Cybersecurity compliance and privacy remain top priorities for financial service providers, regulators, and consumers who are at-risk. According to the 2019 Cost of a Data Breach Report, a study conducted by the Ponemon Institute and sponsored by IBM Security, “institutions are nearly one-third more likely to experience a data breach in the next two years than they were in 2014.”¹ This data point highlights the increasing number of circumstances under which an institution may experience a data breach, especially under the prominent threat of malicious individuals or groups scanning the internet and attacking vulnerable systems. Equifax Inc.’s (Equifax) internal investigation of its 2017 data breach, for example, identified four major factors: identification, detection, segmenting of access to databases, and data governance, that allowed attacker(s) to exploit the vulnerabilities in its system, impacting 147 million consumers and representing one of the worst data breaches in scope and size, resulting in the largest-ever data breach settlement with regulatory agencies. Specifically, Equifax’s global settlement with the U.S. Consumer Financial Protection Bureau (CFPB), U.S. Federal Trade Commission (FTC), 48 states, the District of Columbia and Puerto Rico, provides up to $700 million in monetary relief and penalties for its failure to secure its network.²

Notably, in the wake of the Equifax Data Breach Settlement, CFPB Director Kathleen L. Kraninger stated that “[t]he incident at Equifax underscores the evolving cybersecurity threats confronting both private and government computer systems and actions they must take to shield the personal information of consumers. Too much is at stake for the financial security of the American people to make these protections anything less than a top priority.”³ The prevalence of data breaches has become the new norm which is further evidenced by the two recent cybersecurity incidents announced within a week of Equifax’s settlement with federal and state agencies. On July 29, 2019, Capital One Financial

¹ See https://www.ibm.com/security.
² The proposed settlement allocates $425 million to consumers for credit monitoring services and varying factors for redress, $175 million to 48 states, the District of Columbia and Puerto Rico, and a $100 million civil money penalty to the CFPB.
Corporation (Capital One) announced that the personal information of more than 100 million individuals in the United States and approximately 6 million in Canada, respectively, was compromised by an outside individual who obtained personal information relating to Capital One’s existing credit card customers and applicants. The U.S. Federal Bureau of Investigation detained the suspected hacker who formerly worked for Amazon Web Services, a third party vendor, which hosted Capital One’s breached database. Additionally, the Los Angeles Police Department experienced a data breach of its city-owned computers, exposing the personal information of approximately 2,500 officers and 17,500 officer-applicants which underscores the vulnerabilities shared by both private company and government computer systems alike.

The repercussions and rising costs associated with data breaches are substantial, especially in the absence of an effective compliance management system, ongoing preventative measures, or the implementation of relevant industry standards (e.g., National Institute of Standards and Technology, Payment Card Industry Data Security Standard, European Telecommunications Standards Institute’s Cybersecurity Technology Committee, Cybersecurity Evaluation Tool, etc.). According to the 2019 Cost of a Data Breach Report, “the average cost of a data breach in the United States, excluding mega breaches, increased from $7.91 million in 2018 to $8.19 million in 2019,” which is the highest cost globally. The Ponemon Institute identified four process-related activities that drive costs associated with the breach of an entity’s network: detection and escalation, notification, post-data breach response, and lost business. For example, Capital One’s press release outlined these various costs in its projected losses of $100 million to $150 million in expenses related to the Amazon Web Services database breach, which likely includes notifications to consumers and regulators, credit report monitoring and identity protection services, technology improvements, and litigation and liability exposure.

In January 2018, the Consumer Financial Services Committee’s (CFSC) Compliance Management and Privacy and Data Security subcommittees, respectively, presented a joint continuing legal education panel titled “Cybersecurity Compliance and Data Breach Response in Light of the Equifax Breach and Evolving Regulatory Landscape.” The panel discussed, inter alia, industry best practices for cybersecurity compliance and data breach response programs. Two key elements of an effective data breach response program were identified as early detection and preventative measures which, if taken in tandem, help to reduce the cumulative costs that span the lifecycle of a data breach. To illustrate, the Ponemon Institute found that “institutions that employed incident response teams

---

4 See https://www.ibm.com/security.
5 Id.
successfully reduced their costs by conducting extensive testing of their institutional incident response plans, which helped realize a total data breach cost that was $1.23 million less than those entities who neither had an incident response team nor actively tested their incident response plan.” Consequently, many chief executive officers (CEO) continue to elevate the visibility of cybersecurity risk management programs in their institutions and annual strategic planning to include larger budgets, implementation of industry standards and best practices, and recruitment of experienced staff. For example, Jamie Dimon, Chairman and CEO of JPMorgan Chase & Co. (JPMC), once stated that JPMC spends nearly $600 million a year on data security, which could be surpassed by the Bank of America Corporation whose Chairman and CEO, Brian Moynihan, once said that his bank employs a cybersecurity program without budget constraints.

History suggests that financial institutions will remain a primary target for malicious cyberattacks and, as such, will continue to endure regulatory scrutiny to ensure that executive management effectively use their resources to enhance internal controls governing data security. FTC Chairman, Joe Simons, rightfully stated that companies who profit from personal information have a heightened responsibility to protect and secure that data, and the Equifax Data Breach Settlement is a clear indication that financial regulators will have zero tolerance for negligent security standards.

---

7 See https://www.ibm.com/security.