The State of Data Breach Litigation and How to Avoid It

By Aaron D. Charfoos and Sean C. Griffin

A recent study by Gemalto revealed that the number of records compromised in data breaches in 2016 increased an astounding 86% over 2015 breaches. This has led to numerous data breach litigations in the civil and regulatory context. What are the major cases and trends from 2016? And what can organizations do to try to reduce their risks of breaches and litigations?

Key Legal Developments and Trends in 2016

FTC Enforcement

The FTC has recently worked to expand its jurisdiction to include prosecuting companies that suffer data breaches. This effort got a boost when the FTC brought an action against Wyndham Hotels after Wyndham suffered a data breach. The SEC alleged that Wyndham's supposedly sloppy cybersecurity practices violated the Federal Trade Commission Act (FTCA). Wyndham challenged the FTC's jurisdiction to bring such an action and lost before the U.S. Court of Appeals for the Third Circuit in 2015. Essentially, the Third Circuit held that Wyndham engaged in "unfair" cybersecurity practices that "unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft." These practices included failing to use firewalls, storing unencrypted payment card information, not fixing known security vulnerabilities on the company's servers, not changing the default user IDs and passwords for those servers, and not requiring complex, difficult-to-guess passwords. *See*, *FTC v. Wyndham Worldwide*, — F.3d —, No. 14-3514 (3d Cir. 2015).

Fresh off this victory, the FTC prosecuted LabMD, a clinical laboratory whose billing manager had downloaded peer-to-peer software onto her work computer that allowed others to search LabMD's computer for files. Tiversa, a data security company, was conducting peer-to-peer searches for precisely this sort of vulnerability, so it could notify a company of its vulnerability and offer its services to remedy it. Tiversa discovered LabMD's vulnerability but could not interest LabMD in retaining it. Spurned by LabMD, Tiversa notified the FTC of LabMD's vulnerability, and the FTC brought an action against LabMD for a violation of the FTCA, just as with the Wyndham case. The FTC won the administrative hearing, where the agency ordered LabMD to implement a number of compliance measures. The district court refused to stay the order.

The U.S. Court of Appeals for the Eleventh Circuit reversed. Due to the circumstances of the data breach's discovery, the Eleventh Circuit held that the alleged harm resulting from the FTCA violation was both "intangible" and "unlikely to occur." The court also noted that LabMD was out of business, and thus, forcing it to comply with the FTC's restitution order would constitute irreparable harm. *See*, *LabMD v. FTC*, No. 16-16270 (Nov. 10, 2016).

Either the FTCA prohibits sloppy data security practices, or it does not. Given the tension between the Wyndham case and the LabMD case, the Supreme Court may have to intervene. Expect the resolution to turn on the loss the data breach actually caused — if the FTC can show concrete damages that are substantially likely to occur, it will probably prevail.

Federal Defend Trade Secrets Act

In 2016, President Obama signed into law the Federal Defend Trade Secrets Act (FDTSA). The FDTSA prohibits the unauthorized taking, downloading, uploading, and transmittal of trade secrets with intent to convert said trade secrets and knowing that the offense will injure the trade secrets' owner, as well as the knowing receipt and possession of stolen trade secrets. It broadly

defines "trade secret" to include "all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing."

The FDTSA also grants a private right of action to remedy its violation. A plaintiff may obtain a court seizure of property "to prevent the propagation or dissemination of the trade secret that is the subject of the action." The Act also provides for other injunctive relief and monetary damages of up to $5 million for organizations.

Significantly, the FDTSA makes exceptions for whistleblowers. A whistleblower can disclose a trade secret confidentially to a government official, provided that the disclosure is made solely for the purpose of reporting or investigating a suspected violation of law. A whistleblower may also disclose a trade secret under seal in an anti-retaliation lawsuit.

So far, the FDTSA has found its primary use in cases where a former or soon-to-be-former employee allegedly steals a company's data for his or her own use in a new company. A typical FDTSA case bundles a FDTSA claim with a state cause of action, an unfair competition claim, and a claim for breaching an employment contract's confidentiality or non-compete provisions. Some observers believe that the Act also provides a weapon for outside hacking, including hacking by a foreign entity.

Supreme Court Decision in Spokeo

Last year, the U.S. Supreme Court issued a decision in *Spokeo, Inc. v. Robins*, 136 S.Ct. 1540 (May 16, 2016). Spokeo, a "people search engine," stood accused of disclosing incorrect information about Robins, the plaintiff, in response to a search. Robins filed suit under the Fair Credit Reporting Act, but ultimately, the Supreme Court found that he lacked standing to pursue his claim, because he had not suffered a sufficiently concrete injury-in-fact.

This holding calls into question many data security cases. Courts have construed many data security statutes (as well as data security-adjacent statutes such as the Telephone Consumer Protection Act (TCPA)) to allow statutory damages without an actual injury. *Spokeo* casts doubt on those cases. Recent post-*Spokeo* cases suggest that courts are looking at the standing issue more carefully. For example, *Gubala v. Time Warner Cable*, 846 F.3d 909 (Jan. 20, 2017), the U.S. Court of Appeals for the Seventh Circuit held that the failure to destroy personally identifiable information, as required by the Cable Communications Policy Act, did not by itself confer standing. On the other hand, both the Second and the Ninth Circuit ruled post-*Spokeo* that the recipient of a robocall or robotext, merely by receiving the call, showed sufficient harm to confer standing. Given the specific, consumer-friendly language of the TCPA, *Gubala's* more stringent standing requirements will likely point the way for most federal data security cases. Combined with the LabMD decision, federal case law may be moving toward a "no harm, no foul" view of data breaches — at least from a government enforcement perspective.

Best Practices to Reduce an Organization's Data Breach Risks

With so much risk to a company following a data breach, are there steps that organizations can take now to either reduce the risk of a data breach or lessen its impact? Absolutely. Organizations that make an investment in their privacy and data security compliance programs now can reap significant benefits. So what can companies do?

Below are steps that organizations can take before any breach occurs to minimize the risk of litigation, enforcement actions and other business risks. The key is to identify where an organization's data resides, where it moves to, and what to do in the event of a breach.

Keep an eye on employees. Most data security events do not result from a nefarious foreign hacker typing quickly on a keyboard in a dark basement, probing for weaknesses. Most occur because a company employee, for one reason or another, has stolen company information for his or her own use. In one recent case, a company executive combed through employee emails looking for company malfeasance, apparently to use as leverage against his company in the event the company tried to terminate him. In another criminal matter out of New York, a law firm paralegal, feeling unappreciated, tried to sell a partner's trial plan to his opponent. Several cases under the recent FDTSA involve departing employees allegedly stealing trade secrets to use in their new jobs.

Understand your data. Organizations must understand what information they collect (or receive from third parties), how they use it, how they protect it, whether they share it, and how long it is kept. It is also critically important to understand where it is stored and how it is moved because national and international law (including data localization laws) increasingly deal with data transfers. Today, vast amounts of data are transferred between continents (including by employees who are traveling globally with laptops, smartphones, and tablets that are communicating back with the organization). Creating and maintaining data inventories and data flows are critical to staying on top of this evolving landscape.

Understand your legal and regulatory landscape. It is not simply enough to know where a company's headquarters or offices are located to understand what laws they are subject to. Today, data can be easily and cheaply stored anywhere in the world and transferred with a single keystroke. This subjects organizations to many different legal regimes. With so many players, it is very easy for any organizations to stray into regulated space. Therefore, organizations must regularly identify what laws and regulations apply, what they require, and be constantly vigilant as they change over time.

What do your privacy statements say? It is not uncommon for organizations to have a number of different internal privacy policies and external privacy statements. Organizations should periodically review their privacy statements and policies to ensure that they accurately reflect the organization's business and are consistent with any relevant laws.

Do you really have consent? Obtaining consent from data subjects can be a useful tool for organizations. However, particularly under the EU's newly passed General Data Protection Regulation (GDPR), that consent must be clear and unambiguous. Therefore, organizations should ensure that they are getting proper consent.

Are your certifications up to date? Many organizations rely on certifications to both attract customers and reduce their legal risk. Make sure that you keep them up to date.

Be careful what you promise. Several recent enforcement actions emphasize that organizations must be very careful what they promise their customers (whether on their website, in marketing materials or elsewhere). These statements are likely some of the most difficult to police, but pose some of the greatest risks.

Do you have the right technical safeguards? Depending on the kind of data you have, and where it is located, federal and state laws may dictate what kinds of technical safeguards need to be in place. Similarly many industry standards, such as PCI DSS, include stringent technical requirements. Chief privacy or information security officers, in-house counsel and others will need to work closely with the organization's technical team and vendors to ensure compliance.

Preparing for a Possible Breach

The process of dealing with a data breach should begin long before the breach occurs. Organizations should not be trying to figure out what each state's data breach law is, let alone

whether it applies to them, as a breach is unfolding. Make it a point to regularly review your data breach response plan (or create one) so that it accurately reflects the technical reality of the organization, as well as complies with all of the new changes in the law. The plan should be detailed, in writing, and accessible to all of the key players in the event of a data breach. Your plan should also include the contact information for all of your breach partners, including qualified outside legal counsel, technical data breach response experts, public relations firms and others.

Practice makes perfect. Run mock data breach drills, whether that is a table top exercise or an actual live drill, to ensure that the plan can be implemented as drafted. Are all of the pieces in place for a competent, efficient and manageable response to the breach? Here, outside counsel can be particularly helpful in developing and running the drill and protecting it with the cloak of privilege (in some countries, such a privilege does not attach to communications involving in house counsel). An organization's well-rehearsed response to a breach may play a key role in defending against any future litigation or enforcement actions.

*****

Aaron D. Charfoos (acharfoos@dykema.com) is a member in the Chicago office of Dykema. An accomplished privacy, data protection and patent trial lawyer, Charfoos is also a certified information privacy professional for the U.S. Sector (CIPP/US). **Sean C. Griffin** (sgriffin@dykema.com) is a member in the Washington, DC, office of Dykema. Griffin focuses his practice on commercial litigation, with a specialty in cases involving allegations of breach of contract or fraud.

—❖—