New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 258—NO. 51
WEDNESDAY, SEPTEMBER 13, 2017

Outside Counsel

Expert Analysis

The Equifax Breach: Why This One Is Different

By **F. Paul Greene**

On Sept. 7, 2017, the credit reporting agency Equifax reported a data breach affecting approximately 143 million U.S. consumers. Among the personally identifiable information (PII) that was compromised was name, date of birth, address, and Social Security number. For some affected individuals, driver's license number and credit card number were also compromised.

This is not the first time that a credit reporting agency has been breached, nor is it the first time that Equifax has reported a breach, with its payroll subsidiary TALX experiencing a breach concerning its online portal earlier this year. What is different with the current breach is its size and the nature of information compromised, as well as the implications of the breach in light of the increasingly complex web of cybersecurity regulations governing businesses and other organizations nationwide.

The Equifax breach affected nearly half of all Americans, and over half of those over 18 years of age. It also involved the "holy trinity" of PII: name, date of birth, and Social Security number. These data elements form the core of how many organizations verify identity, whether of their employees or customers. Add to that address and driver's license number, which were also compromised for some or all of the affected individuals, and the potential for widespread identify theft increases exponentially.

Although this has an immediate and direct effect on the individuals whose PII was compromised, the effect on the organizations that employ or serve these individuals is more indirect, and nuanced. At a minimum, the compromise of such a large amount of highly sensitive PII for such a large portion of the U.S. adult population should cause organizations large and small to consider whether this breach has increased their own risk in any material fashion.

Against this backdrop, questions abound, but answers are not always clear.

Do I Need to Notify Customers?

Currently, 48 states have enacted data breach notification laws, all of which focus on data that an organization has in its possession or otherwise owns or licenses. Equifax has stated that it has found no evidence that its core consumer credit reporting database was compromised, so it appears that information provided to Equifax from financial institutions in the credit reporting process may not have been compromised. It remains to

F. PAUL GREENE *is a partner and chair of the privacy and data security practice group at Harter Secrest & Emery. He can be reached at fgreene@hselaw.com.*

be seen, however, exactly where the PII for the approximately 143 million affected U.S. consumers came from. Depending on the legal relationship of Equifax to the compromised PII, entities that provided information to Equifax that was in turn compromised in the breach could have a reporting duty.

Specifically, under the New York data breach reporting statute, N.Y. Gen. Bus. Law §899-aa, any business that "maintains" PII for another entity that "owns" or "licenses" that PII must report a breach to the entity that owns or licenses the PII "immediately following discovery." Any owner or licensor of that PII would then have to notify the individuals affected by the breach. See N.Y. Gen. Bus. Law §899-aa(2).

> Certainly, the Equifax breach begs the question of whether "reasonably equivalent" controls chosen instead of multi-factor authentication can still be considered "reasonably equivalent."

Given that Equifax reported its breach over a month after discovery, it is unlikely that it considers that it was "maintaining" the compromised PII for any New York business. Further, Equifax has disclosed that it has sent notice to all state attorneys general concerning the breach, further underscoring that Equifax was likely the owner or licensor of the PII at issue.

In such a scenario, under New York law, an organization that was not breached but whose customers were affected by the breach would not have an independent reporting duty. At a minimum, however, organizations that provide PII to Equifax should conduct an analysis as to whether any reporting duty applies.

The Role of the Risk Assessment

In the arena of cybersecurity regulation, a baseline cyber risk assessment has become central to many compliance programs. Whether as required under the HIPAA Security Rule (45 C.F.R. §164.308), the Gramm-Leach-Bliley Act (e.g., 12 C.F.R. §364), Massachusetts law (201 CMR 17.03) or the newly in-force cybersecurity regulations from the New York State Department of Financial Services (23 N.Y.C.R.R. Part 500), a risk assessment is both key to establishing appropriate security controls and a living document that must be able to react to events such as the Equifax breach.

Case in point, the requirement under the implementing regulations of the Gramm-Leach-Bliley Act that financial institutions "identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information … and assess the sufficiency of any safeguards in place to control these risks." See 16 C.F.R. §314.4(b). This is a required element in the financial institution's "comprehensive information security program that is maintained in writing," commonly known as a "Written Information Security Program," or "WISP."

Such a risk assessment is not a rote exercise or static document, however. A financial institution subject to the Gramm-Leach-Bliley Act must "[e]valuate and adjust" its WISP "in light of … circumstances that [the financial institution knows] or [has] reason to know may have a material impact on [its] information security program." See 16 C.F.R. §314.4(e).

In light of the Equifax breach, a financial institution covered by the Gramm-Leach-Bliley Act must at least consider whether the breach might have a "material impact on [its] information security program." Such an impact may be present in the fact that core PII elements for so many U.S. adults have been compromised, taken together with the fact that these core elements can be easily correlated with other PII elements, such as email address or mother's maiden name, via open source information or by way of dark-web data analytic services, which vet and enhance stolen records with information taken from other breaches.

This compromise calls into question the reliability of these core PII elements, when used alone or with other easily compromised

data elements to verify identity. For larger financial institutions, for example those that already use multi-factor authentication to verify customer account access, the effect of this breach may be minimal. For others, including lenders who use these core PII elements as the primary method for verifying the identity of consumer borrowers, the impact may be great.

In either case, a covered financial institution must first ask the question of whether a material impact is likely. If the answer is yes, it must then "evaluate and adjust" its WISP accordingly.

This is the case as well under the newly in-force cybersecurity regulations found in 23 N.Y.C.R.R. Part 500. Although Part 500 does not apply to Equifax directly, it does cover a large number of businesses that do business with Equifax (e.g., New York chartered banks). Part 500 requires a periodic "Risk Assessment," akin to what is required under the Gramm-Leach-Bliley Act. The Part 500 Risk Assessment requirement does not come into force until March 1, 2018, but many Covered Entities under Part 500 have already conducted a Risk Assessment, in part because it was required of them under the implementing regulations of the Gramm-Leach-Bliley Act.

Under Part 500, a Covered Entity's Risk Assessment must be "periodic," but that period is not defined. Regardless, the Covered Entity's 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 … ." See 23 N.Y.C.R.R. §500.09(a). Hence, a Covered Entity under Part 500 that relies heavily on the PII elements compromised in the Equifax breach should likely inquire as to whether its continued reliance on those elements, without further compensating controls, is appropriate.

Indeed, when read together with other sections of Part 500, the necessity of this inquiry becomes even more clear. For example, under 23 N.Y.C.R.R. §500.12, Covered Entities are required to consider multi-factor authentication or risk-based authentication (e.g., use of a challenge question when a user attempts to log on from an unfamiliar IP address), based upon the Covered Entity's Risk Assessment. In addition, multi-factor authentication is required for "any individual accessing the Covered Entity's internal networks from an external network, unless the Covered Entity's [Chief Information Security Officer] has approved in writing the use of reasonably equivalent or more secure access controls." See 23 N.Y.C.R.R. §500.12(b). Certainly, the Equifax breach begs the question of whether "reasonably equivalent" controls chosen instead of multi-factor authentication can still be considered "reasonably equivalent."

What Comes Next?

Less than 24 hours after Equifax provided notice of the breach, three state attorneys general opened investigations, the U.S. House Financial Services Committee announced a potential hearing on the breach, and at least one class-action complaint had been filed against Equifax in Oregon. More investigations and litigation are sure to come, and changes to the regulatory landscape are always a possibility, given the sheer number of state and federal jurisdictions that overlap in this arena. The watchword in relation to a data breach is vigilance, whether in relation to your personal credit report or how regulators may adjust cybersecurity rules that affect your organization in response to a massive breach.