Lessons Learned: Vendor Sued in Class Action Suit for Security Misses

By Eric Begun
King & Fisher

You're thinking that something about the title of this post sounds familiar, right? Information technology (IT) vendors and third party service providers have been in the spotlight for security breaches for some time (see, for example, vendor-based security lapses affecting Target, CVS, and Concentra, as just a few), and it doesn't sound surprising that an IT vendor has been sued related to a security incident. After all, whether you're an IT vendor or an IT customer, if you draft or negotiate contracts for a living, these situations are what you try to contract for, right?

Right…but…the recent federal class action suit filed in Pennsylvania against Aetna and its vendor surfaces several new privacy and security considerations for vendors and their customers. The vendor in question was not an IT vendor or service provider. Instead, the plaintiff's allegations relate to Aetna's use of a mailing vendor to send notification letters to Aetna insureds about ordering HIV medications by mail. According to the complaint, the vendor used envelopes with large transparent glassine windows – windows that did not hide the first several lines of the enclosed notification letters. The plaintiff asserts that anyone looking at any of the sealed envelopes could see the addressee's name and mailing address – and that the addressee was being notified of options for filling HIV medications. As a result, the vendor and Aetna are alleged to have violated numerous laws and legal duties related to security and privacy.

For all vendors and service providers, but especially those that don't focus primarily on privacy and security issues, the Aetna complaint is enlightening. To these vendors and service providers, and to their customers: Do your customer-vendor contracts and contract negotiations contemplate what Aetna and its mailing vendor may not have?

- Do your contracts for non-IT and non-healthcare services fully consider the risk of privacy and security litigation? A noteworthy facet of the Aetna case is that the mailing vendor was sued for privacy and security violations that were not exclusively due to the customer's acts or omissions. That is, while the contents of the mailer certainly were key, the vendor's own conduct as a mailing services provider (not an IT or healthcare provider) was instrumental in the suit being filed against the vendor (and Aetna). Vendor services that previously didn't, or ordinarily don't, warrant privacy or security scrutiny, may, after all, need to be looked at in a new light.
- Do your contract's indemnification and limitation of liability clauses contemplate the possibility of class action litigation? Class action litigation creates a path for plaintiffs to bring litigation for claims that otherwise could not and would not be brought. Class action litigation against data custodians and owners for security breaches is the norm, and the possibility and expense of class action litigation is frequently on the minds of their attorneys and contract managers who negotiate contracts with privacy and security implications. But, for vendors and service providers providing arguably non-IT services to these customers – the idea of being subject to class action litigation is often not top-of-mind.
- Before entering into a contract, have you considered whether the specific vendor services being provided to the particular customer in question implicate laws you

hadn’t considered? Vendors that operate in the information technology space – and their customers – generally are well-aware of the myriad of privacy and security laws and issues that may impact the vendors’ business, including, as a very limited illustration, the EU General Data Protection Regulation, HIPAA, New York Cybersecurity Requirements, Vendors that aren’t “IT” vendors (and their customers), on the other hand, may not be. For example, the Aetna mailing vendor may not have contemplated that, as alleged by the Aetna plaintiff, the vendor’s provision of its services to Aetna would be subject to the state’s Confidentiality of HIV-Related Information Act and Unfair Trade Practices and Consumer Protection Law.

- Have you considered which specific aspects of vendor services may directly impact potential legal liability, and have you adequately identified and addressed them in the contract? No, this is not a novel concept, but it nonetheless bears mention. A key fact to be discovered in the Aetna litigation is whether it was Aetna, or the vendor, that made the decision to use the large-window envelopes that, in effect, allegedly disclosed the sensitive and personally identifiable information. Given the current break-neck pace at which many Legal and Contract professionals must draft and negotiate contracts, however, unequivocally stating in a contract the details and descriptions of every single aspect of the services to be provided is often impractical (if not impossible). But, some contract details are still important.

Whether or not this class action suit is an outlier or is dismissed at some point, consider data security and other privacy and security issues in contracts and how vendor or service provider conduct may give rise to a security breach or security incident.

Join Our LinkedIn Group