LOS ANGELES & SAN FRANCISCO
Daily Journal
www.dailyjournal.com
FRIDAY, JANUARY 6, 2017

PERSPECTIVE

It's the most wonderful time of year... FOR CYBERCRIMINALS

By Daniel B. Garrie
and Adrienne Publicover

It's the most wonderful time of the year … for cybercriminals. Black Friday, Cyber Monday and now the January clearance sales present an opportunity for a cyberattack. It has been reported that up to 89 percent of retailers have experienced a data breach in the past two years. While it is easy to imagine the risks to online retailers, data shows that brick and mortar merchants are equally affected.

But it is not just retailers who are under attack. Indeed, it is rare to open a newspaper and not find an article about a recent data breach, as the threat affects nearly every industry. The International Trends in Cybersecurity report from CompTIA found in 2016 that nearly three out of four organizations globally have been attacked by at least one security breach or incident in the past year.

As the number and severity of data breaches have increased in recent years, there has been a corresponding rise in data breach litigation in courts across the country. There are many drawbacks to litigating cybersecurity claims, including time, cost and uncertainty. While the time and cost factors associated with data breach litigation may vary, the legal complexity of most data breach situations, which require relegating legal fault and then aggregating sufficient proof of liability, means that it will likely take millions of dollars and several years to reach resolution. And, during this protracted time period, the uncertainty of the ultimate litigation outcome negatively impacts plaintiffs and defendants. To help avoid these drawbacks, all parties should begin considering arbitration as an alternative to litigation.

Many cybersecurity insurance policies contain written procedures mandating that disputes be resolved through arbitration. This should not be cause for alarm, as there are many potential advantages of arbitration in data breach litigation.

First, the legal landscape in the world of cybersecurity is ever-evolving and uncertain. And in litigation where personal financial or health information arguably has been compromised, the adage that bad facts make bad law may never be truer. Fortunately, in arbitration, unlike a court proceeding, there are opportunities to preserve confidentiality, thereby reducing negative publicity and accompanying reputational damage.

> Many cybersecurity insurance policies contain written procedures mandating that disputes be resolved through arbitration.

Second, arbitration promises a less lengthy and less expensive process for both parties. There generally is greater speed to a decision, which can save anywhere from months to years off the normal trajectory of a litigated case. Similarly, arbitrators can more efficiently address procedural issues, such as standing, and advance more quickly to the merits of the dispute. Discovery also is more limited and controlled in arbitration than in traditional litigation. Less time and more control in the context of litigation typically leads to reductions in legal fees and costs.

Finally, arbitration allows the parties to select their arbitrator or arbitration panel. In the data breach context, the right to appoint the fact-finder can be incredibly important. Data breach cases are complicated, very technical and can require years of experience to truly understand what happened, why it happened and what harms may (or may not) result. Often these technical complexities may be accompanied by intricate insurance coverage issues. A competent arbitration panel can help cut through the many issues in a quick and easy manner, help focus discovery on the substantive issues and ensure that the parties do not waste time and resources fighting over non-substantive issues.

Black Friday, Cyber Monday and now the January clearance sales present an opportunity for a cyberattack. It has been reported that up to 89 percent of retailers have experienced a data breach in the past two years.

New York Times

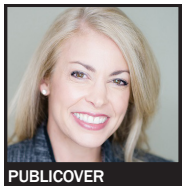
Arbitration is not without its potential for downside. There is minimal (if any) precedential value to an arbitration award, which means that the current uncertainties in cybersecurity law may not get resolved any time soon. There also is a very deferential standard of review for arbitration awards. While this promotes finality and avoids protracted and expensive appeals, it also means that mistakes may go uncorrected. This is yet another reason why it is important to select the best arbitrators for your case.

As the number and severity of data breaches continue to increase, litigants should begin to look beyond the courthouse for ways to efficiently deal with data breach claims. The existing difficulties in litigating these claims hurts both consumers and companies. Arbitration holds the promise of focusing issues, reducing the immense expense of discovery, and eliminating the cost of hiring experts to educate judges on the technical and insurance issues that permeate data breach litigation. For all these reasons, arbitration deserves careful consideration as a more efficient, streamlined and cost-effective method for resolving data breach disputes.

Daniel Garrie *is an arbitrator, forensic neutral and technical special master at JAMS, available in Los Angeles, New York and Seattle. He is executive managing partner of Law & Forensics LLC, and head of its computer forensics and cybersecurity practice groups, with locations in the United States, India and Brazil. He can be reached at dgarrie@jamsadr.com.*

Adrienne Publicover *is a JAMS panelist based in Northern California. She has counseled domestic insurers and brokers, as well as the London market, in litigation matters in state and federal courts throughout the country. She can be reached at apublicover@jamsadr.com.*


GARRIE


PUBLICOVER