecurity and corporate law, particularly as it pertains to the financial and construction industries. Combining her technology and corporate experience, she has developed the firm's cybersecurity practice. Ms. Schaap routinely advises clients on cybersecurity preparedness and incident response and trains companies in best practices for data security procedures. In addition, she has been a panelist for the New Jersey State Bar Association, New Jersey Women Lawyers Association, and Seton Hall University School of Law. Ms. Schaap has been quoted in numerous *NJBIZ* articles and *New Jersey Business* and *New Jersey Law Journal*. She was selected by Leading Women Entrepreneurs as one of New Jersey's 2017 Leading Women Intrapreneurs. She is president-elect of the New Jersey Women Lawyers Association and serves on the Information Technology Committee for the New Jersey Business and Industry Association. Ms. Schaap received her law degree from Rutgers University School of Law, Newark, New Jersey; a certificate in cybersecurity and privacy law from Mitchell Hamline School of Law, St. Paul, Minnesota; and her undergraduate degree cum laude from Cornell University, Ithaca, New York.



Brigitte M. Gladis

bgladis@csglaw.com

Brigitte M. Gladis is an associate in Chiesa Shahinian & Giantomasi's Litigation and White Collar Criminal Defense and Government Investigations groups. She handles a variety of complex litigation matters across different industries, including contract and partnership disputes, shareholder oppression claims, government investigations, and professional liability matters. Prior to joining the firm, Ms. Gladis served as a Superior Court of New Jersey, Appellate Division law clerk. She graduated summa cum laude from Seton Hall University School of Law, Newark, New Jersey.