Tossing the Hot Potato

Shifting Liability for a Data Breach Through Contractual Terms

By Cynthia P. Arends

Companies do have some ways to limit or shift liability through contracts with vendors when it comes to data breaches.

We have all seen the nearly daily headlines about yet another data breach by unidentified hackers. Weeks, months and years after those headlines will follow the next story: giant retailer settles claims with affected customers.

While that may be the end of the front-page headlines, it is not the end of the story. Often, those same large companies are evaluating and potentially separately fighting a battle with one or multiple vendors, seeking indemnification for the consumer damages and fighting direct damages and reputational losses to the companies. The indemnification battle potentially is more costly and may have more reward, depending on the role of the vendor, the contractual language at issue, and the financial situation of the vendor.

There are a number of factors driving the increase in potential data-breach indemnification claims, despite the fact that to date there are very few published decisions on them. In some circumstances, such as when it was the integrity of a vendor's security that allowed a data breach, a claim is not unexpected. And, to counter the circumstance in which only common law indemnification or contribution are available, many companies are now including explicit data-breach indemnification language in all of their vendor contracts, regardless of the vendor or the scope of the data access. Beyond this, though, the increasing use of third-party vendors to store data, frequently in the cloud, has resulted in greater scrutiny of those vendors' security commitments and practices and also an increased focus on the limitations of liability that those vendors traditionally included in their service contracts.

Given the potentially devastating consequences of a data breach, outside and inside counsel are well served by taking the time to review closely the "fine print" on standard service contracts and also to update the indemnification and

■ Cynthia P. Arends is a shareholder in the Minneapolis firm of Nilan Johnson Lewis. Ms. Arends regularly litigates various aspects of indemnification agreements and also advises clients on means to minimize litigation through practical indemnification language. She is licensed to practice in Minnesota and North Dakota, including in the appellate courts, and is also a qualified neutral under Rule 114 of the Minnesota Rules of General Practice. Within DRI, Ms. Arends serves as the Vice Chair of the DRI Data Management and Security Committee.

limits of liability language in their own standard contracts explicitly to call out data breach and the scope of a liability shift. This article will discuss the background of contractual provisions relating to data breaches and considerations in contracting for indemnification or limits on liability.

Even without being held liable for consumer or financial institution claims, business entities face significant costs simply defending the claims, warranting the impetus for some indemnification.

Setting Up the Case for Indemnification

Indemnification claims almost always include coverage for third-party claims. However, in the context of data-breach cases, to date, the most commonly expected claims—consumer claims—have been largely unsuccessful. Court after court has held that consumers pursuing a remedy from the victim of a data breach lack standing to pursue the claim because absent a showing of an actual misuse of their data, they have no injury in fact. *E.g., Reilly v. Ceridian Corp.*, 664 F.3d 38, 45 (3rd Cir. 2011)*; Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629, 637 (7th Cir. 2007); *Allison v. Aetna, Inc.*, No. cv-2560, 2010 WL 3719243, at *4 n.3 (E.D. Pa. March 9, 2010) (listing decisions holding no standing existed). The reasoning that courts apply is that the increased risk of a misuse of data is not an injury in fact, nor is the need for credit monitoring sufficient. *Reilly*, 664 F.3d at 45; *Pisciotta*, 499 F.3d at 637. But the tide appears to be shifting on consumer data-breach claims. In December 2014, the U.S. District Court in Minnesota, handling an MDL for all Target data-breach claims, denied Target's motion to dismiss claims for lack of standing and multiple other bases. *In re Target Corp. Customer Data Security Breach Litig. (Consumer Litigation Cases)*, MDL No. 14–2522, ____ F.3d ____, 2014 WL 7192478 (D. Minn. Dec. 18, 2014). In *Target*, the named plaintiffs alleged actual data misuse to overcome the standing hurdle. *Id.* While the Court dismissed a handful of claims based on state-specific limitations, the bulk of the claims—from consumer fraud, to data security notification breach and negligence—survived Rule 12 and will next proceed to class certification. *Id.* at * 23.

Beyond this shift, though, simply because consumers themselves have had difficulty with these claims does not mean that there is no exposure to third-party claims from a data breach. As the litigation surrounding the Target data breach illustrates, financial institutions also have potential claims without the same damages problems as consumers. For example, in the *Target* financial institutions case, the U.S. District Court in Minnesota also recently denied Target's motion to dismiss claims brought against it by a group of banks that issued payment cards hacked during the Target breach. *In re Target Corp. Customer Data Security Breach Litig.(Financial Institution Cases)*, MDL No. 14–2522, ____ F.3d ____, 2014 WL 6775314 (D. Minn. Dec. 2, 2014). The Court held that the banks had adequately pleaded claims for negligence and violation of Minnesota's Plastic Security Card Act. *Id.*

Even without being held liable for consumer or financial institution claims, business entities face significant costs simply defending the claims, warranting the impetus for some indemnification. An entity that spends hundreds of thousands of dollars or more on litigation, even though it ultimately prevails, could still receive compensation for the defense-related losses if an applicable indemnification clause existed.

As the Target data breach illustrated, there are vendors whose role is unrelated to data storage that nonetheless will access a customer's data and could be the potential pathway for hackers in a data breach. In the Target situation, it is suspected that the malware traveled through a Target HVAC vendor. Krebs on Security, Email Attack on Vendor Set Up Breach on Target (Feb. 12, 2014), http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/ (last visited Jan. 28, 2014). Obviously, Target would not have contracted with an HVAC vendor for data storage or would even be a vendor that someone would traditionally consider a potential data-breach source. *Id.* Instead the breach appears to have occurred through the vendor's online payment system, which Target believed could not access its servers containing consumer information. *Id.* In that circumstance, it is likely that a customer, such as Target, would consider the data security risk very low. *Id.* For such vendors, often the focus of a contract's damage limitations and indemnification clauses is the vendor's business and the consequences of failure to perform as contracted. And while those same contracts may include information on protecting a customer's confidential or proprietary data, they may not address a breach in the context of a third-party's wrongful access based on insufficient security.

Given that the vendor is often a victim of a data breach as well and that the vendor's business was not one of protecting data, it is arguable that it is not appropriate for the vendor to bear the risk associated with a third-party hacker. *E.g., East Tenn. Gas Co.*, Federal Energy Reg. Comm'n Opinion, 65 FERC P 61223, 1993 WL 467760, at *2–3 (Nov. 12, 1993) (holding that the gas company must revise its contracts to make clear that there was no shift of liability to the shipping vendor for a third-party data breach). For a court to conclude that a broad damages or indemnification clause was intended to apply to a data breach, particularly when the vendor is not in the business of data security, it will likely require explicit mention of data security or a third-party data breach in the clause.

Historical Vendor Contracts Disclaim Liability

Setting up the perfect storm, vendor contracts' terms and conditions historically include very one-sided clauses disclaiming all warranties and limiting liability. For example, clauses limiting liability to the amount paid under the contract are fairly standard. Many businesses, without even consulting the terms, will sign off on those agreements and courts routinely enforce them given the plain language of the provisions and the fact that the two parties involved were both sophisticated business entities. With the increasing risk of vendors playing a role in a data breach, the stakes of those limitations contained within the vendor contracts has grown dramatically.

Even those entities tasked with storing and safeguarding data, as a default position, will not offer data security warranties or indemnification. In the credit industry, the argument against such protections is that the margins are too low to justify the vendors accepting the risk. *Why Braintree Won't Indemnify*, https://support.braintreepayments.com/customer/portal/articles/1192545 (last visited Dec. 18, 2014). However, even businesses in other industries also include within their standard contracts clauses that waive all warranties and liability. The clause below is from the "Terms & Conditions" of a popular document management company:

> [VENDOR] WILL NOT BE LIABLE FOR ANY LOSS OR DAMAGE CAUSED BY A DISTRIBUTED DENIAL-OF-SERVICE ATTACK, VIRUSES OR OTHER TECHNOLOGICALLY HARMFUL MATERIAL THAT MAY INFECT YOUR COMPUTER EQUIPMENT, COMPUTER PROGRAMS, DATA OR OTHER PROPRIETARY MATERIAL DUE TO YOUR USE OF THE WEBSITE OR THE SERVICE OR ITEMS OBTAINED THROUGH THE WEBSITE OR THE SERVICE OR TO YOUR DOWNLOADING OF ANY MATERIAL POSTED ON IT, OR ON ANY WEBSITE LINKED TO IT.
>
> IN NO EVENT WILL [VENDOR] BE LIABLE FOR DAMAGES OF ANY KIND, UNDER ANY LEGAL THEORY, ARISING OUT OF OR IN CONNECTION WITH YOUR USE, OR INABILITY TO USE, THE SERVICES OR ANY WEBSITES ASSOCIATED WITH IT, INCLUDING ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL OR PUNITIVE DAMAGES, INCLUDING BUT NOT LIMITED TO, PERSONAL INJURY, PAIN AND SUFFERING, EMOTIONAL DISTRESS, LOSS OF REVENUE, LOSS OF PROFITS, LOSS OF BUSINESS OR ANTICIPATED SAVINGS, LOSS OF USE, LOSS OF GOODWILL, LOSS OF DATA, AND WHETHER CAUSED BY TORT (INCLUDING NEGLIGENCE), BREACH OF CONTRACT OR OTHERWISE, EVEN IF FORESEEABLE.

In effect, these clauses waive all liability for any type of damages resulting from a data breach when the access point was through the vendor. While the vendors are certain to point out that their security platforms should protect the client data and that encryption should protect any transmission, the fact remains that as long as there is a risk of a breach at any point in the chain, someone will bear that risk, and if the vendor has waived it, then it will fall back to the customer.

Considerations for Vendor Contracting

As history suggests, each party will naturally try to limit its exposure through indemnification clauses and it is unlikely that a represented party will agree to substantially skewed provisions. The trick, then, is to prepare language that shifts the liability and the accompanying fee exposure to the party undertaking protecting the data while not attempting to achieve a windfall through the clause. Likewise, the goal of the indemnification clause should be to reduce or to eliminate litigation, not to increase it. Therefore, the clause must be clear and complete enough that the parties can know and understand how to operate under it without litigating extensively.

Damages Limitations

There are two types of claims often covered by indemnification clauses generally: clauses that provide coverage for claims brought by third parties and clauses that cover direct claims belonging to the party that is the beneficiary of the indemnification clause. So in our data-breach scenario, an indemnification clause could cover only claims brought by third parties (consumers or financial institutions), or it could cover the losses of the party that was the victim of the breach as well. While a breach victim would likely have claims against the vendor for its direct claims regardless of the contractual language, including those claims in an indemnification clause can alter the scope of the claims. For instance, a clause could include a right to attorney's fees, which would not ordinarily be available. A clause could also set a limit on liability or indicate that it is a sole remedy. Both of those limitations would serve to prevent other claims or limit the scope of damages available for them. The key when drafting these provisions, or evaluating provisions presented in a contract drafted by someone else, is to ensure that the terms are clear and not contradictory.

Setting up the perfect storm, vendor contracts' terms and conditions historically include very one-sided clauses disclaiming all warranties and limiting liability.

And in the circumstances in which a limitation of liability is included in a contract, both parties should understand the application of that limit and specifically whether it applies to damages due to a data breach. *See Silverpop Sys. Inc. v. Leading Market Tech.*, No. 1:12-cv-2513-SCJ (N.D. Ga. Feb. 18, 2014) (granting summary judgment for vendor because limitation on liability clause precluded recovery for consequential data-breach damages). Unfortunately, what often happens is that an indemnification or liability cap provision is added to an already existing contract and the parties fail to tie the provisions together adequately or there is a dispute about whether the cap applies to data-breach claims.

In contracts that include general limitations on liability, such as a prohibition on the recovery of consequential damages, parties seeking indemnification run the risk that the bulk of the data-breach damages will be precluded from recovery. *Id.* As the Court reasoned in the *Silverpop* case, the lost profits and the lost value due to leaked data were consequential damages, rather than direct damages, and therefore the limitation on liability in the contract precluded them. *Id.* While there are scores of cases and statutes that attempt to define the scope of direct versus consequential damages, parties seeking to remove ambiguity, or the need for a court to decide, should simply define the types of damages specifically limited if they are agreeing to a damages limitation clause. For example, to the extent that the parties agree that damages for third-party claims or lost profit damages will be disallowed, it should be so stated, eliminating the often litigated term "consequential" damages.

While notice and limitations on claims provisions are fairly straightforward, control of defense and settlement are often more tricky or less clearly written.

Not only is the "what" important, but who reviews a contracts is important as well. The vendor language quoted earlier is not unusual. In fact, I suggest that you take a look at the standard "Terms & Conditions" of your own document management vendor. While most vendors will note within the standard "Terms & Conditions" that it is possible for individual service contracts to establish superseding terms, it requires that your business *ask* a vendor. If the only person reviewing a vendor contract at your business is the IT manager, the manger may be very thorough in ensuring that the technical security parameters are included, but he or she may be less likely to focus on the warranty waiver and the indemnification language needed to protect your company should a breach occur despite those protections.

Indemnification Process Provisions

One key provision that is frequently forgotten in indemnification clauses is a process provision. In addition to shifting but also potentially limiting liability, well-written indemnification provisions should also include explicit process requirements so that there is no ambiguity about what needs to be done to obtain the indemnification and how that indemnification will work. How exactly is the indemnification going to work? Should there be an immediate tender? Will the indemnifying party defend and resolve all third-party claims? Or will the party receiving indemnity control litigation and settlement entirely? If so, who will pay the legal costs during the litigation? What is the mechanism for resolving reasonableness of fees and settlements? There is very little that is more frustrating to a client than when there is an indemnification provision in place but actually getting the benefit spawns protracted litigation. The process can include a number of things such as notice requirements and the effect of inadequate notice, time limitations on claims, and control of defense and settlement. While notice and limitations on claims provisions are fairly straightforward, control of defense and settlement are often more tricky or less clearly written.

There is an obvious tension between the control of defense of third-party claims and an obligation on the part of another party to pay for those claims. Generally, one party will not be willing to give the other free rein to control defense and settlement unless a clause also relieves that party of liability. One suggestion is to require as part of the notice provision that the indemnifying party accept a full tender of defense, along with the corresponding control of settlement and defense, within a set time period. If the indemnifying party accepts, the indemnified party could still participate in the claims defense if it so chooses, but it would do so at its own expense. On the other hand, if the indemnifying party fails to accept within that time period, the full control of defense and settlement moves back to the party with the indemnification. Such a clause could require the indemnifying party to pay for some percentage of the fees and costs while the third-party claims are pending. Key to this arrangement is then establishing an abbreviated process for assessing the reasonableness of any resolution of the third-party claims and the litigation costs and fees to avoid protracted litigation about the value of the indemnification.

Don't Forget the Mobile Apps

As a practitioner or in-house counsel, you work through vendor contracts, in conjunction with those with security expertise, and reach a point where both sides are comfortable with the security provisions and the indemnification and liability-limiting language. The contract is signed and everyone goes their way. Then the vendor develops a mobile application. The mobile app will likely make the customer's users happy, but before jumping in to use the mobile app, it is important, at a minimum, to communicate with the vendor regarding the terms that apply to the mobile app. As the Yelp and Fandango voluntary consent decrees with the Federal Trade Commission (FTC) illustrate, too often the development of a mobile app does not follow the same privacy and security protocols as a main site, resulting in troubling inconsistencies. Press Release, Fed. Trade Comm'n, Yelp, TinyCo Settle FTC Charges (Sept. 17, 2014), http://www.ftc.gov/news-events/press-releases/2014/09/yelp-tinyco-settle-ftc-charges-their-apps-improperly-collected (last visited Jan. 28, 2015); Press Release, Fed. Trade Comm'n, Fandango, Credit Karma Settle FTC Charges (Mar, 28, 2014), http://www.ftc.gov/news-events/press-releases/2014/03/fandango-credit-karma-settle-ftc-charges-they-deceived-consumers (last visited Jan. 28, 2015).

While both the Fandango and Yelp situations involved consumers affected directly by the differences between the mobile apps and the main sites, the background story illustrates how potential problems can arise when a mobile app is developed. *Id.* In fact, in settling the Yelp case, the FTC specifically highlighted this point, stating, "As people—especially children—move their lives onto mobile devices, it's important that they have the same consumer protections when they're using an app that they have when they're on a website." Fed. Trade Comm'n, Press Release of Sept. 17, 2014, *supra*. Whether it is simply overlooked or it is because a different business unit develops the mobile app, the fact remains that in both of those circumstances, the security and privacy protections included in the main site did not carry across to the mobile app. The lesson, therefore, is that customers want to be certain that the terms negotiated for a main site apply to a mobile app or that any new terms are equally agreeable. Assuming that the same security and financial protections exist without confirming it is a risky move.

A Note on Insurance

Any discussion on protection from the financial devastation of a data breach would not be complete without mentioning insurance. Increasingly companies will purchase policies that provide protection for investigation and containment, notification of affected parties, media relations, and claims. The details and the considerations to take into account when purchasing those policies would fill another article. But there are a few important things to consider that relate to contractual liability-limiting and liability-shifting provisions when looking for insurance. Most importantly, it is critical to understand where a company's liability starts and to make sure that the insurance coverage starts at that same point. For instance, if a vendor disclaims all liability for the security of data in transmission, then it is critical that the insurer does not also exclude coverage for that piece of the puzzle. Moreover, to the extent that a company takes on liability by using or handling data, that same aspect need also be covered by the corresponding policy. The worst case scenario is one in which the contracts are well negotiated and the cyber policy is in place, but there is a gap between the two and that gap is arguably the point of breach. The goal is to make coverage seamless, which is why ensuring coordination between vendor contracts and the corresponding insurance procurement is critical.

Conclusion

It goes without saying that a data breach is potentially a financially devastating event for a business. It is impossible to do away with all the problems that will accompany a breach in contracts, but it is possible through contracts to reduce some of the financial exposure. Carefully reviewing and negotiating the terms contained in vendor contracts will help a business either limit its exposure or at least know about and prepare for the exposure that it retains.