Cybersecurity Law Report
An Acuris company

cslawreport.com

August 21, 2019

THIRD PARTIES

Third-Party Data Breaches Highlight the Importance of Vetting Vendors in Compliance With GDPR and CCPA

By Linda A. Malek, Jason Johnson and Nora Lawrence Schmitt, *Moses & Singer*

The potentially devastating impact a third-party breach can have on companies necessitates the vetting of third-party vendors, and now new sweeping regulations such as the GDPR and California Consumer Privacy Act (CCPA) are addressing third-party risk, specifically with provisions regarding what companies need to do to vet and monitor their vendors. Companies covered by these regulations should understand these new significant obligations concerning their third-party vendors, as well as how best to structure contractual agreements and implement effective ongoing monitoring.

See CSLR's two-part series on how to maintain effective and secure long-term vendor relationships "Understanding the Risks" (Jun. 20, 2018); "Addressing the Issues" (Jun. 27, 2018).

AMCA Breach Compromises Data of 20 Million Individuals

In early June 2019, the clinical laboratory Quest Diagnostics (Quest) disclosed a data breach impacting upwards of 11.9 million patients. Just one day later, the healthcare diagnostics company LabCorp announced that it also had experienced a data breach impacting roughly 7.7 million individuals. Almost immediately thereafter, the commercial diagnostic laboratory BioReference, a wholly owned subsidiary of Opko Health, Inc., followed suit, announcing that the personal information of nearly 422,000 of its patients had been breached. Altogether, the personal, medical and financial data of roughly 20 million individuals was compromised as a result of these breaches.

The breaches can all be traced back to the same third-party contractor – the billing collections provider American Medical Collection Agency (AMCA). According to SEC filings, the breach lasted for approximately eight months before it was discovered. AMCA has since filed for Chapter 11 bankruptcy, citing a "host of negative consequences" brought on by the breach including "not only a crush of litigation ... but also a host of requests and demands made by numerous government authorities."

However, it is not just AMCA that is under intense scrutiny; the cybersecurity practices of Quest and LabCorp have come under the microscope as well. The Illinois and Connecticut attorneys general have launched

investigations into both companies' security policies. New Jersey Senators Cory Booker and Bob Mendez also have sent letters demanding that Quest and LabCorp provide a detailed explanation of their cybersecurity practices, including how they evaluate the security systems of the third-party vendors to which they outsource data. Individuals who were affected by the breach in several states, including California, New Jersey, and New York, have filed class action lawsuits against Quest and LabCorp, claiming the companies failed to take reasonable security measures to safeguard customers' data.

See also "The Growing Role of State AGs in Privacy Enforcement" (Nov. 28, 2018).

The Importance of Vetting Third-Party Vendors

The Quest and LabCorp breaches make clear that companies should carefully vet and diligently monitor the third-party vendors to which they outsource functions and share customer data. This is particularly important in the wake of the CCPA and the E.U.'s GDPR, which place significant obligations on companies covered by either or both laws (covered companies) concerning their third-party vendors. The CCPA and GDPR require covered companies to "push down" their obligations to third-party vendors which, practically speaking, means covered companies are just as responsible for the security practices of their third-party vendors as they are for their own.

Under GDPR, both controllers (defined as the entity that determines the purposes and means of processing personal data) and processors (defined as the entity responsible for processing the data on behalf of a controller) must implement appropriate technical and organizational cybersecurity controls, including the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of their processing systems and services.

Similarly, the CCPA requires covered businesses to implement and maintain "reasonable security procedures and practices appropriate to the nature of the information." While the term "reasonable security" is not defined in the CCPA, it is generally understood to require reasonable steps to ensure that the third-parties to whom data is disclosed are equipped to protect that data in accordance with law.

See "How to Ensure GDPR-Compliant Third-Party Relationships" (May 18, 2018).

Areas for Due Diligence Focus

Before engaging with any third-party vendor, a covered company should perform careful due diligence, with focus on particular areas, to ensure that the vendor is capable of meeting its obligations under the law. This is also a matter of general best practices for all companies that engage third-party vendors, including those that are not subject to GDPR or CCPA.

See also "Checklist Approach to Effective Third-Party Vendor Oversight" (Aug. 15, 2018).

Categorize Based on Risk

At the outset, it is helpful for covered companies to categorize prospective vendors

by potential risk based on responses to the diligence performed and the nature and amount of consumer data to which they have access. This can be established through careful data inventory and mapping exercises. Vendors that pose higher risks to consumer privacy should be subject to further, more rigorous due diligence, to ensure that there are adequate systems and policies in place to protect the data provided by the covered company.

Technical Security Measures

Covered companies should have a standard procedure in place to evaluate a third-party vendor's technical security measures. This procedure should include an evaluation of the following types of issues:

- Whether the vendor has specific measures in place to prevent against the unauthorized or unlawful processing of data, such as the use of industry-standard encryption, secure access controls, multi-factor authentication and up-to-date perimeter and host-based security, such as firewalls.
- How often the vendor tests its systems for new threats and vulnerabilities and what procedures the vendor has in place to effectively respond when new threats and vulnerabilities are identified. Can the vendor effectively identify, assess and address reasonably foreseeable risks, both internal and external, to the security, confidentiality or integrity of data?
- Whether the vendor has the technical and operational capabilities to meet its obligations to the covered company under the law and its contract. For example, can the vendor comply with a covered company's instructions to delete particular consumer information? Similarly, can the vendor perform its data breach reporting obligations to the covered company, and would it be capable of providing meaningful assistance in the event of a breach?

Cybersecurity Policies and Procedures

Covered companies should consider performing a thorough review of the third-party vendor's cybersecurity policies and procedures or, alternatively, asking their vendors to make representations that they have a program in place to address the following types of questions:

- Does the vendor have designated cybersecurity personnel, such as a chief information security officer, and does the vendor require its staff to undergo cybersecurity and data privacy training?
- Does the vendor have a data breach response plan in place and, if so, is it compliant with applicable law? Additionally, does the vendor have a data breach mitigation plan in place? Have these plans been tested?
- Does the vendor have data backup and disaster recovery plans, and are the plans consistent with industry standards?
- Is there a policy that addresses the assignment and management of user access controls such as unique identification codes and passwords and restrictions on the remote access of data, such as the storage of customer data on employees' personal phones and laptops?

- If the vendor is handling sensitive data such as medical information, Social Security numbers, or financial information, are there policies and procedures in place to adequately protect this type of sensitive data?

Past Security Incidents

The covered company should request information as to whether the prospective vendor has experienced a data breach in the past and, if so, how the vendor responded, including whether the vendor implemented additional security measures to prevent similar future incidents.

Third-Party Assessments

It is also critical to understand whether the third-party vendor will utilize any of its own sub-processors. If so, the prospective vendor should be required to perform its own third-party risk assessments on those sub-processors and report those findings to the covered company.

Ultimately, when performing initial due diligence on a prospective vendor, covered companies should endeavor to perform a thorough gap analysis to identify any areas where the security practices of the vendor may fall short. Once those gaps have been identified, the covered company can work proactively with the vendor to address them, often through contractual arrangements.

Structure Contractual Arrangements Carefully

Both GDPR and CCPA place significant obligations on covered companies with respect to their contractual relationships with third-party vendors.

See also "Forensic Firms: Key Contract Considerations and Terms (Part Two of Three)" (Mar. 8, 2017).

GDPR and CCPA Contractual Requirements

GDPR is especially rigid with respect to the contractual relationships between controllers and processors. Under GDPR, controllers may only engage processors that can provide sufficient guarantees of their ability to comply with the law's data protection requirements, and this must be agreed to by the processors in a written contract or another binding agreement. Article 28 of GDPR establishes 13 required provisions that must be contained in this agreement, including obligations on the processor to only process personal data on the controller's documented instructions, maintain specific security measures and provide assistance with data breach responses.

The CCPA is less prescriptive than GDPR concerning the actual terms that must be contained within a contract between a covered company and a service provider (defined as a for-profit entity that processes information on behalf of a CCPA-covered business). CCPA requires that the service provider be bound by a contractual arrangement that prohibits it from retaining, using, or disclosing the personal information "for any purpose other than for the specific purpose of performing the services specific in the contract[.]"

Other Important Contract Terms

It is not enough for covered companies to rely on the minimum required provisions of either

or both of these laws, whichever is applicable, however. In addition to the required elements, covered companies should draft contracts with vendors that require ongoing diligence and obligations in certain areas related to the protection of data provided to the vendor; this is also recommended as a matter of best practices for all companies that engage third-party vendors, regardless of GDPR or CCPA applicability. Some important issues to consider when structuring these contractual arrangements include:

- *Representations and Warranties:* Ensure the contract contains specific representations and warranties regarding the third-party vendor's compliance with applicable law, existence of and adherence to cybersecurity policies and procedures, and industry-recognized security standards.
- *Liability for Downstream Vendors:* Covered companies should require vendors to ensure that their own data protection obligations are also required of sub-processors and to assume at least a certain degree of liability for the actions of sub-processors to whom they disclose data.
- *Inspections, Audits and Cooperation:* The contract should allow for ongoing inspections and audits of the third-party vendor or, alternatively, require that the vendor conduct internal audits and submit reports of results of each analysis to the covered company. Such protections enable the covered company to ensure consistent compliance with law and the terms of the contract. Similarly, the agreement should require the third-party vendor to cooperate with a covered company's incident response plan and provide all reasonable assistance necessary for the company to investigate, respond to, and address security risks and incidents.
- *Breach Notification:* It is especially important to include robust data breach notification provisions that require the vendor to notify the covered company of suspected or known breaches within a specific amount of time. Under GDPR, processors are required to notify a controller of a breach "without undue delay," and the CCPA does not currently place any breach notification requirements on service providers. (Note, however, that many states, including California, have separate breach notification laws that require notification in the event of a breach). Specific timeframes should be built into contractual arrangements to ensure each party has a solid understanding of its obligations in the event of a breach. It is also prudent to determine in advance which party will bear the costs associated with a breach – such as the cost of notifying impacted customers or providing credit monitoring services when required – particularly if the third-party vendor is at fault.

See also "Analyzing New and Amended State Breach Notification Laws" (Jun. 6, 2018).

Ongoing Monitoring and Testing of Security Procedures

A covered company's responsibilities under GDPR and CCPA do not end once the contract is signed. It is imperative for companies to perform ongoing monitoring of third-party

vendors to verify the effectiveness of their cybersecurity measures. Vendors should be required to provide covered companies with results of security systems tests and cybersecurity training, as well as confirmation that they have been conducted at regular intervals.

The Cost of Violation

Both GDPR and CCPA impose heavy penalties in the event a company violates its legal obligations. GDPR sets out maximum fines of the higher of 20 million euros or 4 percent of the controller or processor's worldwide turnover. Civil penalties under the CCPA range from $2,500 for each violation to $7,500 for each intentional violation, with no cap on total liabilities. The CCPA also allows for a private right of action in the event of a data breach.

Both GDPR and CCPA place some limitations on secondary liability. For example, under GDPR both controllers and processors may be exempt from liability if they are "not in any way responsible for the event giving rise to the damage." Similarly, under the CCPA a company will not be liable for the misconduct of a service provider if the company was in compliance with the CCPA's requirement to execute a written contract and, at the time of disclosure the business did not have actual knowledge or reason to believe that the service provider intended to violate the Act. The practical application of these exceptions, however, remains unclear, and the standards for determining whether a company was "not in any way responsible" for misconduct, or lacked a "reason to believe" misconduct would occur are ambiguous at best.

Perhaps more important than monetary penalties is the reputational harm that can result from a third-party breach. As the Quest and LabCorp breaches demonstrate, in the event of a breach, consumers, government enforcement agencies and regulatory authorities are all likely to focus as much on the conduct of the primary company as on the third-party vendor.

See our two-part series on preparing for the CCPA: "Securing Buy-In and Setting the Scope" (Feb. 27, 2019); and "Best Practices and Understanding Enforcement" (Mar. 6, 2019).

Linda A. Malek is chair of the healthcare and privacy & cybersecurity practices at Moses & Singer in New York.

Jason Johnson is a partner in the firm's healthcare, intellectual property and privacy & cybersecurity practices.

Nora Lawrence Schmitt is an associate in the firm's healthcare and privacy & cybersecurity practices.

Elizabeth O. Nwabueze, a law clerk with the firm, contributed to this article.