Insight

IN-DEPTH DISCUSSION

SEPTEMBER 15, 2017

Vendor Breaches and Their Implications for Employers

BY ZOE ARGENTO, PHILIP GORDON, AND ANDREW EPSTEIN

The announcement by Equifax, Inc. that it had been victimized in a hacking incident involving the personal information of 143 million Americans generated headlines this past week.[1] The sheer size of the hack means that most employers likely have affected employees. As a practical matter, the impact on employers may be a decrease in workforce productivity. At least some employees will almost certainly take time during the workday to check their credit reports, enroll in credit monitoring, or request a security freeze. Moreover, if the hackers were to commit identity fraud using the stolen personal information, many employees will have to engage in the time-consuming and distracting effort of repairing their credit.

While it is not yet known what types of information were compromised in the most recent hacking incident, employers should be aware of their obligations in responding to security breach incidents.

Employer's Responsibility for a Vendor's Data Breach

Some employers may be surprised to learn that they could be responsible for a vendor's breach. A common misconception about data breaches is that *only* the breached organization has legal obligations with respect to the breach. To the contrary, when a business vendor suffers a data breach involving data that the vendor has created or received on the employer's behalf, data breach notification laws impose ultimate responsibility for breach response on the employer.[2] The vendor's statutory responsibility is generally limited to informing the employer of the breach.

For example, Anthem, Inc., a large health insurance company, announced a breach of health information in 2015 that affected approximately 79 million

1 https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html (last visited Sept. 11, 2017).

2 *See, e.g.*, Cal. Civ. Code § 1798.82(a).

individuals.[3] As a third-party administrator for employer-sponsored group health plans, Anthem handled at least some of this health information on behalf of employers.[4] Consequently, the obligations imposed by data breach notification laws fell on those employers. Fortunately for the employers, Anthem itself took most, if not all, the steps that the notification laws required of its employer-customers. Nevertheless, the employer-customers had to closely review Anthem's breach response efforts to make sure that Anthem adequately satisfied their responsibilities.

Data Breach Laws

1. State Data Breach Laws

Data breach laws impose substantial obligations on entities that own, license, or maintain "personal information," also known as "trigger data." Forty-eight states, the District of Columbia, and certain U.S. territories require notification as a result of a data breach subject to certain exceptions.

State data breach notification laws generally require notice to affected individuals as a result of the unauthorized acquisition of unencrypted personal information. Personal information typically is defined to include first name or initial and last name plus (i) Social Security number, (ii) driver's license number and/or state identification number, or (iii) credit or debit card number or financial account number in combination with any required password.[5] Some states include additional information in the definition of personal information. Information such as account passwords,[6] health information,[7] and health insurance information[8] may constitute "trigger data" in certain jurisdictions.

These laws require breach notifications to the affected individuals.[9] Depending on the state, the breached entity may also have an obligation to notify state attorneys general, state consumer protection authorities[10] and/or the national credit bureaus.[11] Moreover, California,[12] Connecticut,[13] and Delaware[14] require the responsible entity to provide identity-theft prevention services to affected individuals. Even when these services are not legally required, most companies offer identity-theft prevention services to affected individuals in an effort to help mitigate damages and reduce the risk of lawsuits, and, in many cases, out of a sense of moral responsibility.

2. Federal Data Breach Laws

Federal law imposes data breach notification obligations on two industries that handle particularly sensitive information – the financial services and healthcare industries. For the healthcare industry, the predominant legal structure is the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which requires covered entities, *i.e.*, healthcare providers, self-insured health plans, etc., to notify affected individuals and the

---

3 *Id.*

4 https://www.anthemfacts.com/cyber-attack#faq20 (last visited Sept. 11, 2017).

5 *See, e.g.*, Idaho Code Ann. § 28-51-104(5).

6 *See, e.g.*, Ga. Code Ann. § 10-1-911(6).

7 *See, e.g.*, Fla. Stat. § 501.171(1)(g)(1)(a)(iv).

8 *See, e.g.*, Or. Rev. Stat. § 646A.602(11)(a)(F).

9 *See, e.g.*, Mass. Gen. Laws ch. 93H, § 3.

10 *Id.*

11 *Id.*

12 Cal. Civ. Code § 1798.82(d)(2)(G).

13 Conn. Gen. Stat. § 36a-701b(b)(2)(B).

14 Del. Code Ann. tit. 6, § 12B-102(e) [Eff. Apr. 14, 2018].

U.S. Department of Health and Human Services of data breaches involving protected health information.[15] In the financial services industry, the Gramm-Leach-Bliley Act (GLBA) and its attendant guidance from regulators[16] require financial institutions to establish a security breach response program and, in general, to notify affected customers when a breach occurs.[17]

3. International Data Breach Laws

Multinational employers must report data breaches in an increasing number of countries. The most significant recent development in this regard is the new data protection framework in the European Union (EU) – the General Data Protection Regulation (GDPR), which becomes effective on May 25, 2018.[18] While only a few EU member states currently require breach notification, the GDPR imposes that requirement on all 28 member states.[19] Under the GDPR, breached companies must notify the relevant, national data protection authority (DPA), and must also notify affected individuals if the breach is "likely to result in a high risk to the rights and freedoms of natural persons."[20]

Two aspects of the GDPR will make compliance with its breach notification requirements more challenging than compliance with U.S. data breach laws. First, under the GDPR, a personal data breach can involve any individually identifying information, not just the limited categories of sensitive information protected by U.S. laws. Second, the GDPR requires that compromised entities report a personal data breach to the DPA within 72 hours of discovery. Meeting this deadline will likely prove difficult in many circumstances. In the hectic period immediately after discovering a breach, companies are usually consumed with determining the extent of the breach and containing it.

Vendor Data Breaches

Breach notification laws generally impose few obligations on vendors. Most laws require only that the vendor promptly report the fact of the breach to the employer-customer that is responsible for the breached data. This puts the customer in a difficult position. The customer has the legal obligation to provide breach notifications, but may not have the information that applicable breach notification laws require the customer to include in the notifications. Moreover, the vendor might not adequately investigate or contain the breach, leaving the information vulnerable to further breaches.

The cost of responding to a breach can be massive. According to the Ponemon Institute, the average U.S. company incurs a cost of $225 per breached record.[21] In even a small breach, the cost of a response could quickly multiply into tens of thousands of dollars. If the vendor is uncooperative, not only would the full cost of the breach fall on the customer's shoulders, but the customer also may fail to meet its legal obligations.

In practice, however, vendors often voluntarily assume most breach response burdens in order to maintain their customer relationships. After the Anthem breach, for example, Anthem notified affected individuals and regulators and provided identity-theft monitoring.

---

15 45 C.F.R. §§ 164.400 *et seq.*

16 12 C.F.R. App'x B to Part 30.

17 *See* 15 U.S.C. § 6801(b)(1).

18 For more information about the GDPR's requirements applicable to employers with employees in the EU, please see Philip L. Gordon, "The Next HR Data Protection Challenge: What U.S. Multinational Employers Must Do To Prepare for the European Union's Impending General Data Protection Regulation," Littler Insight (Sept. 13, 2017).

19 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR), Art. 33.

20 Id. at Art. 34.

21 Ponemon Institute, "2017 Cost of Data Breach Study: Global Overview," (June 2017), (last visited Sept. 11, 2017).

Reducing the Risks of a Vendor Data Breach

Employers should consider the following steps to help reduce the risks of a security incident involving the employer's data while in the possession of vendors. First, employers should carefully vet the data security policies and procedures of any vendors that will handle data subject to data breach notification laws. Second, employers should consider adding provisions to vendor contracts that pass down the employer's breach response obligations to the vendor.

Vetting Vendors

With regard to vetting, employers should consider requesting and reviewing the following documents before engaging a vendor that will handle sensitive personal data:

- The vendor's data security policies and incident response plan;
- Any reports from third-party data security auditors or inspections;
- The vendor's employee confidentiality and/or non-disclosure agreements;
- The vendor's data security training program; and
- Template subcontractor agreements to check for data security provisions.

Depending on the sensitivity and amount of data involved, the employer might also request interviews with key data security personnel at the vendor and an inspection of the vendor's facilities. In addition, employers with personnel in the EU should know that the GDPR requires companies to conduct due diligence on any vendor that will handle the employer's personal data about those personnel. These employers should start this vetting of vendors now to prepare for the May 25, 2018 deadline, if they have not already.

Key Contract Provisions in Vendor Agreements

Before entrusting the vendor with personal information, the employer should execute a contract with the vendor that addresses the parties' obligations and rights regarding personally identifiable information. At minimum, the vendor contract should stipulate that the vendor:

- promptly notify the employer of a data breach and provide all the information necessary for the employer to provide notifications satisfying applicable law;
- notify affected individuals under the direction of the employer;
- mitigate the harmful effects of a data breach, including reimbursing the employer for all the employer's reasonable costs that result from the vendor's data breach;
- indemnify the employer for all third-party claims arising out of the vendor's data breach;
- maintain insurance that covers data breach response costs and liability for data breaches; and
- return or destroy an employer's data at the end of the engagement.

A contract covering data security is not only a recommended practice; some laws require companies to obtain a written agreement regarding data security from vendors. For example, HIPAA requires that covered entities sign a contract with any "business associate" that handles protected health information on behalf of the covered entity.[22] The HIPAA regulations explicitly require that the contract include a long list of data security provisions.[23] The GDPR includes a similarly detailed list of provisions that EU employers must include in the contracts with vendors that process EU personal data on their behalf.

22 45 C.F.R. § 164.502(e)(2).

23 45 C.F.R. § 164.504(e).

Responding to the Recent Breach

Despite the fact that employers do not appear to have any legal responsibility to respond to the Equifax breach, employers should consider encouraging their employees to take steps to protect themselves. Employees who act quickly in response to the breach can reduce the risk of identity theft and potentially avoid the time-consuming and frustrating process of resolving such theft. Not only may employees appreciate their employer's concern, encouraging employees to protect themselves also may boost the employer's bottom line. Employees distracted by identity theft may be less productive, especially if they have to take time off work to file police reports regarding identity theft, call merchants to close fraudulent accounts, and dispute information on their credit report.

Employers should ask their employees to review information provided by Equifax concerning the breach at https://www.equifaxsecurity2017.com/. While on the website, employees can check whether the breach implicated their personal information. Furthermore, employers may want to encourage affected employees to enroll in the identity theft monitoring product, TrustedID Premier, offered by Equifax. Through Equifax's offer, TrustedID Premier is free for individuals for 12 months and includes credit-file monitoring at all three credit bureaus and identity-theft protection. Additionally, employers should consider encouraging their employees to place a fraud alert or even a security freeze on their credit files. Employees, however, should be mindful that placing a fraud alert or security freeze on their credit file may delay their ability to obtain credit. Additionally, employees may consider filing their taxes early to minimize the risks of fraudulently filed tax returns which could delay the payment of tax refunds to the rightful individual.

Conclusion

As the Equifax breach demonstrates, even large, sophisticated companies can fall victim to data breaches. Employers should assume that the same thing could happen to any vendor. Although employers can never entirely protect their employees from data breaches, they can at least reduce the risk that employee data will be breached while under their control or the control of a vendor and mitigate the risk to the employer when a vendor breach does occur.