New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 254—NO. 2
MONDAY, JULY 6, 2015

Outside Counsel

Expert Analysis

Strategies for Navigating Business-to-Business Data Breaches

By **Joseph V. DeMarco**

And **Urvashi Sen**

There is no shortage of attention in the media to data breaches affecting consumers in the United States—so called "business to consumer," or "B2C" data breaches. And rightfully so—the Identity Theft Resource Center, which has been tracking data breaches in the United States since 2005, released a report in January 2015 which showed that U.S. B2C data breaches hit a record high of 783 in 2014.[1] This number represents an increase of 27.5 percent over similar breaches reported in 2013, and pushes the total number of U.S. data breach incidents tracked since 2005 to 5,029 reported incidents involving over 675 million estimated records.[2]

For example, in January 2014, Target revealed that it had been the victim of a computer hack through which the contact information of 70 million individuals and information relating to 40 million credit and debit card accounts were stolen.[3] In early 2015, Anthem announced that a cyberattack had compromised the personal information of almost 80 million individuals, including names, dates of birth, Social Security numbers, health care ID numbers, home addresses, email addresses, and employment information.[4]

> Even if no consumer data is impacted by the breach, the impact of a B2B breach can result in tremendous losses to a company.

In large part, it is the number of consumers affected that has led to the increased media onslaught that follows these types of B2C breaches, as well as the call to arms for legislative changes to address these security issues across industries. It is no coincidence that the Obama Administration has made consumer data protection a priority with its proposed data protection act, which will, among other things, require companies to publicly disclose a data compromise within 30 days of it occurring.[5]

In the midst of all this focus on consumer data protection and B2C breaches, however, the media and the Legislature have largely ignored data privacy breaches that are not directly consumer-facing privacy concerns—so-called "business to business," or "B2B" breaches. Such breaches tend to occur quietly, for two main reasons: (1) there are currently no overarching statutory obligations to report data breaches that do not involve statutorily defined categories of personally identifiable information (PII) belonging to consumers; and (2) it is in a company's best interest to keep breaches of this nature (really, any breaches at all) quiet, so as to prevent

JOSEPH V. DEMARCO *is a partner at DeVore & DeMarco and previously served as an assistant U.S. attorney for the Southern District of New York, where he founded and headed the Computer Hacking and Intellectual Property Program.* URVASHI SEN *is counsel at DeVore & DeMarco.*

the public airing of their potential security flaws.

It is also for these reasons that companies tend not to focus their attention, and their resources, on B2B breach scenarios. It is easy to understand why a B2C breach, which can so directly affect a company's bottom line in a much clearer and more quantifiable manner through public notification and media involvement, is generally where companies put their best thinking and resources. However, to ignore the potential damage that B2B breaches can cause would be a huge mistake. Indeed, companies can go a long way toward protecting themselves from B2B data breach incidents by implementing two simple, yet critical, measures: (1) retaining expert privacy counsel to perform due diligence on potential business partners and vendors, and (2) ensuring that vendor and other business contracts contain key clauses addressing potential cybersecurity incidents—in particular, arbitration clauses that cover data breaches.

B2B Breaches

While it is certainly in neither party's interest in a B2B data breach to air its grievances publicly, this does not mean that such situations are simple affairs that are quickly and painlessly resolved. In fact, the opposite is most likely the case—without regulatory or statutory parameters to inform the discussion, and without a direct public fallout to steer companies in the right direction, these types of "quiet" breaches can result in very contentious disputes that may drag on and become difficult to resolve.

In one public example of just how far the fallout from a B2B breach can extend, it was reported in March 2014 that a security breach had impacted the e-commerce platform of Createthe Group (CTG), a digital luxury agency that provides e-commerce solutions to a number of recognizable brands in the retail and fashion space, including Calvin Klein, H&M, Hugo Boss, Louis Vuitton, and many more.[6] CTG ultimately retired its e-commerce platform and exited the e-commerce space altogether (although the security breach was not cited specifically by CTG as a reason for this decision).[7] Notably, in this case the security breach resulted in the alleged compromise of credit card numbers belonging to customers of the various brands CTG represented,[8] no doubt one of the reasons why the breach was reported in the press at all.

Even without a public media backlash, however, it is not difficult to imagine how damaging a B2B data breach incident can be to a company. A compromise of a company's systems, whether through malware received from a vendor or business partner, or through a breach of such a third party's own security systems, consumes the time, energy, and resources of an organization. Even if no consumer data is impacted by the breach,[9] the impact of a B2B breach can result in tremendous losses to a company, including the costs involved in assessing the breach itself, which often can encompass its impact on the company's systems and data, determining and implementing solutions necessary to prevent such an incident to future, spending employee and attorney (in most cases, outside counsel) hours interfacing with the third party responsible for the breach, and managing any reputational damage that may have occurred.

Pre-Contract Due Diligence

One important step a company should take prior to entering into an agreement with a business partner or vendor is to ensure that these third parties follow robust, industry-appropriate security and privacy protocols. What these protocols should be will vary greatly depending on the industry and the size of the third party in question. As such, it is essential that each company contemplating a third-party business relationship retain outside, expert counsel to guide them in this process. The amount of money at stake in each business relationship and the level of data connectivity that will result between the company and the third party will determine how much due diligence is necessary prior to entering into a contractual relationship.

Smaller, simpler associations may only require a basic review of the third party's policies and procedures, whereas for more complex and long-term relationships, a more robust

vetting of the third party's cybersecurity policies and protocols may be appropriate. In all cases, the vetting should be done under counsel privilege to the maximum degree permitted by law.

While such due diligence may, on its face, appear arduous, in fact this type of "pre-screening" not only goes a long way toward preventing a potential external security breach that may affect the company, but also sends a very clear message about the level of importance the company places on cybersecurity matters. This can often be a critical deterrent to a third party that may ordinarily choose to play fast and loose with cybersecurity best practices.[10]

Contracts and Arbitration

Another key strategy companies can employ in protecting themselves from potential B2B data breaches is to ensure that contracts with vendors and business partners specifically address cybersecurity matters, from preventative measures, to risk allocation and dispute resolution in the event of a data security breach.

As a preliminary matter, contracts should outline the data security procedures and protocols that the third party agrees to comply with. What these procedures should be will, ideally, become clear in the due diligence phase discussed above. Contracts should also address the procedures that should be followed in the event of a security breach and how risk in that context should be allocated.

Specifically, companies should ensure that (1) the third party is contractually obligated to report any security incidents in a reasonably prompt manner to the company; (2) the contract includes a clause allocating risk for certain basic types of data breach incidents; (3) the contract addresses indemnification in the data breach context; and (4) the contract includes a broad-form arbitration clause covering all disputes, including disputes relating to data security and privacy matters, and data breaches in particular.[11]

Arbitration affords parties the ability to elect in advance whether to have the arbitrator (or arbitrators) issue a bare, standard award or a reasoned award, which has implications relating to delay, expense, and susceptibility to vacatur.

An arbitration clause is, in our view, a critical component to handling data security breaches in B2B relationships. There are undoubtedly numerous advantages to companies across various industries that choose to arbitrate, rather than litigate, their contractual disputes, regardless of the subject matter of the dispute itself. However, B2B data breach incidents actually present what appears to be the perfect case for the use of arbitration clauses.

First, arbitrating a B2B security incident is more likely to result in a speedier, more efficient, and less costly resolution, not least of all because the evidentiary hearing can proceed uninterrupted, hour-to-hour, on sequential days as needed, as opposed to courtroom proceedings with myriad interruptions and off-days. Additionally, pre-hearing procedures such as discovery and motion practice are streamlined. This frees up company resources to address and rectify the root problems that resulted in the breach, particularly when preceded by mediation, as is generally recommended by the various arbitration associations.[12]

Notably, the efficiency of an arbitration proceeding can be greatly increased by carefully negotiating contractual agreements between parties, such as including a "stepped" arbitration clause, which requires the parties to engage in meaningful mediation prior to entering into a formal arbitration proceeding, and an indemnification clause that covers various security incident scenarios. Here, too, having knowledgeable, expert data privacy counsel to review contracts with third parties for data security issues will go a long way in preventing long and messy disputes when breaches do occur.

Second, an arbitration not only can ensure that legitimate subject-matter expert arbitrators, with all the technical qualifications necessary to understand complex data security and privacy

matters, will resolve the matter, but also eliminates the possibility that an emotional jury, panicking at the prospect of potential effects on consumers from the breach and ill-equipped to comprehend the technical nature of the subject matter, will be the ultimate decision-makers. Additionally, arbitration affords parties the ability to elect in advance whether to have the arbitrator (or arbitrators) issue a bare, standard award or a reasoned award, which has implications relating to delay, expense, and susceptibility to vacatur.

Third, arbitration proceedings can be kept confidential, whereas courtroom proceedings typically cannot be, even if a jury is not involved. This is a key factor for companies navigating a security breach incident, particularly in the current climate of intense scrutiny facing reported breaches. In many cases, it is a tremendous uphill battle to recover from the reputational damage that can result from the public revelation of a data breach, for both parties involved—so much so, that without the option of a confidential arbitration, companies may choose to forgo dispute resolution, swallowing their losses instead. Arbitration provides an ideal environment to ensure that such situations do not arise.

Fourth, arbitration affords far greater finality of decision than court proceedings, where appellate possibilities abound. In data breach disputes, this finality allows both parties to put the dispute behind them quickly, and focus their energies on rectifying the breach and working toward preventing future incidents.

Top of the Agenda

Ultimately, in this current environment of record-high breaches and, undoubtedly, record-high scrutiny of companies impacted by breaches, it is in each company's best interest to put cybersecurity at the top of the agenda, regardless of whether or not consumer data is likely to be implicated in a security incident. Preventive and protective measures can go a long way toward saving a company from catastrophic losses, both financial and reputational.

1. See "Data Breach Reports, Dec. 31, 2014," Dec. 31, 2014, available at http://www.idtheftcenter.org/images/breach/DataBreachReports_2014.pdf.

2. "Identity Theft Resource Center Breach Report Hits Record High in 2014," Jan. 12, 2015, available at http://www.idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html.

3. See "Data Breach FAQ," https://corporate.target.com/about/shopping-experience/payment-card-issue-faq.

4. See "Anthem Facts," last updated May 8, 2015, https://www.anthemfacts.com/; see also "State Breakdowns: Anthem Breach by the Numbers," Feb. 26, 2015, available at http://www.scmagazine.com/victims-of-the-anthem-breach-stretch-across-multiple-states/article/400489/.

5. "Fact Sheet: Safeguarding American Consumers and Families," Jan. 12, 2015, available at https://www.whitehouse.gov/the-press-office/2015/01/12/fact-sheet-safeguarding-american-consumers-families.

6. "American Express Customers Receiving New Breach Notifications," June 20, 2014, http://www.csoonline.com/article/2365803/data-protection/american-express-customers-receiving-new-breach-notifications.html.

7. "Fashion Firms Probing Alleged Data Breach," March 26, 2014, http://www.zeereport.com/breaking_news/4023-Fashion_Firms_Probing_Alleged_Data_Breach.html.

8. "American Express Customers Receiving New Breach Notifications," supra note 6.

9. Notably, it is also possible that a B2B or other type of breach will impact certain customer data, but not the types of data that trigger reporting obligations. For example, in New York (and many other states), name, date of birth, and address information, although considered "personal information," are not, standing alone, "private information" that, if compromised, requires notification of either individuals impacted or governmental agencies. See N.Y. GBS. Law §899-aa.

10. Of course, it is also crucial for companies to ensure they have appropriate cybersecurity insurance coverage that will protect them from security incidents prior to entering into contracts with third parties. This is not an easy task—all too often companies purchase expensive products that are peppered with loopholes, either rendering the coverage ineffective even in some of the most basic breach scenarios, or requiring policy modifications in order to become effective. Legal expertise, through outside data privacy counsel, can be critical here to ensure that the most cost-effective, robust policy is purchased, and that it appropriately covers B2B data breaches.

11. There are a range of reasons why arbitration clauses may be beneficial for all business-to-business matters. While a discussion of those reasons is beyond the scope of this article, we note that broad-form arbitration clauses are, at the very least, procedurally preferable. This is because carving up disputes into different silos for different treatment can be incredibly problematic and inefficient, particularly if parties are forced to arbitrate certain claims and litigate others (and, indeed, to go to court to determine what disputes are covered by the scope of the arbitration clause).

12. For example, under the American Arbitration Association Rules, parties must mediate disputes for claims in excess of $75,000 unless one of them actively opts out of the mediation process. See American Arbitration Association's Commercial Rules and Mediation Procedures, Rule 9.