Published on *The National Law Review* https://www.natlawreview.com

Tech Transactions & Data Privacy 2022 Report: Third-Party Data Incidents: Preparing and Responding as the Volume of Incidents Rise

Article By:

Bruce A. Radke

Caitlin A. Smith

Noor K. Kalkat

Anna K. Schall

Tech Transactions & Data Privacy 2022 Report

Preparing for and Responding to Third-Party Data Incidents

I. **The Rise in Frequency and Size of Third-Party Data Incident**

Many organizations realize that using technology to support both customer-facing and back-office tasks deliver the efficiency and accuracy that employees and customers have come to expect. These technological solutions often reduce overhead internally and allow customers, employees and external third parties to interact with the organization more transparently. However, by incorporating software-as-a-service (SaaS) solutions used in-house, or off-premises services managed entirely by a third party, organizations are exposed to additional 1See 12 C.F.R. Part 30, App. B A (Office of the Comptroller of the Currency); 12 C.F.R. Part 208, App. D-2 (Federal Reserve); 12 C.F.R. Part 364, App. B (Federal Deposit Insurance Corporation); and 12 C.F.R. Part 748, App. A (National Credit Union Administration)).potential privacy and security risks.

A large reason for the increase is that threat actors are exploiting the technology supply chain—targeting technology providers with direct access to many customer systems, rather than trying to compromise customer systems one by one. The attacks are very clever, and many times go undetected by even the most sophisticated organizations. In late 2020, around 20,000 organizations using the SolarWinds Orion IT monitoring and management software ran what appeared to be a routine update/patch to the software, only to later discover malicious code was pushed through the update that granted threat actors unauthorized access to thousands of organizations. The attack impacted U.S. government organizations, including Homeland Security, and technology giants like

Microsoft, Cisco and FireEye.

While the SolarWinds breach was responsible for allowing direct access to customer systems and data, organizations also need to be mindful of data shared externally with third parties. Organizations should understand that state and federal data breach notification laws put the responsibility of notifying individuals of a data breach on the owner of the data, which in these cases is most often the organization rather than the vendor. The vendor's only legal, and oftentimes financial, responsibility is to notify its customer organizations, and in turn, the customer organizations provide legal notification of a data breach to customers or employees.

In addition to the data privacy and access concerns when a security incident occurs, organizations also need to contemplate the potential operational impacts. While technology solutions create efficiencies, an organization could become largely dependent on the software or service functioning properly. When the third-party solution fails, the downstream business interruption could be disastrous. In December 2021, a major HR technology provider announced that it was hit with a ransomware attack that took many of its core services offline. Further, the company reported that the services would have to remain offline for several weeks. Customers reverted to manually tracking time and issuing physical paychecks, a process many employees may have never experienced in their careers. Most companies were able to get paychecks out on time, at a very crucial time of the year, but the longer-term effort of reentering the time, and adjusting for deductions, overtime and hours cannot be quantified.

Gone are the days when an organization can prepare its own privacy and security practices in a vacuum. As discussed mover fully below, organizations are much more dependent on our third-party solutions, and it is imperative that organizations (1) sufficiently vet vendors' privacy and security standards, (2) include contract terms to address outages, data privacy and costs associated with both, (3) continue to train contingency plans for employees who may depend on technology or software solutions to do their jobs and (4) actively seek out network vulnerabilities, in addition to the defensive antivirus and firewall solutions.

II. **Federal and State Requirements Related to Third-Party Providers**

A. **Federal Requirements**

In light of the potential risks, federal and state authorities have promulgated regulations addressing third-party vendor relationships. For example, several federal agencies that regulate banking and financial institutions (including federally insured financial institutions) under the interpretive authority granted by the Gramm-Leach-Bliley Act of 1999 issued the interagency Guidelines for Safeguarding Member Information (the "Interagency Guidelines") that, among other things, requires each financial institution to develop and implement an information security program.[1] Under the Interagency Guidelines, the financial institution's information security program must include provisions to "[e]xercise appropriate due diligence in selecting its service providers." To demonstrate the requisite level of due diligence, the Interagency Guidelines require financial institutions to require service providers by contract to implement appropriate steps to protect the security and confidentiality of sensitive customer information. Additionally, the Interagency Guidelines require, as indicated by the financial institution's risk assessment, the monitoring service providers to confirm that they have

satisfied their obligations and as part of the monitoring, the financial institutions should review audits, summaries of test results or other equivalent evaluations of service providers.

In the context of health care, the HIPAA Security Rule mandates that a written contract between a HIPAA covered entity and a business associate must require the business associate to implement appropriate safeguards to prevent unauthorized use or disclosure of the information, including implementing requirements of the HIPAA Security Rule with regard to electronically protected health information. The HIPAA Security Rule further requires the business associate to report to the covered entity any use or disclosure of the information not provided for by its contract, including incidents that constitute breaches of unsecured protected health information.[2]

B. **State Requirements**

Likewise, several states have adopted regulations governing third-party service providers as follows:

1. **CALIFORNIA**

California's Consumer Privacy Act ("CCPA") does not impose specific requirements upon third-party service providers; rather, it requires businesses subject to the CCPA to include in their contracts with third-party service providers certain terms pertaining to the use, retention and disclosure of personal information. Therefore, if a business is not subject to the CCPA, any personal information sent to or shared with a third-party service provider is also not subject to CCPA requirements.

The CCPA defines a "service provider" as a legal entity that processes personal information on behalf of a business.[3] To qualify as a service provider, the legal entity must be party to a written contract with the business that prohibits the legal entity from retaining, using or disclosing personal information for any purpose other than performing services specified in the contract or as otherwise permitted under the CCPA.[4]

In certain circumstances, a legal entity may not qualify as a service provider under the CCPA, including where the legal entity is not party to a written contract with the business or where a written contract exists, but the written contract permits the legal entity to do or more of the following:

- Retain personal information beyond termination of the contract;
- Use personal information for its own purposes; and/or
- Disclose personal information in accordance with its own policies and procedures.

The CCPA does not impose a direct requirement on service providers to delete a consumer's personal information upon request. Instead, the CCPA requires businesses to delete a consumer's personal information upon verifiable request, and the business is thereafter obligated to direct service providers to delete that consumer's personal information from the service provider's records.[5] Deletion of personal information by businesses and service providers is not required in certain circumstances, including but not limited to, where the personal information is necessary to complete the customer's requested transaction or services, to detect and protect against security incidents and/or to comply with other state or federal laws.[6]

Notably, the CCPA does not prohibit a service provider from retaining, using or disclosing personal information received from a business that is "deidentified or in the aggregate consumer information."[7] A service provider with an interest in retaining the personal information originally provided by a business may, therefore, deidentify (e.g., anonymize) or aggregate the information to non-personal information and avoid CCPA restrictions.[8] Furthermore, where a business and service provider have executed a CCPA-compliant written contract, the service provider is not required to indemnify the business for the service provider's mishandling of personal information, nor is the service provider liable if the business fails to comply with the CCPA's requirements.[9]

A service provider that breaches a written contract with a business that prohibits the service provider from retaining, using or disclosing personal information in violation of the CCPA may be subject to an injunction and civil penalties of not more than two thousand five hundred dollars ($2,500) for each violation or seven thousand five hundred dollars ($7,500) for each intentional violation by the State of California's Attorney General.[10]

2. **COLORADO**

The Colorado Privacy Act ("CPA") defines a "[t]hird-party service provider" as an entity that has been contracted to maintain, store or process personal information on behalf of a "covered entity", defined under the CPA in relevant part as a legal entity that maintains, owns or licenses personal information in the course of its business. [11]

Unless the covered entity agrees to provide its own security protection for personal information disclosed to a third-party service provider, the covered entity must require the third-party service provider to implement and maintain reasonable security procedures and practices appropriate for the type of personal information disclosed from unauthorized access, use, modification, disclosure or destruction.[12]

If a third-party service provider believes a breach may have occurred, the CPA requires that the provider notify the covered entity in the most expedient time possible and without unreasonable delay, if misuse of personal information about a Colorado resident occurred or is likely to occur.[13] The third-party service provider is also required to cooperate with the covered entity, including sharing information relevant to the security breach.[14]

3. **MASSACHUSETTS**

Massachusetts' regulations define a "service provider" as a legal entity that "receives, stores, maintains, processes or otherwise is permitted access to personal information" through its provision of services directly to another legal entity subject to Massachusetts' regulations.[15]

Owners or licensees of personal information pertaining to Massachusetts residents, including legal entities as described above, are required under Massachusetts's data breach notification law to develop, implement and maintain comprehensive information security programs that include provisions for overseeing service providers, including:

- Taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such personal information consistent with state and federal regulations; and

- Requiring third-party service providers by contract to implement and maintain appropriate security measures for personal information.[16]

4. **VIRGINIA**

Virginia's data breach statute, to the extent that it applies to service providers, only applies to tax preparers, employers and payroll service providers that own or license computerized data related to income tax withholdings.[17]

These entities are required to provide notice to the Virginia Office of the Attorney General, without unreasonable delay after the discovery of unauthorized access and acquisition of computerized data containing a taxpayer identification number in combination with the income tax withheld for that taxpayer that compromises the confidentiality of such data and that creates a reasonable belief that the information was accessed and acquired by an unauthorized person and causes, or may reasonably cause, identity theft or other fraud.[18]

III. **Proactive Steps to Minimize Third-Party Data Incidents**

In light of these regulatory requirements and increased frequency of third-party data incidents, organizations can undertake proactive steps to meet their regulatory obligations and minimize the potential risks and consequences of such incident as follows:

Vetting the vendor: As indicated above, before engaging vendors and providing them access to sensitive information, organizations must properly vet the vendors to ensure that they have implemented appropriate administrative, technical and physical safeguards to protect the data that has been entrusted to the vendors. Additionally, it is important to understand what type of security procedures and protocols the vendor has in place to avoid a potential security incident as well as the vendor's response plans in the event that the vendor has an incident. Not only will proper vetting potentially reduce the likelihood of a data incident, but it could assist the organization in demonstrating adequate due diligence in selecting the vendor in subsequent litigation where plaintiffs allege that the organization was negligent in its choice of vendor.

Understand what data is shared and to whom it is shared: Many organizations whose vendors that experienced a data incident are unaware of the full nature and scope of the data that has been shared with their vendors. Accordingly, organizations should understand what and how much data is being shared, with whom and for what purposes. Additionally, organizations need to understand how long they retain the data and whether other parties have access to the data via the immediate vendor. In large organizations, this is crucial, as it is not easy to identify which vendor has access to what data. Further, many third-party incidents frequently occur because a certain vendor has access to more information than they needed to complete the task. Therefore, the amount of sensitive information provided to vendors should be narrowly tailored to only what is required for their services.

Notice requirements: Under state data breach notification laws, if a vendor has a breach, the vendor's only obligation is to notify the owner of the personal information of the incident. Absent any contractual agreement to the contrary, the owner is then obligated to notify affected individuals and

regulators. As a result, the language in the vendor contracts will be critical in determining notification obligations. The contract terms should specify, among other things, who is the owner of the data, when and how the vendor must notify its customer of a data incident and whether the vendor is obligated to provide notification to affected individuals and regulators.

Indemnification language and recovery limitations: The contract should also include indemnification language to ensure that the company is not putting itself at risk and will not have to pay reputationally and financially for an incident they did not cause. The contract should include clear language about the costs of covering the breach and the insurance details.

Continuously monitoring: Most organizations forget to continuously check up on their third-party vendors. Companies only check-in when they have been notified of an incident. It is important that companies continuously monitor the vendor's new updates and respond when vendors reach out regarding new software or system update within their system.

FOOTNOTES

1 See 12 C.F.R. Part 30, App. B A (Office of the Comptroller of the Currency); 12 C.F.R. Part 208, App. D-2 (Federal Reserve); 12 C.F.R. Part 364, App. B (Federal Deposit Insurance Corporation); and 12 C.F.R. Part 748, App. A (National Credit Union Administration)).

2 12 C.F.R. § 164.314(a)(2)(i)(B), (C).

3 Cal. Civ. Code § 1798.140(v).

4Id.

5Id.

6 Cal Civ. Code § 1798.105(d).

7 Cal Civ. Code § 1798.145(a)(5).

8 The CCPA requires that steps be taken to ensure that such personal information cannot be re-identified. See Cal Civ. Code § 1798.140(v).

9 Cal Civ. Code § 1798.145(h).

10 Cal Civ. Code § 1798.155(b).

11 Colo. Rev. Stat. § 6-1-716(1)(b)(i).

12 Colo. Rev. Stat. § 6-1-713.5(2).

3 Colo. Rev. Stat. § 6-1-716(2)(b).

14Id.

15 201 Mass Reg. 17.02.

16 201 Mass Reg. 17.03(2)(f) (provided, however, that until March 1, 2012, a contract a person has entered into with a third party service provider to perform services for said person or functions on said person's behalf satisfies the provisions of 201 CMR 17.03(2)(f)2, even if the contract does not include a requirement that the third party service provider maintains such appropriate safeguards, as long as said person entered into the contract no later than March 1, 2010).

17 Va. Code Ann. § 18.2-186.6.(M).

18 Id. (applicable only to the employer’s employees and not to the employee’s customers or other non-employees).

National Law Review, Volumess XII, Number 41