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

EDITORIAL BOARD

EQUIPMENT LEASING & FINANCE FOUNDATION
Your Eye on the Future

CONNECT WITH THE FOUNDATION

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.

 • ISSN 0740-008X

Thriving Millennials: The Next Generation of Industry Professionals

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.

The Millennial generation is quickly influencing and re-shaping the U.S. economy, culture, workplace, geopolitical arena, and the commercial equipment leasing and finance industry. This article examines the attributes that Millennials (born between the early 1980s and mid-to-late 1990s) are looking for from an employer, how they want to contribute, what the industry has to offer to the brightest and most productive young professionals, and how the industry must work harder to attract talented professionals.

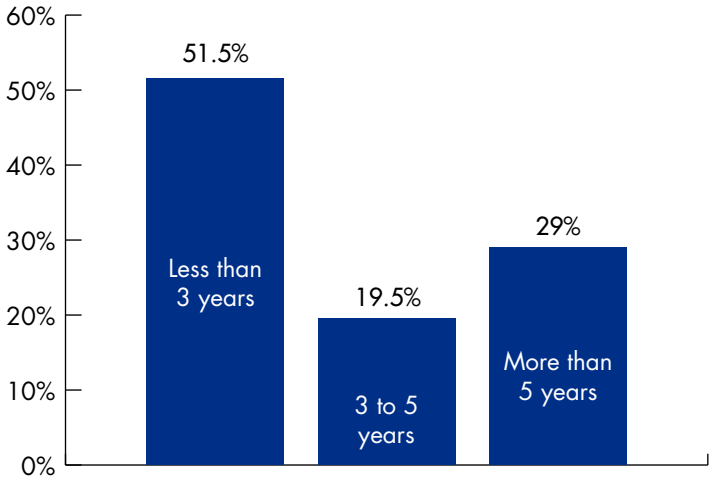
Wheeler Business Consulting conducted a research project to determine key factors motivating thriving Millennials in the equipment leasing and finance industry; and how organizations are embracing the next generation of industry participants. The information provided is based on industry specific surveys completed in 2016 and 2017, interviews with young professionals participating in the equipment leasing and finance industry and their managers, and ongoing communication with leaders throughout the industry.

The 2017 survey included 111 participants representing multiple sectors, positions, and employers within the industry. As shown in Figure 1, 51.5% have three years or less of industry experience, 19.5% have three to five years' experience, and 29% have over five years' experience.

The Millennial generation follows Generation X, born between 1965 and 1979; and Baby Boomers, born between 1946 and 1964. The research participants and the focus of the article ranged in age from the low 20s to mid-30s and are often referred to in this article as "young professionals." The Millennial label is not easily embraced by many professionals in that age group.

The most aggressive and ambitious Millennials share strong, aspirational attributes with past generations and they are reluctant to identify with some of the negative, generalist characteristics that so often are attached to the Millennial label. The most successfully focused Millennials want opportunities and upward mobility.

Figure 1. Experience in Commercial Equipment Leasing and Finance Industry



Source: Wheeler Business Consulting, 2017.

Seasoned veterans, managers, and business owners often state that the missing link for younger professionals is the lack of a comprehensive, global understanding of the industry, inasmuch as many understand their own company's capabilities.

The most successful young professionals are finding their way to the top by embracing employers that match their needs; they are attracting strong clients, providing superior services; and they are doing whatever is necessary to outperform their peers. The brightest and most ambitious Millennials are already assuming leadership roles in the industry. They are lead sales originators, strong credit managers, team leaders, industry volunteers, and top management participants.

Younger professionals who have entered the industry over the last five to 10 years see the potential for success, with 84.5% of surveyed respondents claiming the industry is currently robust and full of opportunities for young professional talent. Not only do 89.4% see multiple paths to success within their current organizations and/or within the industry, but the same percentage sees a bright future for the entire equipment leasing and finance industry. As with past generations, the young emerging professionals know the industry is competitive (94%) and realize that success will take perseverance, dedication, and hard work.

OTHER CHARACTERISTICS

Millennials require a defined career path. The process must be a collaboration between the employer and employee, with mutually beneficial outcomes. All employees require benchmarks and goals; younger employees may need better defined benchmarks to provide clarity and to more closely measure their own accomplishments.

They also want the tools necessary to exceed expectations. Their exceeding reasonable goals and desired benchmarks should result in meaningful rewards and compensation to encourage their career advancement.

One of the most vocal frustrations expressed by young professionals in the research was that employers too often overpromise and underdeliver with regard to benchmarks and expectations. Career paths are often based on timing matrices, rather than results. (For example, within six months, an individual should be able to accomplish X; within three years, a successful candidate should be making Y amount of money.) Successful younger professionals want to know what will happen when they meet their goals within, say, half the time expected. Similarly, they want assurance that if they appear well on the path to success, but that the process is taking slightly longer than expected, that the opportunity for advancement will still be there.

All employees want to be treated fairly and to be recognized for their accomplishments. Employee loyalty is best achieved when expectations are clearly defined, when the work environment is conducive to career advancement, and when the employer provides the necessary tools to allow them to succeed.

Conversely, employers are loyal to their employees when the employees embrace the culture of the company; use the tools made available by the employer, work to advance the organization as well as their personal goals; and contribute to the well-being of the entire organization. The path to success is mutual and should be communicated upfront, without any ambiguity, in the interviewing process and during employment.

Young professionals aspire to be well trained, knowledgeable, and strong participants in the industry. One of the challenges for the industry is the means to expedite education and training. Millennials in the industry want immediate gratification and success. Although the equipment leasing and finance industry is not difficult to learn, it often takes hands-on experience and time to fully understand the many nuances involved in originating, underwriting, funding, and collecting strong, well-performing assets.

The two-year management training programs of the 1970s and 1980s are ancient history. Many independent companies, banks, and institutional players can no longer justify long-term investment when they need immediate results. Aggressive, younger professionals are looking to contribute more quickly, and they are unwilling to assume subpar incomes during a long-term training program. Therefore, the industry has been forced to accept on-the-job training, which too often results in frustration and impatience on the part of both the employers and employees.

Seasoned veterans, managers, and business owners often state that the missing link for younger professionals is the lack of a comprehensive, global understanding of the industry, inasmuch as many understand their own company's capabilities. In the recent survey of young professionals in the industry, only:

- 48.5% had an above average or higher understanding of the application-only credit process
- 36.5% had an above average or higher understanding of full disclosure transactions

- 46.9% had an above average or higher understanding of pricing and structures in the industry
- 13.3% had an above average or higher understanding of residual evaluations
- 19.4% had an above average or higher understanding of portfolio management
- 20.6% had an above average or higher understanding of the legal aspects of the industry

Of the surveyed participants, 94.1% desire additional, ongoing learning opportunities, and they recognized their lack of industry knowledge is limiting their ability to succeed (Fig.2). Interviews suggested that emerging talent routinely express frustration with regard to their knowledge limitations. (Many internal and external resources are available through associations, industry events, foundations, and service providers.)

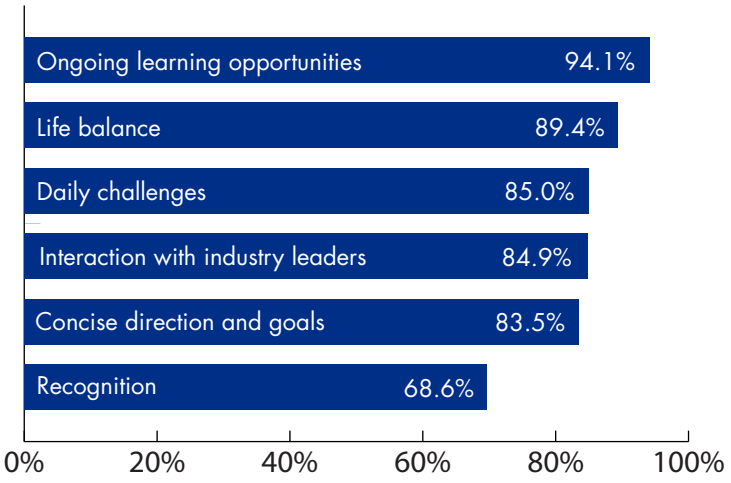
EXPEDITING THE LEARNING CURVE

However, ongoing educational opportunities are not being sufficiently embraced by employers and employees to expedite the learning curve of the Millennial generation. An impatient, yet driven, emerging workforce can provide advancements, innovation, and a clear path toward corporate growth. Comprehensive understanding of the industry — which Millennials must have the patience to gain — encourages better decisionmaking processes, more efficiencies, stronger performing assets, and better client relationships.

Top-performing organizations among banks, independents, captives, investors, and service providers are investing time and money into comprehensive training programs and encouraging career advancement. Career advancement training programs are being well received by both new and seasoned employees.

Survey interviews reflected that young professionals in the industry do not want micromanagement, but rather to be trained and then left alone to get the job done. There is a paradox between old-line supervisors wanting daily activity reports to monitor efforts and determine individual challenges and younger professionals wanting the freedom to make mistakes, to learn through trial and error, and to individually determine their best work habits.

Figure 2. Attributes That Millennials Desire in an Employer



Source: Wheeler Business Consulting, 2017.

One manager reluctantly explained how when he enforced a strict 9-to-5 workday, his younger professionals were less productive than when he provided them the freedom to create their own schedules. With more flexible schedules, employees were coming in early to make calls on the East Coast and staying later to make calls on the West Coast. He found some top producers working additional hours to accomplish necessary paperwork. The flexible work habits created some internal conflicts; however, the staff adjusted and sales and operational production increased.

Freedoms such as flexible schedules come with responsibility and accountability and often need to be earned over time. There is a fine line between productive freedoms and an environment that encourages abuse. Strong senior leadership encourages best practices and is not afraid to empower the top talent to make the right choices. Young, aggressive professionals want mentorship and encouragement and will always follow a strong leader who demands high results.

Of the surveyed participants, 94.1% desire additional, ongoing learning opportunities, and they recognized their lack of industry knowledge is limiting their ability to succeed.

Inasmuch as each new generation has similarities, there also are differences. Millennials want diversity of ethnic groups, age groups, task groups in their work environment, and similar variety in their social circles. They seek and require more balanced lifestyles than their predecessors. Most families have two income-producers who are equally committed to their careers and families. Both partners are engaged in every aspect of child rearing, family responsibilities, and their personal career advancement. Time is a valuable commodity at work and at home, mandating efficiency 24/7. Therefore, Millennials want to be assured

that their time at work is being used wisely and is fully aligned with their global perspective, life goals, and financial security.

Young professionals in the industry want to be part of the decisionmaking process. They want to fully understand the mission and vision of the company they are helping to move forward.

As shown in Figure 2, the participants in the survey overwhelmingly (89.4%) indicated life balance as an important or higher attribute in considering career choices (59% ranked life balance as significantly important). Several interviewees indicated life balance as the number one influencer of workplace acceptability, and they voiced their observation that top employers are embracing more holistic work environments, which encourage family-work integration. (Employers are providing onsite services to help younger professionals — day care services, finess centers, and so on.)

THE ROLE OF TECHNOLOGY

A company's willingness to embrace technology is a main driver in recruiting new and younger talent. Because the Millennial generation is the most educated and technologically advanced generation of all time, its members want employment and career opportunities that embrace technology. While they are encouraged by recent advancements that their companies have made, they crave additional automation for real-time data and better communications.

Many individual comments made throughout the survey revolved around the use of technology: how younger employees are more proficient in using, designing, and promoting technology as an effective tool, and how more progressive organizations are leaning on the next generation not only to use technology, but to implement technology that drives bottom-line results.

Of the surveyed participants,

- 61% stated that the industry is behind or significantly behind the times with regard to automation and technology.
- 97.6% believe that technological advancements will distinguish the winners and losers in the industry over the next few years.

At the same time, veteran management teams often see younger professionals using automation as a substitute for client interaction and are critical of the lack of personal contact between service providers and their clients. Automation is not necessarily a substitute for personal customer service. Top performers use technology as a tool and a means to effectively communicate with their clients, to interact on multiple levels to enhance their in-person contacts, to be more efficient, and to deliver better services to their business partners and their clients.

On another front, Millennials are becoming the corporate decision-makers involved in equipment acquisitions. In the near future, vendors, end-users, and other stakeholders will require (and in many cases are already demanding) advanced technologies to expedite and fund transactions.

Financial-technology (fin-tech) will have a significant influence on how businesses and consumers will interact with financial partners in the future. Fin-tech is the next generation of financial services, and even the most conservative financial institutions are embracing its capabilities and viabilities in the market. The Millennial generation is positioned to drive new technological advancements in the financial sectors, which will greatly alter the current processes and product delivery systems used by the equipment leasing and finance industry.

Young professionals in the industry want to be part of the decisionmaking process. They want to fully understand the mission and vision of the company they are helping to move forward. More progressive companies are including them in decision-making meetings, allowing their younger staff members to watch, learn, understand, and contribute to the conversation.

IMPROVING CUSTOMER RELATIONSHIPS

Contributions being made by Millennials are positively changing the landscape of customer relationships and services offered by old-line companies. This generation is wired into the new economy, new technology, and new resources that are readily available to progressive organizations.

Part of the learning process is to be involved, and many managers are finding positive results by asking more, not less, from their younger staff. Professionals of all ages want to know why policies are created and how they impact the bottom line. Empowering younger professionals to participate in the policy decisionmaking process, develop and expand their career paths, grow, and learn through experiences is critical to the long-term development of industry leaders.

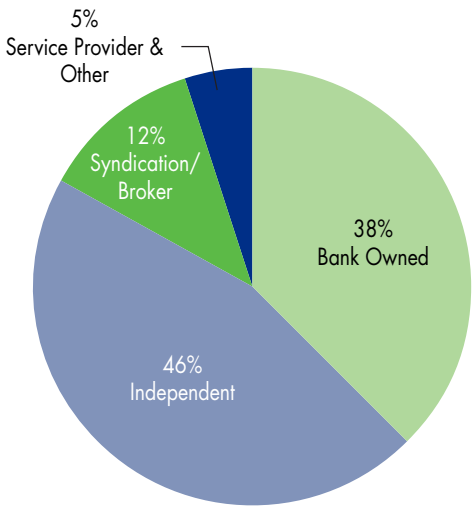
The equipment leasing and finance industry offers unlimited opportunities for Millennials. This mature industry has a history of innovation and adaptability. The equipment leasing and finance industry has a wide range of employers, positions and career paths for younger professionals (shown in Fig. 3 and Fig. 4). Participants in the industry typically perceive that most new entries are cultivated through the sales and marketing track, which remains strong and viable.

However, the industry offers many opportunities in operations, credit functions, technology, capital markets, accounting, legal, and more. The industry is rich in diverse opportunities in small, privately held companies; banks; captives; international organizations; investment firms; and entrepreneurial ventures — no matter what the aspirations of the Millennial or his or her skill sets. Clearly, young professionals can choose a multitude of equipment types, industries, and individual clients based on their skill sets.

The equipment leasing and finance industry has a history of providing above-average income potential for committed participants. Although 51.5% of the surveyed participants have less than three years' experience, 30% of the participants have incomes between $50,000 and $125,000; 25% of the participants have incomes between $125,000 and $200,000; and 7.3% have incomes above $200,000.

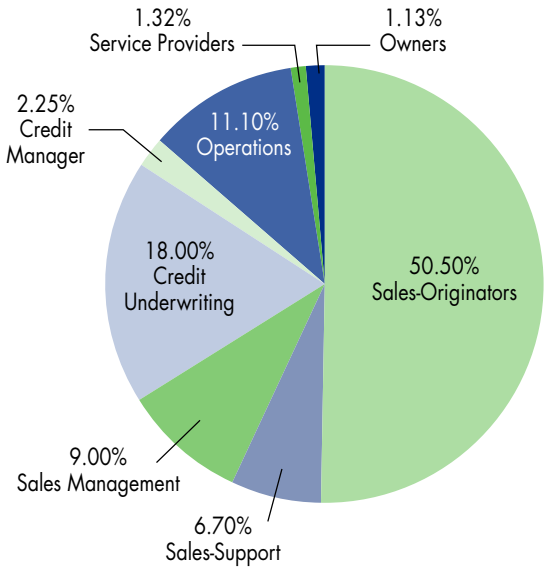
Prior to entering the equipment leasing and finance industry, most participants had little if any knowledge or understanding of the business. However, they embraced the opportunity and leveraged their personal skills to build a rewarding career. Many of the seasoned top leaders have had multiple positions in the industry, have experiences in every aspect of the business, and have engaged on multiple levels with their industry peers, business partners, investors, and other stakeholders. Top leaders in equipment leasing and finance continue to seek new opportunities and they are excited to share their experiences with younger professionals.

Figure 3. Employers of Millennials in the Equipment Leasing and Finance Industry



Source: Wheeler Business Consulting, 2017.

Figure 4. Positions Held by Millennials in the Equipment Leasing and Finance Industry



Source: Wheeler Business Consulting, 2017.

RECRUITING THE BEST TALENT

One of the universal challenges conveyed by employees, through the interviewing process, is that better efforts need to be given to recruiting the best talent available. The industry has so much to offer, but too few outside of the industry know about the $1 trillion commercial equipment leasing and finance industry that supplies needed capital to small, medium, and large companies throughout the United States. The many resources include the Equipment Leasing and Finance Foundation's guest lecturing program and internship resource database to educate university and college students.

However, the grass roots will ultimately drive the major recruiting efforts. Of the survey participants, 90.4% claim that they would highly recommend the industry to a friend. Companies are actively recruiting and promoting the significance of the equipment leasing and finance industry. Select companies are hiring paid interns and helping them to learn about the industry, with the expectation of retaining the interns as full-time employees. Our research produced the following key takeaways for the industry's employees and employers. Millenials:

The grass roots will ultimately drive the major recruiting efforts. Of the survey participants, 90.4% claim that they would highly recommend the industry to a friend.

- are a tech-driven generation, already accustomed to functioning in a fast-paced world.
- are impatient and are looking for success in the short term. However, they are impressed with the long-term potential offered by the equipment leasing and finance industry. The

challenge for Millennials and employers in the industry is to integrate short-term results with sufficient long-term preparation and development of future leaders.

- will be attracted and retained by those organizations that offer a defined career path, comprehensive training, and career enhancement opportunities.

Proactive employers are embracing Millennials and are incorporating these key takeaways as motivators and career enhancers to recruit and retain the best talent. It is the responsibility of the industry and all its participants — from top management on down — to showcase the attractiveness of the industry, to communicate strongly and often the opportunities that are available, and to encourage talented professionals to participate in the equipment leasing and finance industry.

Young professionals are offering a new perspective to a mature industry. Millennials are demanding change, innovation, and efficiencies. Organizations and industry veterans are sharing past knowledge and wisdom with young professionals; they are helping the Millennial generation to prepare for all economic conditions; and they are encouraging the next generation to reach new levels of productivity and success.

The brightest and most productive in the equipment leasing and finance industry are sharing their successes with other Millennials through networking groups, association participation, and internal mentoring programs. They have an appreciation for the personal growth potential available in the industry; and they are excited about the future possibilities for themselves and their peers.

Scott A. Wheeler

scott@wheelerbusinessconsulting.com

Scott A. Wheeler is president of Wheeler Business Consulting LLC, based in Fallston, Maryland. The company offers training and consulting to lessors, banks, origination firms, and investors in the commercial equipment leasing and financing industry. Prior to starting his firm, Mr. Wheeler led several leasing operations and has held executive positions with publicly held bank leasing operations and privately held independent lessors. His book, *Call to Action – For Equipment Leasing and Finance Professionals,* was published in 2015. His article "Efficiencies in the Indirect Market" appeared in the Spring 2013 issue of this journal. Mr. Wheeler is a member of ELFA and the National Equipment Finance Association. A certified lease and Finance professional, he holds a BS in economics from McDaniel College, Westminster, Maryland, and an MBA from the Sellinger School of Business, Loyola University of Maryland, in Baltimore.

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?

Competition for market share is the key to innovation and improved choice for customers, but the playing field must be at least reasonably level to sustain competition. The current system of determining capital adequacy for Canadian banks gives the largest advantage to a small group of six domestic banks. The advantage is so great that these banks have the ability to outprice or profitably acquire any domestic competitor that is of interest or a threat to these dominant players.

Canadian regulators have been trying for many years to improve competition without adding risk to the banking system in Canada. The efforts of regulators, while preserving the strength of the main Canadian banks, have significantly reduced competition and created a concentration of market share that is unhealthy.

The dominant banks are now among the largest and strongest in the world, but this success has come at a price. The Canadian domestic economy is heavily reliant on the six largest banks. The Big Six are Royal Bank of Canada, Toronto-Dominion Bank, Bank of Nova Scotia, Canadian Imperial Bank of Commerce, Bank of Montreal, and National Bank of Canada, and their success has become a threat to innovation and competition in the Canadian banking sector.

This problem is not new in Canada: in 1999 the Department of Finance introduced measures intended to reform Canada's financial services sector.[1] As a result of reforms, the number of domestic banks in Canada increased from eight to 30 between 1999 and 2016. However, during the same period the market share of the largest six banks has grown.

According to the Department of Finance Canada (1999),

> The six largest banks continue to hold most of the market share in the banking sub-sector. Together, they hold $4.6 trillion in assets. The large banks' share of all assets in the banking sub-sector has increased since the financial crisis, and they now represent 93% of all banking assets, compared with about 90% in 2007.[2]

Part of the gain in market share came from the changes forced on U.S. and other global financial institutions that found themselves with much less capital to lend. U.S. lessors including GE Capital, Key Equipment Finance, and CIT rapidly, and in some cases completely, reduced their funding activity in Canada. The merger and acquisition activity that followed the 2008 financial crisis led to Canadian banks acquiring Canadian entities and assets from GE Capital, CIT, and others. Between the years 2000 and 2013, the percentage of Canada's financial industry assets under foreign control dropped from a high of 17% to 12%.[3]

CAUSE FOR CONCERN?

Is there reason to be concerned? The incredible market share of the Big Six is alarming; however, consumers and businesses appear to have sufficient access to capital, and the financial sector was tested in 2008 and passed with flying colors. There would appear to be enough domestic competition in the market to give good access to diverse products, low rates, and sufficient capital. However, a deeper look at the

competitive advantages of the Big Six gives insights into some of the domestic consequences of the different capital requirements of banks operating in Canada and how this limits the ability of small and medium-sized banks to gain meaningful market share.

The Canadian commercial equipment finance market has shown fundamental changes in market share since 2008. There have been well over 30 merger and acquisition transactions.

On the surface, the Canadian banking sector is the envy of the world. Canadian banks were relatively unscathed by the 2008 global credit crisis and the regulatory regime in Canada was praised for keeping the banks strong and stable. The Canadian banks had been operating under domestic regulation that required higher levels of capital than their foreign competitors and higher than levels recommended by the Basel committee on banking supervision. At a time when most banks operating globally were in need of additional capital, the six largest Canadian banks were healthy and had the capacity to grow.

The Big Six banks, like most publicly traded banks, must grow profits and market share to meet their shareholders' expectations. Growth has been achieved organically but also through acquisitions across a range of product lines including deposits, mortgage lending, wealth management, securities dealing, commercial equipment finance, and auto loans. The Big Six have also increased their geographic reach, with expansion to many countries around the world.

The expansion domestically has increased the power of the Big Six to influence the domestic economy dramatically. By 2013 the Office of the Superintendent of Financial Institutions (OSFI) designated the Big Six as domestic systematically important banks (D-SIB). These banks now carried the added risks of international operations, such that if foreign performance impacted the viability of one of the Big Six it would affect the Canadian economy.

The Canadian financial industry, while considered healthy, has become less competitive and is now dominated by a small group of domestic banks with the strength and competitive advantage to dominate any financial sector in Canada. The very systems that keep the banking community healthy have also led to dominance by a small group of Canadian Banks.

GAP IN COMPETITIVE ADVANTAGE

The gap in competitive advantage is well illustrated in the commercial equipment finance sector. A group of smaller Canadian financial institutions have chosen to focus expansion efforts in the commercial equipment finance market. The group includes Laurentian Bank, Canadian Western Bank (CWB), and Meridian OneCap, which are three smaller domestic financial institutions that have made acquisitions and investment in the commercial equipment finance sector over the past several years.

These companies are growing their commercial equipment finance market share significantly, although a deeper understanding of the system of determining risk and capital adequacy reveals some significant competitive hurdles for smaller Canadian financial institutions.

The Canadian commercial equipment finance market has shown fundamental changes in market share since 2008. There have been well over 30 merger and acquisition transactions, with several of the most significant transactions involving banks acquiring the largest and most profitable independents. The consolidation has changed the dynamic of who is fighting for origination and profit in the market.

Most independents of size have been acquired by financial institutions (banks, credit unions), and now the main battle for market share is mainly between foreign and domestic banks with strong liquidity, low cost of capital, and a desire for growth. However, some banks are stronger than others. This article explores the issue of how competition in Canada is impacted by domestic and global banking capital requirements. There is a large discrepancy in the leverage available to different financial institutions, and this gap impacts competition in Canada.

The Basel Committee on Banking Supervision (Basel) is the primary global standard-setter for the prudential regulation of banks and provides a forum for cooperation on banking supervisory matters.[4] Basel is made up of central bank governors from numerous countries who cooperate on bank supervisory matters.

Before and since the financial crisis, Basel has been providing information on the recommended minimum capital requirements for banks operating internationally. These recommendations have evolved over time with the most recent recommendations being derived from lessons learned since 2008. Basel has struggled to maintain a consensus on the best methods to determine risk and whether the same approach for international banks is effective for banks operating only domestically.

RISK RATIOS AND CAPITAL REQUIREMENTS

In Canada, the Big Six gain a significant advantage from regulators because these banks, and only these banks, are allowed to use the advanced internal ratings-based (AIRB) method of determining capital requirements. The other, smaller banks are required to use the standardized rates set forth in Basel, causing the smaller banks to hold significantly more capital.

In addition, the Basel approach deems business loans to have significantly higher risk than residential mortgages and other retail loans. A smaller bank specializing in commercial lending faces a much higher capital requirement. Table 1 shows a comparison of the risk ratings used to calculate capital requirements. The table shows the enormous discrepancy between the capital required by a small bank and the Big Six.

The risk weightings shown above are used to calculate capital that the bank must hold to offset the risk of each type of lending. The weighted amount is then multiplied by the common equity Tier 1 (CET1) ratio established by Basel III. When the Big Six were designated D-SIB, their Tier 1 capital ratios were increased by 1% but the net amount of calculated capital is still much lower than for CWB and Laurentian.

Canadian banks have also had the ability to offload much of the risk of underwriting mortgages onto taxpayers through a unique insurance program. Homebuyers with down payments of less than 20% require insurance. This insurance provides the banks with ironclad government support and is unique to Canada. Mortgages with government insurance are risk weighted "0" for the purposes of calculating capital adequacy.

More than 50% of Canada's $1.4 trillion home loan market is made up of insured home mortgages.[5] The Department of Finance has acknowledged that the level of government insurance protection is too high and is contemplating changes that will transfer a greater portion of the risk back to the banks originating the transactions.

There are multiple issues with the current risk weighting system including concerns about shifts in lending toward lower risk-rated residential mortgages and a movement away from business lending. Table 1 illustrates that current risk weighting gives banks a greater leverage if they pursue residential mortgages and retail loans over commercial lending. The larger banks have been historically connected to retail customers through a network of branches and now a dominant internet presence.

Smaller banks lacking a retail presence often pursue commercial lending because it is more suited to their resources and capabilities. Available data illustrates that the distribution of bank credit to individuals has grown enormously in the residential mortgage sector. Figure 1 illustrates the massive shift by lenders over the past 40 years to a more residential mortgage based portfolio.

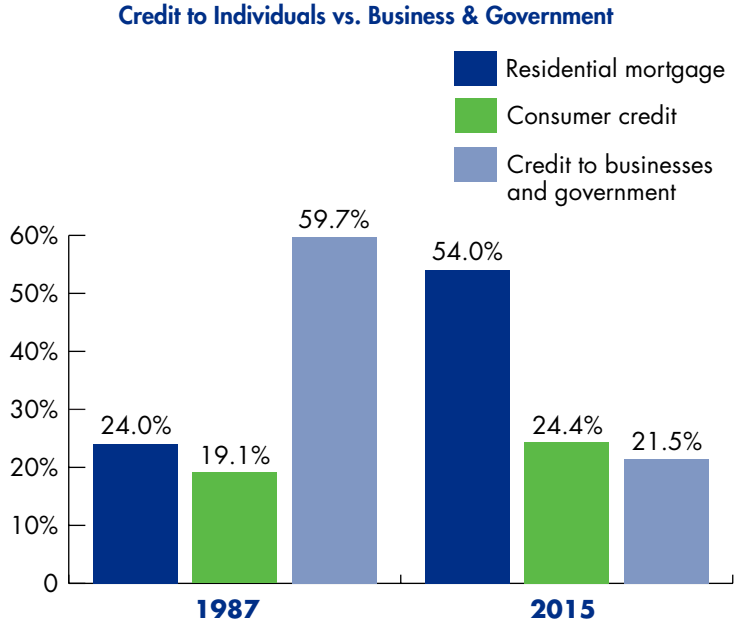
Table 1. Risk Weighting by Category

	Standardized		Advanced internal rating based (AIRB)					
Category	**CWB**	**LB**	**BMO**	**BNS**	**CIBC**	**NB**	**RBC**	**TD**
Residential mortgage	30.4%	17.2%	8.0%	11.3%	6.4%	11.7%	7.5%	8.8%
Other retail loans	76.6%	66.3%	25.2%	41.7%	31.9%	37.9%	22.6%	34.3%
Business loans	99.9%	100.1%	42%	58.1%	35.2%	47.0%	58.4%	44.6%
Avg. equity required	9.2%	8.0%	10.1%	11.0%	11.3%	10.1%	10.8%	10.4%

Note: Category Abbreviations – Canadian Western Bank (CWB), Laurentian Bank (LB), Bank of Montreal (BMO), Bank of Nova Scotia (BNS), Canadian Imperial Bank of Commerce (CIBC), National Bank of Canada (NB), Royal Bank of Canada (RBC), Toronto-Dominion Bank (TD).

Source: CWB Financial Group, corporate presentation, 1st quarter 2017. Used with permission.

Figure 1. Distribution of Bank Credit in Canada



Source: Chris Fowler, Western Bank of Canada. (See endnote 2.)

The Big Six have grown their residential mortgage books with cheap capital and high leverage. They have a substantial advantage over smaller financial institutions in every category of lending.

EXPOSURE FROM RESIDENTIAL MORTGAGES

The shift away from business credit is clear. In recent times, the exposure of the banks to residential mortgages in general and to residential mortgages in certain provinces specifically has been identified as an area of concern for the Office of the Superintendent of Financial Institutions. The Big Six have grown their residential mortgage books with cheap capital and high leverage. They have a substantial advantage over smaller financial institutions in every category of lending. Moreover, the impact of their ability to use the internal ratings-based approach has led to a dramatic shift in lending activity.

Canada has 23 small and medium-sized domestically owned banks that collectively make up 2% of all the assets of all banks in Canada. This is but one example of the many challenges facing those who regulate and monitor the financial services sector in Canada. Although the health of the banking sector is not in doubt, the long-term ramifications of such a concentration of market share continue to be a concern for policy-makers and regulators.

An effective capital regime is intended to provide confidence in the banking system. In theory, the regime dissuades banks from taking riskier credit because these deals will require higher capital. In negative credit cycles, the intention is that effective levels of adequate capital will not require the sale of assets or reduced lending activities when times are tough.

Two smaller Canadian banks have made significant efforts to expand their commercial equipment financing operations. Canadian Western Bank and Laurentian Bank have been actively acquiring equipment finance firms and increasing their originations post-acquisition. The smaller banks have had to stay away from the hypercompetitive residential mortgage space and have pursued commercial lending (including equipment). Their capital requirements for all forms of lending are significantly higher than the Big Six, creating an unlevel playing field in the domestic lending market.

Smaller financial institutions are less profitable because of their higher capital requirements and resulting thinner margins. Table 2 shows a simplified calculation of Tier 1 capital required to offset business loan risk for two smaller financial institutions compared to the average required for the Big Six. The premise of the regulation is to ensure these banks have adequate capital to sustain themselves in periods of economic strain and loan stress.

The impact of the gap in risk weighting is well stated by Chris Fowler, president and CEO of Canadian Western Bank, in his submission for the Consultation Paper on Review of the Federal Financial Sector Framework[6]:

> Non-AIRB banks that specialize in servicing the financial needs of small to medium sized businesses are at a competitive disadvantage in terms of the higher capital that they have to hold relative to the large dominant Canadian Banks. This is because commercial loans represent a higher percentage of their overall portfolio as well as the fact non-AIRB banks currently utilize the standardized method of calculating risk weighted assets and therefore carry more capital compared to AIRB banks for the same credit risk. This limits the ability of smaller banks to focus on the business segment. Notwithstanding the significant impact of capital requirements on competition, products offered and the potential systemic risk associated with federal banks all incentivized to offer the same types of credit, there is no mention in the Consultation Paper of the need to examine the effects of capital requirements on the policy objectives of the Government.

COMPETITION FOR THE BIG SIX

Can domestic financial institutions and foreign financial entities compete with the dominance of the Big Six? The data presented above shows that the six largest Canadian banks have a considerable advantage over their competition. There is no doubt that the advantage is significant and the difference in capital requirements materially impacts the profits of smaller banks. Under the current system of risk weightings, it remains

Table 2. Simplified Tier 1 Capital Calculation

Tier 1 %	Business loan total	Weighted calculation	Weighted loan amount	Tier I capital required
Big Six Avg 10.6%	$100 Million	$100 Million × 47.6%	$47.6 Million	$5.0 Million
CWB 9.2%	$100 Million	$100 Million × 99.9%	$99.9 Million	$9.1 Million
Laurentian 8.0%	$100 Million	$100 Million × 100.1%	$100.1 Million	$8.0 Million

Source: Alta Canada. Derived from CWB Financial Group, corporate presentation, 1st quarter 2017. Used with permission.

more difficult for smaller financial institutions to attract capital and generate comparable return on equity to the Big Six.

For U.S. lessors there are opportunities in Canada in spite of the competitive advantage of the Big Six. Thus, U.S. lessors with strong vendor and manufacturer programs should consider expanding their offerings to include the Canadian market. Many Canadian dealers want the same finance options as their U.S. dealer counterparts but often the U.S. equipment finance firm is not active in Canada.

Entering Canada to support existing relationships would bring additional volume as well as protect from competitors trying to enter the United States by leveraging Canadian relationships. U.S. firms would also find opportunity offering residual based financing where the Big Six banks face some regulatory restrictions.

The Big Six banks have a pricing and leverage advantage, but this does not mean there is not room for U.S. firms with a value proposition that distinguishes themselves from low-priced competitors. Many U.S. firms are thriving in Canada (Wells Fargo, Key Equipment Finance, Bank of America, PNC Bank) and these firms exemplify companies with strong value propositions and mature sales strategies.

Even with the advantages described in this article, the Big Six face stiff competition in the Canadian commercial equipment finance sector. The industry has a diverse group of competitors including captives, foreign banks, and independents in addition to the domestic financial institutions. The Big Six are a presence in the industry and have significant market share, but there does not appear to be a concerted effort to dominate the industry.

Banks and credit unions represent an estimated 70% market share,[7] and the Big Six are estimated to hold 43.6% of the Canadian commercial equipment finance portfolio. The commercial equipment market share of the Big Six is considerably smaller than their overall 93% share of Canadian banking activity including retail and commercial banking, wealth management services, wholesale banking operations, and insurance services.

Although the smaller market share is encouraging, it indicates a market segment that may become a target of the Big Six to add origination. Given the considerable competitive advantages of the Big Six and the historical effort to grow through acquisitions, there is the potential for further industry consolidation.

CONCLUSION

The Canadian banking system, while often praised as among the strongest in the world, has in some ways become a victim of its own success. The six largest banks now represent 93% of banking assets and because of current Basel regulations have an incredible competitive advantage. Canadian governments and financial service regulators acknowledge that the dominance of the Big Six needs to be addressed but have not yet articulated or scheduled clear actions. At the root of the problem is the use of the risk-weighting system recommended by Basel and used, in part, as the basis for bank capital requirement calculations in Canada.

In recent remarks, the superintendent of OSFI, Jeremy Rudin, made it clear that the internal ratings based approach is an area of concern[8]:

> If we turn to the internal ratings based approach, we find that risk weights vary too much across banks. This is seen most clearly when banks using the internal ratings based method are asked to determine the risk weight that they would assign to a common, specific portfolio of assets.

The comments of Mr. Rudin include additional statements that neither the standardized approach used by small and mid-sized banks nor the internal ratings based approach used by the global banks (including the Big Six) is a satisfactory solution[9]:

> The underlying problem in each approach is the mirror image of the problem in the other. In the standardized approach, the problem itself is risk weights that do not vary enough from bank to bank. In the internal ratings based approach, risk weights vary too much from bank to bank.

If it is true that the first step toward finding a solution is identifying the problem, it would appear that Canadian regulators are making some progress. Unfortunately, finding a solution that works for domestic banks, the Big Six, and Basel is complicated and further hampered by a lack of consensus among the 27 jurisdictions represented on the Basel committee. Any solution to risk weightings involves the commercial lending segment, and Basel is struggling to find consensus about how to treat commercial lending in general and equipment finance specifically.

U.S. lessors with strong vendor and manufacturer programs should consider expanding their offerings to include the Canadian market. Many Canadian dealers want the same finance options as their U.S. dealer counterparts but often the U.S. equipment finance firm is not active in Canada.

Trade associations including the Canadian Finance and Leasing Association, Equipment Finance and Leasing Association, and Leaseurope have all made submissions to Basel articulating how default rates for commercial transactions need to reflect lower default rates and accurate risk weights.[10] The efforts of the commercial equipment finance industry associations are only a small example of the challenges faced by Basel at this time.

The concentration of market share is of concern to policymakers in general but the threat to the number and volume of financing choices for small and medium-size enterprises (SMEs) is a serious concern. The Big Six have historically been passive pursuers of SME business and have evolved consumer origination strategies with more priority than SME solutions. SMEs in Canada are looking for more options and would be receptive to additional providers of commercial equipment finance.

The Big Six banks have proven over many decades that they have the ability to dominate any sector of the domestic banking system in Canada including the commercial equipment finance business. The Canadian government has the responsibility to ensure the stability of the domestic banking community, and the performance of the banks during events like the global financial crisis of 2008 shows Canadian measures were among the few that were adequate.

The unintended consequence of Canadian regulatory policy is a concentration of market share in the banking sector that is a threat to competition. The banking system is in good health, but the concentration of assets among the Big Six is cause for concern. The risk weightings used to determine capital adequacy for all Canadian banks do not adequately reflect the risk profile of smaller financial institutions. It appears that the Department of Finance is aware of this issue but has yet to propose a viable solution.

Until the gap in capital requirements between the Big Six and other small and medium-sized domestic banks can be closed, the ability to close the competitive gap between financial institutions will be limited.

Endnotes

1. Department of Finance Canada. Reforming Canada's Financial Services Sector – A Framework for the Future. Ottawa: Government of Canada, 1999. http://publications.gc.ca/collections/Collection/F2-136-1999E.pdf.

2. Department of Finance Canada. Supporting a Strong and Growing Economy: Positioning Canada's Financial Sector for the Future. Ottawa: Government of Canada, 2016. https://www.fin.gc.ca/activty/consult/ssge-sefc-eng.pdf.

3. Ibid.

4. Bank of International Settlements. BIS Quarterly Review, March 2017. https://www.bis.org/publ/qtrpdf/r_qt1703.htm.

5. Department of Finance. Balancing the Distribution of Risk in Canada's Housing Finance System. A Consultation Document on Lender Risk Sharing for Government-Backed Mortgages. Ottawa: Department of Finance Canada, February 2017. https://www.fin.gc.ca/activty/consult/lrs-prp-eng.asp.

6. Chris Fowler, Canadian Western Bank Response to Leverage Issue, Consultation Document for the Review of the Federal Financial Sector Framework. Department of Finance Canada, Nov. 15, 2016. [see endnote 2] https://www.fin.gc.ca/consultresp/ssge-sefc-eng.asp or https://www.fin.gc.ca/consultresp/pdf-ssge-sefc/ssge-sefc-17.pdf.

7. Alta Canada. Data Base of Canadian Industry Players. Winnipeg, Manitoba: The Alta Group, August 2017.

8. Jeremy Rudin, "Waiting for Basel? Next Steps for Canada's Bank Capital Regime" (remarks to the C.D. Howe Institute, Toronto, Ontario. April 6, 2017). http://www.osfi-bsif.gc.ca/Eng/osfi-bsif/med/sp-ds/Pages/jr20170406.aspx.

9. Ibid.

10. (Canadian Finance and Leasing Association, 2015), (Equipment Leasing and Finance Association, 2015) (Leaseurope, 2015).

Hugh Swandel

hswandel@thealtagroup.com

Based in Winnipeg, Manitoba, Hugh Swandel is the senior managing director of The Alta Group in Canada. He has assisted many equipment leasing and asset finance firms in market entry, due diligence, funding, and strategic planning. Moreover, he has a strong reputation as an effective negotiator with regard to mergers and acquisitions, business development, market entry, securitization, and other areas of importance to lessors. Prior to founding his consulting firm, Swandel and Associates, in 2001, Mr. Swandel served as president and CEO of Electric Financial Group. During the global credit crisis, he was retained by the Canadian Finance & Leasing Association (CFLA) to provide insight into the effects on independent finance companies. He presented his findings to advisors of the Canadian minister of finance and contributed to policy development discussions with government and industry representatives. In both 2006 and 2010, Mr. Swandel received the Canadian leasing industry's highest honor when he was named CFLA Member of the Year. He serves on the board of CFLA, is past president of the National Equipment Financing Association, and is a member of the Equipment Leasing and Finance Association (ELFA). The Fall 2016 issue of this journal published his article titled "M&A Has Rapidly Changed the Canadian Commercial Equipment Finance Marketplace." Mr. Swandel received a bachelor of arts degree with honors and distinction from the University of Winnipeg in Manitoba and also holds a bachelor of commerce degree with honors from the University of Manitoba in Winnipeg.

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 worldwide[1] — 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 statutes 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 Horizon 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 *$1.1 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 securities[13]) 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 information[22] 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 companies[35] 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 security 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* Vindu 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-infants-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

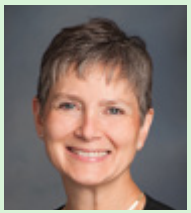
fperetore@csglaw.com

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

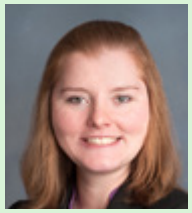
Robert L. Hornby is co-chair of Chiesa Shahinian & Giantomasi's Equipment Leasing and Financing Group. An experienced litigator, he represents national and regional banks and finance companies in all aspects of equipment leasing, asset based lending, and civil litigation in New York and New Jersey state 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.