Clients&FriendsMemo

# States Respond to Equifax Cyber Breach with Enforcement Actions and Calls for Enhanced Regulatory Powers

**October 13, 2017**

In the wake of last month's historic cyber breach of Equifax, which resulted in the theft of sensitive personal information belonging to over 140 million Americans,[1] states have wasted no time in seeking a greater role in regulating cybersecurity risk. Historically, while state consumer agencies and attorneys general have enforced notification requirements for victims of cyberattacks where consumer data was compromised, significant enforcement actions have been the purview of federal agencies such as the Federal Trade Commission, the U.S. Department of Justice, the Securities and Exchange Commission, and the Commodity Futures Trading Commission. However, given the scope of recent breaches and the sensitivity of the information that was stolen, states have recently stepped up and launched their own investigations and enforcement actions, and have imposed new data protection standards on various types of businesses. Assuming this trend continues, organizations responsible for defending against cyberattacks, or who find themselves the victim of a successful hack, may find themselves with both federal and state cyber regulators to deal with.

## I. Massachusetts Brings the First Enforcement Action

Since the announcement of its data breach, on September 7, 2017, Equifax has faced a barrage of criticism from regulators, litigants, and Congress on its failure to adequately secure its information systems against attack, as well as its multi-week delay in disclosing the breach to consumers and the investing public. On September 19, 2017, the Commonwealth of Massachusetts took this criticism a step further and filed a civil action against Equifax for failing to adequately protect consumer data and for other related violations.[2]

---

1 *See* Cadwalader Clients & Friends Memo, *Equifax Data Breach Highlights SEC Disclosure Obligations for Public Companies in the Wake of Cybersecurity Attacks* (Sep. 18, 2017), http://www.cadwalader.com/resources/clients-friends-memos/equifax-data-breach-highlights-sec-disclosure-obligations-for-public-companies-in-the-wake-of-cybersecurity-attacks.

2 *See* Press Release, *AG Healey Sues Equifax* (Sep. 19, 2017), http://www.mass.gov/ago/news-and-updates/press-releases/2017/2017-09-19-equifax-lawsuit.html.

In the complaint filed by Massachusetts Attorney General Maura Healey, Equifax is alleged to have (i) failed to adopt appropriate safeguards of customer data, as required by Massachusetts regulations regarding data security; (ii) failed to provide timely notice of the data breach to the state and to affected consumers, as required by the state's data breach notification law; and (iii) engaged in unfair and deceptive trade practices based on, among other things, the company's failure to abide by its own promises to consumers regarding its data security policies and procedures, in violation of the state's consumer protection law.[3]

The Massachusetts action focuses on Equifax's alleged failure to implement the widely-available security patch to the Adobe Struts application, which is believed to have contributed to the vulnerability. Specifically, the complaint alleges that, in early March 2017, the developers of the Adobe Struts application as well as cybersecurity watchdog groups notified the public of a severe vulnerability in the application that would leave systems using it vulnerable to hacking. Notwithstanding this notice, Equifax allegedly failed to implement an available security patch to the application, which was released in early March 2017. Equifax's system was reportedly first breached two months later, in May 2017, by hackers who took advantage of the Adobe Struts vulnerability. Equifax did not detect the breach until late July 2017. The lawsuit further alleges that Equifax faltered in its response to the breach by failing to ensure that adequate call center staffing and online resources were available to answer questions from affected consumers, and by improperly seeking to make a profit from consumers by charging for certain credit protection services beyond a one-year period.

According to AG Healey, customers have experienced and will continue to experience significant financial losses, lost time, and aggravation as a result of Equifax's alleged misconduct. The State of Massachusetts is seeking injunctive relief, civil penalties, restitution and legal costs.

## II. Multiple States Launch Investigations and Demand Information

In addition to the Massachusetts lawsuit, attorneys general in New York, Illinois, California, and in other states announced investigations of Equifax, with AG Schneiderman of New York declaring the purpose was getting to "the bottom of how and why this massive hack occurred."[4]

---

[3] *See* Complaint, *Massachusetts v. Equifax, Inc.* (Suffolk Cty. Super. Ct., Sept. 19, 2017), http://www.mass.gov/ago/docs/press/2017/equifax-complaint.pdf.

[4] *See* Press Release, *A.G. Schneiderman Launches Formal Investigation Into Equifax Breach, Issues Consumer Alert* (Sep. 8, 2017), https://ag.ny.gov/press-release/ag-schneiderman-launches-formal-investigation-equifax-breach-issues-consumer-alert; *see also* Press Release, *Attorney General Madigan Investigating Massive Equifax Data Breach & Urges Illinois Residents to Be Vigilant* (Sep. 8, 2017), http://www.illinoisattorneygeneral.gov/pressroom/2017_09/20170908.html; Press Release, *Attorney General Becerra Issues Consumer Alert Following Equifax Data Breach* (Sep. 10, 2017), https://www.oag.ca.gov/news/press-releases/attorney-general-becerra-issues-consumer-alert-following-equifax-data-breach.

States have a variety of tools at their disposal to investigate and penalize companies for data breaches. For example, most states in addition to the District of Columbia and certain U.S. territories have data breach notification laws that generally require prompt notification to consumers and/or state regulators of data breaches that affect the personal information of those states' residents. These notification laws typically allow state attorneys general to bring enforcement actions for non-compliance.

In New York, for example, the attorney general may seek to recover any consequential damages suffered by consumers who were entitled to notice but were not notified, as well as a fine of up to $150,000 if the failure to provide notice was knowing or reckless.[5] A smaller number of states have laws that expressly require companies to adopt certain cybersecurity measures to protect the personal data of their residents. In New Mexico, for example, companies that fail to adopt "reasonable security procedures and practices" may be sued by the attorney general for actual damages caused by a company's failure to maintain such safeguards as well as receive a fine of up to $150,000 for knowing or reckless violations.[6] Finally, some states rely on pre-existing consumer protection laws, which usually prohibit deceptive or unfair trade practices, to pursue companies for damages, penalties, and injunctive relief for either (i) failing to adopt appropriate safeguards for consumer data or (ii) misleading customers about the existence or strength of the company's cybersecurity safeguards.

Further, on September 19, 2017, the attorneys general and consumer protection regulators from over forty states signed a letter to Equifax that expressed "profound concerns" regarding the breach, primarily concerning the rollout of Equifax's consumer notice of the data breach and offer of free credit monitoring to consumers.[7] These concerns include (i) language that initially appeared in the terms of service that required customers to agree to an arbitration clause and class action waiver as a condition of accepting the free credit monitoring;[8] (ii) Equifax's marketing of fee-based identity protection services alongside its offer of free identity protection services, which could potentially deceive consumers into selecting the fee-based service; and (iii) Equifax's failure to provide sufficient call center support and internet resources, such that consumers reported being unable to obtain additional information regarding the breach.

---

5 *See* N.Y. GBS § 899-aa.6(a), https://www.nysenate.gov/legislation/laws/GBS/899-AA.

6 *See* N.M. Stat. Ann. §§ 57-12C-4, 57-12C-11.

7 *See* Letter from State Attorneys General to Equifax (Sep. 19, 2017), http://www.michigan.gov/documents/ag/Equifax.Letter+to+Counsel.9-15-17_600904_7.pdf.

8 Equifax ultimately removed the arbitration language and declared that it would not seek to compel any consumers into arbitration. *See* https://www.equifaxsecurity2017.com/2017/09/13/progress-update-consumers-4/.

These same state attorneys general have also turned their attention to Experian and TransUnion, the other two major credit reporting agencies.[9] Although there is no evidence that these other credit reporting agencies were affected by the Equifax breach, on October 10, 2017, the state attorneys general demanded that the other credit agencies voluntarily waive the fees they charge consumers – often $10 – to impose or lift credit freezes, noting (i) that consumers must seek credit freezes from all three credit reporting agencies in order to fully protect themselves from the Equifax breach and (ii) that it is inappropriate for these credit agencies to impose fees for credit freezes, given that consumers do not voluntarily choose to do business with credit reporting agencies.

## III. New York Calls for Expanded Regulatory Powers

New York's Attorney General and Governor have also used the Equifax breach as an opportunity to impose new and tougher cybersecurity standards on credit agencies such as Equifax as well as any business that handles the private information of New York residents.

### A. Renewed Call for Passage of New York Data Security Act

On September 15, 2017, AG Schneiderman wrote in an op-ed article that he was renewing his call for the passage of the New York Data Security Act, which would require New York businesses to implement and maintain data security programs.[10] AG Schneiderman had previously proposed the legislation in January 2015,[11] but it failed to gain traction. If enacted, the law would implement the following cyber-related provisions.[12]

- *Data Security Standards and Programs*. Any entity that does business in New York and maintains certain private information regarding New York residents would be required to develop, implement and maintain "reasonable safeguards" to protect the confidentiality of that information. Entities would also be required to implement an information security program that includes: (i) administrative safeguards, such as conducting risk assessments and training employees; (ii) technical safeguards, such as assessing risks in network and software design; and (iii) physical safeguards, such as protecting against unauthorized access to private information during collection, transportation, destruction, and disposal.

---

[9] *See* Press Release, *Attorney General Madigan Calls on Credit Bureaus to Halt Fees for Consumers Impacted by Massive Equifax Breach* (Oct. 10, 2017), http://www.illinoisattorneygeneral.gov/pressroom/2017_10/20171010b.html.

[10] *See* Eric Schneiderman, "Raising our guard vs. mega-breaches," *N.Y. Daily News* (Sep. 15, 2017), http://www.nydailynews.com/opinion/raising-guard-mega-breaches-article-1.3496434.

[11] *See* Press Release, *N.Y. State Office of the Attorney Gen., A.G. Schneiderman Proposes Bill To Strengthen Data Security Laws, Protect Consumers From Growing Threat Of Data Breaches* (Jan. 15, 2015), https://ag.ny.gov/press-release/ag-schneiderman-proposes-bill-strengthen-data-security-laws-protect-consumers-growing.

[12] *See* Data Security Act, Assembly Bill 6866 (2015-2016 Regular Session), http://nyassembly.gov/leg/?default_fld=&leg_video=&bn=A06866&term=2015&Summary=Y&Actions=Y&Committee%26nbspVotes=Y&Floor%26nbspVotes=Y&Memo=Y&Text=Y.

- *Broad Definition of Private Information*. The definition of private information would be expanded beyond standard forms of personal information, such as social security numbers, to also cover biometric information, unsecured protected health information, and a username or email address in combination with a password or security question and answer that would permit access to an online account.
- *Safe Harbor and Law Enforcement Sharing*. To encourage compliance with the new standards, a rebuttable presumption of compliance would be provided if an entity's cybersecurity program is certified annually by an independent third party auditor. The legislation would also offer immunity from liability in a civil action, including an action brought by the attorney general, for entities that comply with certain information security guidelines published by the National Institute of Standards and Technology. In addition, the bill would incentivize companies to share information about data breaches with law enforcement by establishing that the production of forensic reports to local and state law enforcement agencies for the purpose of investigating a breach is not a waiver of any privilege or protection, such as the work product doctrine or trade secret protection.
- *Penalties and Enforcement*. The New York Attorney General would be empowered enjoin violations and seek civil penalties of $250 for each person whose private information was compromised, up to a maximum of $10 million per breach. For violations found to be knowing or reckless, these amounts increase to $1,000 for each affected person, up to the greater of $50 million or three times the aggregate amount of any actual costs and losses.

**B. Proposed Oversight of Credit Reporting Agencies**

On September 18, 2017, Governor Cuomo directed the New York Department of Financial Services ("DFS") to implement new regulations that would expand the jurisdiction of the DFS, which regulates financial services firms and insurance companies, to include credit reporting agencies, such as Equifax, that collect data on consumers in New York.[13] The proposal would mandate that credit reporting agencies not only register with the DFS but also comply with the DFS's "first-in-the-nation" cybersecurity rules.[14]

Under the proposal, credit reporting agencies that collect information on consumers in New York would be required to register with the DFS and would be subject to DFS's cybersecurity rules. The credit reporting agencies would also be subject to ongoing DFS examinations and investigations to evaluate compliance. Should a credit reporting agency or its officers fall out of compliance, or

[13] *See* Press Release, *Governor Cuomo Announces New Actions to Protect New Yorkers' Personal Information in Wake of Equifax Security Breach* (Sep. 18, 2017), https://www.governor.ny.gov/news/governor-cuomo-announces-new-actions-protect-new-yorkers-personal-information-wake-equifax.

[14] Cadwalader attorneys have written several memoranda on DFS's new cybersecurity rules, most recently on September 12, 2017. *See* Cadwalader Clients & Friends Memo, *Compliance with Initial New York DFS Cybersecurity Rules Now Mandatory* (Sep. 12, 2017), http://www.cadwalader.com/resources/clients-friends-memos/compliance-with-initial-new-york-dfs-cybersecurity-rules-now-mandatory.

otherwise appear to be "not trustworthy and competent to act as or in connection with a consumer credit reporting agency," the DFS could suspend or revoke the credit reporting agency's registration and thereby prohibit the firm from doing business with consumers and certain financial institutions in New York.

Under the proposal, consumer credit reporting agencies would be required to register with the DFS by February 1, 2018, and would have a phased period to comply fully with the cybersecurity regulations by October 4, 2019.

## IV. Conclusion

Even before the Equifax breach, states had begun taking an increasingly active role in penalizing companies that failed to safeguard consumer information.[15] However, the scope of the Equifax breach is likely the tipping point that will call states to more muscular action, including more aggressive statutes, compliance examinations, and enforcement actions. As a result, businesses must be increasingly mindful of not just federal data protection standards and rules, but of increasingly strict state rules as well. Businesses that possess sensitive data that cybercriminals might seek to exploit would do well to regularly revisit their cybersecurity controls, policies, and procedures to ensure that they comply with all applicable laws.

* * * *

Please feel free to contact any of the following Cadwalader attorneys if you have any questions about this memorandum.


| | | |
|---|---|---|
| Joseph Moreno | +1 202 862-2262 | joseph.moreno@cwt.com |
| Joseph Facciponti | +1 212 504-6313 | joseph.facciponti@cwt.com |
| Peter Carey | +1 202 862-2339 | peter.carey@cwt.com |


[15] For example, in May 2017, Target agreed to pay $18.5 million to resolve claims by 47 states and the District of Columbia arising from a 2013 data breach involving the theft of 40 million payment card records from Target's computer network. *See* S. Ramakrishnan and N. Bose, *Target in $18.5 million multi-state settlement over data breach*, Reuters (May 23, 2017), https://www.reuters.com/article/us-target-cyber-settlement/target-in-18-5-million-multi-state-settlement-over-data-breach-idUSKBN18J2GH. In August 2017, Nationwide Mutual Insurance entered into a $5.5 million settlement with 32 states concerning a 2012 data breach that compromised personal information for over one million customers. *See* Press Release, *A.G. Schneiderman Announces $5.5 Million Multi-State Settlement With Nationwide Mutual Insurance Company Over 2012 Data Breach* (Aug. 9, 2017), https://ag.ny.gov/press-release/ag-schneiderman-announces-55-million-multi-state-settlement-nationwide-mutual.