Protecting Against Data Breach Liability:

How Service Providers Can Manage the Inherent Risk of Cyber Incidents

by Mikaela M. Witherspoon and Maureen E. Fulton

Special thanks to Koley Jessen Law Clerk Lukas Schnepel for his assistance with this article.

Most service providers of a company interact with that company's data, or the company's third-party client data, in some way. Service providers, such as marketing or advertising agencies, providers of software-as-a-service or other hosted application services, as well as other providers of professional services, generally use at least a minimal amount of customer data to perform their services. For some, customer and third-party data is integral to the services provided, such as a marketing agency that uses the company's mailing lists to send promotional offers to the company's customers. Other service providers may only interact with customer contact and payment information.

Regardless of the degree to which data will be shared with and utilized by the service provider, the surge in state data privacy laws has left many customers concerned about potential regulatory enforcement and fines in the event that data they control is subject to a breach event.[1] This means the security of personal data and resulting liability in the event of a data breach is quickly becoming a major component of many commercial contracts as service providers face potential liability for cyberattacks that compromise third-party and customer data. This is an especially pressing concern given the increasing frequency and complexity of cyberattacks in the private sector.

For example, in June 2022, Carnival Cruise Lines agreed to

Maureen Fulton

Maureen Fulton is the chair of Koley Jessen's Data Privacy and Security practice area. Maureen dedicates her practice to advising businesses in developing comprehensive privacy and data security programs. Maureen uses her experience as a Certified Information Privacy Professional (CIPP/US) to guide companies in navigating through state, federal, and international privacy laws and regulations. She also performs data privacy and security due diligence for buyers and sellers in merger and acquisition transactions. Maureen has worked with businesses to ensure compliance with the General Data Protection Regulation (GDPR), the California Consumer Privacy Act of 2018 (CCPA), and the Federal Trade Commission Act. She has assisted clients in preparing for and remedying data breach incidents and identifying the associated litigation risks. Maureen is a member of the International Association of Privacy Professionals and has frequently presented on data privacy and security issues.

Mikaela M. Witherspoon

Mikaela Witherspoon is a staff attorney with Koley Jessen P.C., L.L.O. She counsels clients on various data privacy matters, including compliance with privacy laws such as the EU's GDPR and California's CCPA. She drafts and reviews data transfer, data license, and software license agreements, as well as other technology-related contracts. She ensures license owners maintain their legal and intellectual property rights while limiting liability and ensuring compliance with privacy and data protection regulation. Mikaela is a member of the International Association of Privacy Professionals.

a $1.25 million multistate class action settlement after cyber-attacks exposed sensitive personal information of more than 180,000 Carnival employees and customers.[2] In January 2022, Morgan Stanley agreed to a $60 million class action settlement that was the result of two separate data breaches involving the personal information of more than 15 million current and former clients.[3]

Service providers can face enormous exposure for such attacks, given that they are frequently responsible for hosting customer and end-user data. The compromise of personal information and the resulting lawsuits, legal fees, and settlements or fines may result in exorbitant damages that could threaten the commercial existence of some service providers. Perhaps the most notable service provider data breach in recent years is the 2017 Equifax data breach that exposed the personal information, including first and last name, Social Security number, and address, of more than 147 million Americans.[4] In 2022, Equifax agreed to a class action settlement with the Federal Trade Commission, the Consumer Financial Protection Bureau, and all 50 states for $425 million.[5]

Service providers have three key opportunities to manage their data breach liability risk: contractual language, insurance coverage, and internal operating procedures. All of these approaches must be tailored to accommodate a service provider's unique industry, client base, and business operation. They must also be designed to synergize, rather than hinder, each other. There is no "one size fits all" solution. This article seeks to explain some of the basic ways in which service providers can navigate these issues in order to reduce risk and safeguard their bottom lines.

Contractual Language

Limiting Contractual Liability

In 2021, the average cost of a data breach in the U.S. was $9.05 million.[6] When the breach results in some way from the action or inaction of its service provider, a customer is likely to seek compensation from the service provider for their role in the breach. The most significant way that a service provider can limit its potential liability for a data breach is by including a limitation of liability clause in its contracts with its customers. A customer contract should minimize the service provider's potential liability by ensuring that such liability remains within a set range. Such liability caps may be defined by a fixed dollar amount, the fees paid by the customer in the period preceding the claim or some factor of such fees, the coverage limits pursuant to a service provider's cyber insurance policy, or a combination of these methods.[7]

Additionally, a service provider's contract language should waive consequential and other indirect damages. The majority of damages arising from a data breach are not direct damages, but consequential damages. Consequential damages stemming from a data breach could include lost profits or reputational damages, which may be hard to estimate at the time the contract is executed. In 2021, the average cost of lost business resulting from a data breach was $1.59 million.[8] The cost of responding to the breach by providing notification to the data subjects, as well as the cost of providing affected individuals with credit monitoring or reporting services, can also result in significant expense and would be categorized as consequential damages. Given these factors, the service provider's liability can quickly escalate in this area without contractual limitations of liability in place.

The extent to which liability can be limited depends on the service provider's negotiating leverage, the degree to which the provider's service is either critical or substitutable for the customer, the nature of the data at issue, and the overall value of the transaction. For example, where the service provider offers a unique product with no comparable competitors, the customer may be more willing to accept less than ideal terms when negotiating the contract. However, for smaller service providers or those who are new to the market and are still establishing themselves with their target customer base, the service provider may need to weigh the risks of accepting greater liability for data breach against gaining access to the industry through a major customer or high value contract. Where the service provider has access to customer data, networks, or systems, such as a provider of on-premises software, customers are likely to expect a service provider to offer broad indemnity for any data breach affecting the customer's data and will not want to agree to limit the service provider's liability or cap liability at an amount that is unlikely to cover the customer's potential losses in the event of a data breach.

However, a service provider could still attempt to limit its liability by narrowly defining the circumstances in which it will provide indemnity for a breach, such as by requiring that the breach stem solely from the service provider's failure to comply with the data security requirements set forth in the contract. This would avoid liability for damages resulting from a breach that occurs despite the service provider undertaking all security measures and access restrictions to which they agreed in the contract—essentially a breach that occurs despite the best efforts of the provider to maintain a secure technical environment.

Defining a Data Breach

Another important aspect of service provider contracts is what qualifies as a "breach." Sometimes it is advantageous to define "breach" in accordance with applicable state or federal regulations to ensure consistency if the service provider generally agrees to the same governing law in each agreement. However, variation in such regulations can complicate this approach, especially if the data in question falls within the

purview of the Health Insurance Portability and Accountability Act ("HIPAA") or the Gramm-Leach-Bliley Act ("GLBA") and is subject to specific breach notice requirements codified in those laws. Where possible, service providers should seek to utilize a definition of "breach" that only covers security incidents where customer data is affected in a way that causes an *actual loss* to customers.

Customers will seek broader language that covers a larger set of security-related incidents or attempted incidents even if there is no loss or damage to data, especially due to the fact that customers often have contractual duties to notify their end users or data subjects of such incidents.[9] The definition of "breach" within a contract can be an important point of contention in negotiations with customers and should be drafted as narrowly as possible.

Imposing Security Requirements on the Customer

Service providers should also seek to impose some security requirements on the customer when the services will require the provider to access the customer's system or when the customer will have some access to the provider's own system. For example, a service provider might obligate customers and their end users to shore up the security of their technology ecosystems by mandating maintenance of firewalls or network access protocols. A service provider could also require the customer to ensure its system is up to date and to incorporate all patches or updates provided by the service provider where appropriate. This language should be carefully constructed to prevent developments in technology and cyber threats from rendering it obsolete. One way to accomplish this is to reference generally accepted industry cybersecurity standards, such as the U.S. Department of Commerce NIST framework.

However, if service providers decide to include these kinds of requirements in their contracts, they would be well advised to treat and contractually require their customers to treat them as strictly confidential, because knowledge of a service provider's security protocols can be useful to malicious actors attempting to breach the service provider's system or service.

Insurance Coverage

A service provider should also ensure that it has proper insurance coverage for data breach liability. Many commercial general liability insurance policies contain exclusions for cyberattacks and related issues. Some insurers will not cover data breach liability, while others will only do so if an insured purchases the correct endorsement. Service providers should seek out cyber coverage that will pay the costs of investigating potential breaches, providing affected parties with notice of breaches, and paying employees for additional time and effort required to respond to breaches. Such coverage may also pay

for the costs of data restoration, blackmail or extortion, loss of business income, and legal fees that arise out of data breaches.

Internal Operating Procedures

Service providers should also adopt operational practices to reduce their risk of data breach liability. Adopting formal operating procedures for managing security risks is highly advisable and may even be contractually required in some instances. Service providers should consider developing centralized guidance containing all data security-related actions that must be taken pursuant to agreements with customers and the service provider's own vendors, including specific firewall requirements or user authentication systems. These requirements should be reviewed prior to any changes to the service provider's IT and security systems to ensure any update does not inadvertently put the provider in breach of an agreement. This document should also summarize the substantive contractual requirements related to a data breach, such as the time for notice to the other party and any indemnification obligations for the service provider. A similar approach should be taken with regard to keeping track of all duties imposed by federal, state, and local laws and regulations, as well as relevant case law developments that have an impact on those duties.

Finally, service providers should also keep record of internal plans regarding data breaches, making sure to build out contingency plans for various types of breaches. These plans should involve any legal or public relations response that a vendor may need to undertake. Consulting with legal counsel is highly recommended in developing these plans, as such plans must take account of rapid changes in privacy and data security law and should be developed with an eye towards potential future litigation.

If you have questions regarding the steps your business should take to ensure it is protected from data breach liability, please contact one of the specialists in Koley Jessen's Data Privacy and Security Practice Area.

Endnotes

1 The Virginia Consumer Data Protection Act and the California Privacy Rights Act become effective on January 1, 2023, the Colorado Privacy Act and the Connecticut Data Privacy Act become effective on July 1, 2023, and the Utah Consumer Privacy Act becomes effective on December 31, 2023.

2 *Carnival Cruise Line Pays $1.25M Settlement in 46-State Breach Lawsuit*, International Association of Privacy Professionals (June 2, 2022), https://iapp.org/news/a/carnival-cruise-line-pays-1-25-million-settlement-in-46-state-breach-lawsuit/.

3 Jonathan Stempel, *Morgan Stanley to Pay $60 mln to Resolve Data Security Lawsuit*, Reuters (Jan. 3, 2022), https://www.reuters.com/markets/funds/morgan-stanley-pay-60-mln-resolve-data-security-lawsuit-2022-01-02/.

4 Todd Haselton, *Credit Reporting Firm Equifax Says Cybersecurity Incident Could Potentially Affect 143 Million US Consumers*, CNBC (Sept. 7, 2017), https://www.cnbc.com/2017/09/07/credit-reporting-firm-equifax-says-cybersecurity-incident-could-potentially-affect-143-million-us-consumers.html.

5 *Equifax Data Breach Settlement*, Federal Trade Commission (February 2022), https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement.

6 2021 Cost of Data Breach Report released by IBM, https://www.ibm.com/downloads/cas/OJDVQGRY#:~:text=The%20average%20per%20record%20(per,per%20record%20cost%20was%20%24141.

7 A common approach that can offer additional comfort to customers is to include two options for the liability cap, such as "the greater of (a) two times (2x) the fees paid by Customer in the twelve (12) month period preceding the event giving rise to the claim, or (b) the amount of insurance proceeds actually received by Service Provider pursuant to its cybersecurity insurance policy."

8 *See* IBM 2021 Cost of Data Breach Report. https://www.ibm.com/downloads/cas/OJDVQGRY#:~:text=The%20average%20per%20record%20(per,per%20record%20cost%20was%20%24141.

9 Customers frequently include contractual provisions requiring the service provider to provide information relating to the breach and to refrain from disclosing any information on the breach or contacting data subjects without the customer's consent. These provisions generally align with requirements under state privacy laws as well as the European Union General Data Protection Regulation ("GDPR") but can be revised at the margins, particularly regarding the issue of disclosure of the breach by the service provider, as the service provider should ensure it is at least permitted to share such information with its legal counsel.