Bloomberg BNA

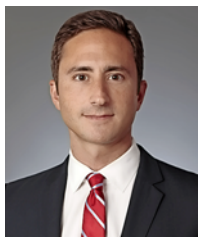
Privacy and Security Law Report®



**Cloud Breaches**

Although high-profile data breaches against the Democratic National Committee and large retail companies have grabbed headlines, the risk of a data breach cuts across industries and affects businesses large and small, causing some companies to migrate mission-critical data, including sensitive customer information, to third-party cloud providers. Even if the cloud is more secure, data stored there face many of the same threats and can be an attractive target for hackers, the authors write.

# Contracting in the Cloud: Who Pays for a Data Breach?



BY SCOTT NONAKA AND KEVIN RUBINO

*Scott Nonaka is partner in Sidley Austin LLP's International Arbitration practice in San Francisco. Kevin Rubino is an associate in Sidley's Complex Commercial Litigation practice in San Francisco.*

*This article has been prepared for informational purposes only and does not constitute legal advice. This information is not intended to create, and the receipt of it, does not constitute a lawyer-client relationship. Readers should not act upon this without seeking advice from professional advisers. The content therein does not reflect the views of the firm.*

The recent hack of the Democratic National Committee is the latest in a string of high-profile data breaches that have exposed the private information of millions of Americans (15 PVLR 1565, 8/1/16). Retail companies, in particular, have been hard hit, resulting in millions of dollars being spent to secure computer systems and compensate consumers. One large retailer agreed to pay over $100 million in legal settlements to banks and customers after hackers stole tens of millions of credit card numbers from its database in 2013. That retailer also incurred millions of dollars more in other expenses, including the cost of the investigation, attorneys' fees and voluntary credit-monitoring and identity-protection services.

Although these high-profile data breaches have grabbed headlines, the risk of a data breach cuts across industries and affects businesses large and small. Since 2013, hackers have accessed the sensitive electronic records of at least 500 U.S. companies, according to the Privacy Rights Clearinghouse.

As data breaches have increased, so have the number of companies migrating mission-critical data to the cloud, including sensitive customer information. These companies often turn to third-party cloud service providers to provide data hosting, software or infrastructure services. This trend is driven, in part, by the growing perception that cloud services are more secure than traditional information technology environments. But even if the cloud is more secure, data stored there faces many of the same threats as locally-stored data and,

 ISSN 1538-3423

due to the growing amount of information in the cloud, it can be an attractive target for hackers.

The increased reliance on third-party cloud service providers raises the question: who is responsible for paying the expenses and costs associated with a data breach? Millions of dollars turn on the answer. According to a 2014 report by the Ponemon Institute, the average cost of a data breach involving the theft of at least 100,000 customer records could be as high as $5.32 million. *See* Ponemon Institute LLC, *Data Breach: The Cloud Multiplier Effect*, Sponsored by Netskope (June 2014).

Although much is at stake, the answer to the question is not always clear because allocating costs will usually depend on the terms of the cloud services contract, which in most cases will contain a limitation of liability clause that is commonplace in contracts for the sale of goods and services. Standard clauses usually state that, in the event of a breach, neither party will be responsible for the other party's ''consequential damages,'' thereby limiting their potential liability to ''direct damages.'' While the clause may seem clearly worded, the meaning of the term ''consequential damages'' is by no means clear, let alone in the context of a cloud services contract. Below, we identify some issues to consider when negotiating and drafting a limitation of liability clause so as to provide greater clarity and predictability in allocating risk and costs.

## What are Consequential Damages?

The familiar distinction between ''direct'' and ''consequential'' damages has been a staple of contract law since it was first announced by an English appeals court in 1854 in *Hadley v. Baxendale*. *Hadley v. Baxendale*, 9 Exch. 341, 156 Eng Rep 145 (1854). But while lawyers are now accustomed to hearing that ''direct'' damages are those that flow directly from a breach ''in the ordinary course of events,'' and ''consequential'' damages are those that result from the breach due to some ''special circumstances,'' these terms do not have a clearly established meaning and are still the subject of misunderstanding among lawyers, which can lead to contentious litigation.

**The increased reliance on third-party cloud service providers raises the question: who is responsible for paying the expenses and costs associated with a data breach?**

For example, it is commonly thought that consequential damages are simply those that were not foreseeable at the time the parties entered into the contract. But no damages, whether characterized as direct or consequential, are recoverable unless they were reasonably foreseeable. Restatement (Second) of Contracts § 351. Even the ''special circumstances'' that are the distinguishing characteristic of consequential damages must have been either known or foreseeable at the time of contract. *Id*. In other words, reasonable foreseeability is a minimum threshold for all damages, it is not a criteria that distinguishes direct and consequential damages.

Similarly, parties often assume that the lost profits due to a breach of contract never qualify as direct damages. This too is wrong. For example, a 2014 decision by New York's highest court found that a supplier of coronary stents that issued a recall was responsible for the lost profits its distributor suffered as a result, despite that the parties' agreement included a consequential-damages waiver. *Biotronik v. Conor Medsystems*, 22 N.Y.3d 799 (2014). Rejecting any ''bright line rule'' about the categorization of lost profits, the New York Court of Appeals held that a ''case-specific approach'' involving ''a careful look'' at the ''nature'' of the underlying agreement was required to determine what damages were a ''natural and probable consequence'' of a breach and therefore direct. *Id*. at 807–09. Examining the distribution agreement at issue in that case, the court found that reselling stents ''was the very essence of the contract'' and the pricing provisions in the agreement tied together the supplier and distributor in an arrangement akin to a ''joint venture.'' *Id*. at 809–10.

Applying similar reasoning, the California Supreme Court in *Lewis Jorge Construction Management, Inc. v. Pomona Unified School District*, 34 Cal. 4th 960 (Cal. 2004), found that lost profits could qualify as direct damages if a careful consideration of the nature of the contract suggested that they were ''a natural and necessary consequence'' of the breach. *Id*. at 969–72. According to the court, the critical first question is ''what performance did the parties bargain for?'' *Id.* The court went on to write, ''[p]rofits which are the direct and immediate fruits of the contract are part and parcel of the contract itself, entering into and constituting a portion of its very elements. . . .'' *Id.* (quotations omitted).

## Are the Damages and Costs Arising From a Data Breach Consequential Damages?

So how would these principles apply to the damages resulting from a data breach in the cloud? While there are no cases that directly address the issue, earlier this year the U.S. Court of Appeals for the Eleventh Circuit addressed an analogous situation in *Silverpop Systems v. Leading Market Technologies*, 641 Fed. Appx. 849, 2016 BL 736 (11th Cir. January 5, 2016) (unpublished). Silverpop Systems (now a part of IBM Corp.) provided an e-mail marketing tool that Leading Market Technologies used to send advertising content to hundreds of thousands of e-mail addresses. *Id*. Hackers accessed Silverpop's system and appeared to have exported at least some of Leading Market's e-mail addresses. *Id*. When Leading Market sued to recover the lost value of its e-mail list, Silverpop argued that this was consequential damages barred by the waiver in the parties' agreement, and the Eleventh Circuit agreed. *Id*.

In reaching this decision, the court focused on the purpose of the contract, which it found was e-mail marketing services and not the safe storage of data. The court accordingly concluded that the diminished value of the e-mail list qualified as consequential damages under Georgia law. *Id*. The court reached this conclusion despite its acknowledgement of a provision in the agreement requiring Silverpop to protect against the disclosure of Leading Market's ''confidential informa-

  PVLR ISSN 1538-3423

tion,'' the inclusion of which would seem to suggest that the security of the e-mail list was at least an aspect of what the parties had bargained for. *Id*.

Another decision that reached a similar conclusion involved Heartland Payment Systems, a company that processes credit card information for banks. *In re Heartland Payment Sys., Inc. Customer Data Sec. Breach Litig*., 834 F. Supp. 2d 566 (S.D. Tex. 2011). When hackers stole credit card information from Heartland's system, several banks sought the costs they incurred in paying for the fraudulent transactions and replacing consumers' cards. *Id*. at 580. Applying Ohio law, the court found that these damages were barred by the consequential-damages waivers in the banks' contract with Heartland. *Id*. To separate consequential from direct damages, the court applied a bright-line rule that was expressly rejected by the New York Court of Appeals in *Biotronik* and impliedly rejected by the California Supreme Court in *Lewis Jorge Construction Management*. According to the *Heartland* court, ''[w]hen a contract limits recovery to direct damages, a plaintiff may recover only the difference between the amount paid and the value received''—a principle under which the costs of a data breach would always qualify as consequential damages. *Id*.

**When courts examine the purpose of cloud services contracts, an important consideration will be whether providing a "secure" cloud environment is an essential and necessary part of such contracts.**

The *Silverpop* and *Heartland* decisions provide some comfort to cloud service providers and raise concerns for cloud customers who may believe that they would not have to shoulder all the costs associated with a data breach. It would be a mistake, however, to conclude that future courts would necessarily follow the same reasoning in the context of a data breach in the cloud. First, not all courts—particularly courts in New York or California—can be expected to apply the same bright-line rules relied on by the courts in *Silverpop* and *Heartland*. Second, the law on damages as it relates to cloud services is in its infancy. If the law on damages for cloud services follows the same path as in other industries, over time courts interpreting such contracts can be expected to take a more nuanced view and will almost certainly look more closely at the purpose of the contract and the nature of the breach, as the court did in *Biotronik*.

When courts examine the purpose of cloud services contracts, an important consideration will be whether providing a ''secure'' cloud environment is an essential and necessary part of such contracts. Business customers who migrate their data to the cloud often do so because they believe they are gaining greater security, and cloud service providers often tout their security as a key selling point. If data security is an important element of cloud services agreements, it is quite possible that courts interpreting such contracts would conclude that unauthorized third-party access to customer data is a ''natural and probable consequence'' of a breach of such agreements and that the resulting damages are therefore direct, which would be in line with the New York court's reasoning in *Biotronik*. *Biotronik*, 22 N.Y.3d at 807.

At this time, and for the foreseeable future, it will be difficult to predict with great certainty how courts will decide whether any particular harm arising from a data breach is direct or consequential damages. Given this uncertainty, as well as the potentially massive costs associated with a data breach, both consumers and providers of cloud services would be well-advised not to rely on standard, boilerplate language in limitation of liability clauses that simply waives consequential damages to allocate their potential liability. They should instead address the issue of potential future costs associated with a data breach in detail at the outset of their relationship by bargaining for and expressly assigning or excluding those costs in their agreement. Addressing the issue up front will not only help to prevent costly disputes and avoid unpleasant surprises, but it will also allow the parties to more effectively manage the risk of a data breach, including through preventative measures and cybersecurity insurance.

Among the issues to consider during negotiations are liability caps, carve-outs and carve-ins. Liability caps often accompany standard limitation of liability clauses and can be used to make clear the maximum amount a cloud service provider can be expected to pay regardless of the type of damages. By setting an upper limit on damages, the parties are in a better position to determine their potential risk or recovery from a data breach. Parties can then manage risk by, among other things, identifying the type and amount of insurance that should be maintained and which party should pay for such insurance. Contracts can also expressly exclude (a carve-out) or include (a carve-in) various categories of damages, such as lost profits or customer notification or litigation costs. Although it is not always possible to identify all potential future costs at the time of contracting, a fulsome discussion during negotiations can go a long way to reducing uncertainty. Finally, parties should also ensure that indemnification provisions are fully consistent with the provisions of a well-drafted limitation of liability clause so as not to inject unnecessary ambiguity.