Client Advisory | *April 2011*

Massachusetts Attorney General Breaking New Ground in Data Security Enforcement?

The Massachusetts Attorney General appears to have broken new ground with a recent enforcement action and fine against Briar Group, LLC, a restaurant chain that sustained a security breach exposing credit and debit card data. The papers filed in the case, and a related press release, shed light on the posture taken by the Massachusetts Attorney General in the enforcement of data security obligations, including the use of an alleged failure to comply with the Payment Card Industry Data Security Standards ("PCI-DSS") as a basis for an enforcement action alleging consumer fraud. The fine levied in the amount of $110,000 and the continuing obligations imposed represent significant sanctions that may be faced by companies with personal information of Massachusetts residents that allegedly is not adequately protected against breach incidents.

History of the case

Briar Group operates restaurant chains with several locations in Massachusetts and elsewhere. The complaint alleged that computer systems used by Briar Group to process credit and debit card transactions for its restaurants were infected by malware that intercepted card data as it was submitted for payment at the various restaurant locations, and transmitted the data to a data thief. Briar Group was allegedly informed of a potential data breach by card processors on October 29, 2009. According to the complaint, a forensics investigator was not engaged until three weeks later and the malware was not removed until December 10, 2009. During this period, Briar Group's restaurants continued to accept credit and debit cards, even though Briar Group allegedly knew or had reason know that its security had been breached and that the cards of its customers continued to be vulnerable to theft. Ultimately, over 125,000 credit and debit cards were allegedly affected by the breach.

The grounds of the Massachusetts AG as set forth in its complaint and the consent judgment entered included Briar's alleged failure (i) to change default passwords, (ii) to change passwords for more than five years, (iii) to control sharing of login credentials among employees, (iv) to change passwords after termination or resignation of employees, (v) to adequately control the number of employees with administrative access to the computer network, (vi) to properly secure remote access utilities and wireless network, (vii) to alert patrons to the data breach while continuing to accept cards from consumers after it had knowledge of the data breach and before remediation steps were taken, (viii) to store payment information securely rather than in clear text, and (ix) to satisfy the requirements of PCI-DSS.

The Massachusetts AG took the position that these purported failures, notably including the lack of PCI-DSS compliance, contributed to the breach. According to Count I of the Complaint, Briar Group engaged in unfair or deceptive acts or practices in violation of the Massachusetts consumer protection statute, MGLA c. 93A, by accepting credit and debit cards from consumers while failing to take reasonable steps to protect the personal information obtained from its patrons. It should be noted that the relevant incident(s) occurred prior to the March 1, 2010 effective date of the Massachusetts data security regulation (201 CMR 17.00). Therefore, the Massachusetts AG did not include an allegation or count related to a breach of the technical requirements and safeguards currently in effect in Massachusetts. The judgment, however, did include the on-going requirement to comply with the Massachusetts data security regulation, a future violation of which would presumably also constitute violation of the judgment.

Status of PCI-DSS as a legal standard

PCI-DSS is a demanding set of industry standards imposed through contracts by card brands and acquiring and merchant banks on merchants and others accepting credit cards, subject to amendment and revision from time to time. Most U.S. jurisdictions including Massachusetts have not incorporated PCI-DSS into their statutes or regulations. Very few, like Nevada, Minnesota and Washington State have codified PCI-DSS obligations and, to varying degrees, made it part of the standard under their data security laws. Various levels of PCI compliance are determined by the annual number of electronic card transactions handled by the merchant. The Briar Group case was settled by a consent judgment, and thus there is no judicial opinion in that case that can be relied upon as a precedent.

No court has yet authoritatively determined whether a violation of PCI-DSS constitutes evidence of consumer fraud in Massachusetts. Two cases applying Massachusetts law to data breach incidents in a slightly different context may offer some guidance. The two cases involve lawsuits brought by credit unions and banks that issued credit cards against merchants that suffered data breach incidents, and the decisions suggest that in that context it would be quite difficult, but not

impossible, to sustain a misrepresentation or related c. 93A claim based on a violation of PCI-DSS. In *CUMIS Ins. Soc. Inc. v. BJ's Wholesale Club, Inc.*, 455 Mass. 458, 918 N.E.2d 36 (2009), the Supreme Judicial Court of Massachusetts held that a retailer's violation of operating regulations of major credit card brands could not form the basis for misrepresentation and fraud claims under Massachusetts law where the plaintiff institutions did not allege that the retailer made any direct representations to them regarding the operating regulations. Following the *CUMIS* decision, the United States Court of Appeals for the First Circuit vacated a lower court's dismissal of a misrepresentation claim that was based in part on a retailer's violation of PCI-DSS, because the claim was "facially valid" as written (i.e., it contained all the necessary allegations). Citing *CUMIS*, however, the Court expressed skepticism that the misrepresentation claim would survive an eventual motion for summary judgment. *In re TJX Companies Retail Security Breach Litigation*, 564 F.3d 489 (1st Cir. 2009).

The Briar Group enforcement action may nevertheless have broad implications and telegraph the posture of the Massachusetts Attorney General in future data breach cases. It may also be a harbinger of similar actions pursued in other jurisdictions on like grounds. Were such an enforcement position to prevail in the future, PCI-DSS arguably may become a *de facto* legal standard, without any substantive or technical review or involvement by any legislature or governmental agency, and enforced by attorneys general pursuant to their authority under general consumer fraud statutes. Given the complexity and difficulty of full compliance with PCI-DSS, this would present a major challenge for many merchants. As an evolving industry standard that depends on the merchant level, asserting PCI-DSS deficiencies as a legal basis for claims may prove problematic for regulators.

Timely Forensic Intervention

Another lesson to be learned from the Briar Group case, even for businesses in general compliance with PCI-DSS, is the emphasis the Massachusetts AG placed on delays alleged in the reaction time of the affected merchant. The complaint asserted a delay in engaging outside forensics investigation; a delay in time between the commencement of the forensic investigation and the deletion of the malware causing the breach; and the delay in time between the company's learning of a breach and the remediation of the breach, all while it continued to accept additional cards from consumers, subjecting them to the allegedly on-going vulnerability. Given the limited amount disclosed, it is not clear what precautions the Briar Group undertook, and they may well be more robust than alleged. Other enforcement actions (e.g., the action against HealthNet by the Connecticut AG) have also emphasized the importance of reacting promptly.

Conclusion

Based on Briar Group and other enforcement actions, a company involved in a potential data breach incident will be expected to react promptly by undertaking the necessary computer forensics, and by eliminating or curtailing the identified or relevant vulnerabilities. Doing so will markedly reduce the risk of fines, sanctions or claims, and bolster defenses of the merchant. Failure or delay in doing so may expose a company to a higher degree of regulatory scrutiny, and potentially higher fine levels and other sanctions.

Boston ma | Ft. Lauderdale fl | Hartford ct | Madison nj | New York ny | Newport Beach ca | Providence ri
Stamford ct | Washington dc | West Palm Beach fl | London uk | Hong Kong (associated office)

Mark E. Schreiber, Partner, Chair - Privacy and Data Protection Group	+1 617 239 0585	mschreiber@eapdlaw.com
Theodore Augustinos, Partner, Co-chair - Privacy and Data Protection Group	+1 860 541 7710	taugustinos@eapdlaw.com
Laurie A. Kamaiko, Partner, Co-chair - Privacy and Data Protection Group	+1 212 912 2768	lkamaiko@eapdlaw.com
Barry J. Bendes, Partner	+1 212 912 2911	bbendes@eapdlaw.com
Nicholas Bolter, Partner	+44 (0) 20 7556 4380	nbolter@eapdlaw.com
Kenneth Choy, Partner	+852 2116 6653	kchoy@eapdlaw.com
Ben Goodger, Partner	+44 (0) 20 7556 4188	bgoodger@eapdlaw.com
Peter C. Schechter, Partner	+1 212 912 2934	pschechter@eapdlaw.com
David S. Szabo, Partner	+1 617 239 0414	dszabo@eapdlaw.com
Patrick J. Concannon, Counsel	+1 617 239 0419	pconcannon@eapdlaw.com
Eric D. Fader, Counsel	+1 212 912 2724	efader@eapdlaw.com
Brian J. Green, Counsel	+1 212 912 2755	bgreen@eapdlaw.com
James D. Gustafson, Counsel	+1 949 423 2118	jgustafson@eapdlaw.com
Karen L. Booth, Associate	+1 860 541 7714	kbooth@eapdlaw.com
Mia H. Finsness, Associate	+1 212 912 2927	mfinsness@eapdlaw.com
Joseph R. Geoghegan, Associate	+1 860 541 7749	jgeoghegan@eapdlaw.com
Theo C. Godfrey, Associate	+44 (0) 20 7556 4176	tgodfrey@eapdlaw.com
Brian R. Landry, Associate	+1 617 239 0150	blandry@eapdlaw.com
Socheth Sor, Associate	+1 860 541 7773	ssor@eapdlaw.com