B2B Cyber Breaches:
How an Arbitration Clause Can Help

The simplest precaution that a business can take for mitigating the financial impact from a data security breach is to insert an arbitration clause including causes of action arising out of data breaches in contracts with its vendors and business partners.

Much has been written about the complicated tech aspects of ensuring the cybersecurity of a company's data and websites.

That is not the focus of this article, which is that ***arbitration can be instrumental in lessening the financial impact once a compromise occurs,*** specifically in business-to-business (B2B) cases. Inserting a pre-dispute arbitration clause in business contracts is the quickest way to enable the process.

A 2015 global survey of top managers and IT professionals in 5500 companies reported that 90% of those businesses had a security incident, and *third-party failure of suppliers or contractors was ranked as the most expensive security breach.*[1] Third-party errors include all manners of compromise on the part of the contractor or supplier—its computers or servers, its methods of disposal, and errors by its employees.

Major Consequences of a Data Breach[2]

1. Loss of access to business-critical information
2. Damage to company reputation
3. Temporary loss of ability to trade

The rest, in order

- Loss of contracts and/or business opportunities in the future
- Costs associated with professional help to remedy loss (e.g., legal costs)
- Cost of additional software and/or infrastructure to prevent future problems
- Competitors obtaining previously confidential data (e.g., intellectual property, financial, or strategic.)
- Financial losses caused by reimbursing or compensating clients
- Damage to credit rating

The cost of a compromise of sensitive data could include the derailment of a merger or acquisition, upending the pricing of a business negotiation, and the loss of valuable research and development.

Why Arbitration—Not Litigation

In *Strategies for Navigating Business-to-Business Data Breaches,* the authors assert that an arbitration clause is "a critical component to handling data security breaches in B2B relationships," and that "B2B data breach incidents actually present what appears to be the perfect case for the use of arbitration clauses."[3] Why?

- **Arbitration gets businesses back to business quickly and efficiently,** avoiding court delays and lengthy, costly pre-hearing procedures. A company stricken with a data breach is in a time-sensitive position and can use its resources better to find and remedy the source of the breach.
- **The confidentiality offered by arbitration**—as opposed to the public nature of litigation—is vital. Disclosure of a company's data breach could be catastrophic to its reputation. Depending on the nature of the breach, companies may be required to disclose certain aspects of the data breach, but the arbitration process allows for the dispute resolution process between businesses to be confidential.
- **Arbitrators with subject-matter expertise**—as opposed to judges and/or juries without—are particularly important for data breach cases that hinge on in-depth understanding of the technical aspects involved. The AAA roster, for example, is well represented by arbitrators with expertise in cyber security and data breaches.

Third-Party Breach Cases in Point

A cybersecurity firm

The publicly disclosed hack on the internal network of a third-party contractor, an international supplier of cybersecurity platforms to individuals, companies, and governments, was one of the biggest security breaches in 2015.[4] The company confirmed the safety of its clients and partners and that there was no impact on the company's products, technologies, and services.[5] If that were not the case, the financial ramifications to their customers would be enormous.

Law firms

Law firms have access to vast amounts of confidential information—business strategies, pending deals, mergers and acquisitions, corporate secrets, and intellectual properties—of the corporations and banks that they represent. The FBI issued a warning in 2011[6] and again in 2013[7] that law firms were targets of hacking. Major law firms that represent Wall Street banks and Fortune 500 companies suffered data breaches in 2015.[8] "A growing number of big corporate clients are demanding that their law firms take more steps to guard against online intrusions that could compromise sensitive information as global concerns about hacker threats mount."[9] General counsel would do well to insert an arbitration clause in their contracts with outside law firms to help mitigate the financial impact involved in resolving disputes between the business and outside law firm in the event that the law firm's site is infiltrated.

Footnotes

(1) "Damage Control: The Cost of Security Breaches IT Security Risks Special Report Series 2015," Kaspersky Lab. https://usa.kaspersky.com
(2) *Ibid.*
(3) Joseph V. DeMarco and Urvashi Sen, "Strategies for Navigating Business-to-Business Data Breaches," http://www.newyorklawjournal.com, (July 6, 2015)
(4) Sarah Kuranda, "The 10 Biggest Data Breaches of 2015, www.crn.com, (December 21, 2015)
(5) Eugene Kaspersky, "Kaspersky Lab investigates hacker attack on its own network," www.kaspersky.com. (June 10, 2015)
(6) Sue Reisinger, "Experts: GCs Are Aghast over Hacks at Top Law Firms, www.corpcounsel.com, (March 31, 2016).
(7) "FBI Again Warns Law Firms about the Threat From Hackers," ridethelightning.senseient.com, (February 4, 2013)
(8) Nicole Hong and Robin Sidel, "Hackers Breach Law Firms, including Cravath and Weil Gotshal," www.wsj.com, (March 29, 2016)
(9) Matthew Goldstein, "Law Firms are Pressed on Security for Data," http://dealbook.nytimes.com (March 26, 2014)