Law Office of Edward E. Sharkey LLC

September 2014

BUSINESS LAW DEVELOPMENTS

Legal updates for entrepreneurs and business owners from the Law Office of Edward E. Sharkey LLC.

Dear Friends of the Firm,

This is the September issue of our firm's newsletter, featuring coverage of legal developments important to business owners and entrepreneurs. You are receiving it because you are a client or have previously solicited legal resources from the firm.

Please let us know what you think.

Very truly yours,

Ed

In This Issue

Do You Need Data Breach Insurance?

In the course of conducting business, many companies acquire customer names, addresses, e-mail, credit card information, and Social Security numbers. This, and any other information by which an individual may be identified or contacted, is known as personally identifiable information ("PII"). Businesses are required to use reasonable care to safeguard PII in their possession.

Even with a good faith effort to meet this standard, a business may find that its stored PII has been compromised by an unauthorized person. Unauthorized access can lead to serious and costly consequences for the business obligated to guard the information. We have written about some of these, including lawsuits by customers and claims by credit and debit card issuers.

Not surprisingly, businesses faced with these types of claims have looked to their general liability insurers to defend and indemnify them. Insurance companies have typically denied that their general policies provide coverage for data breaches, often resulting in additional lawsuits. For example, the general liability insurer of a grocer that suffered a data breach sued the grocer for a declaration that its policy did not cover the data breach because the lost data was "intangible." Similarly, after it suffered a breach, Sony's insurer sued it for a declaration that the breach was not covered because of particular language in the policy and the circumstances of the breach.

Coverage disputes decided thus far leave open the question of when, if ever, a general liability policy would apply to a data breach. Rather than continue to fight it out in court, insurance companies have begun crafting new exclusions to expressly limit data breach coverage and preclude it for third party hacks. As a result, businesses that handle PII must decide whether to purchase separate cyber-insurance to supplement their general liability policies or bear the risk of a data breach.

To make a prudent decision, a business needs to assess its specific risks and the scope of coverage afforded by the policy it is considering. A business with a risk of credit card and account information theft, for example, will need different coverage than a company concerned with disruptions to network access. Each business will want to ensure that any policy affords coverage for all of the harm a data breach might cause, including:

- Protection from third-party claims, including those made by consumers, regulatory agencies, and financial institutions;
- Protection for first-party losses, including legal fees, investigation costs, restoration costs, public relations costs, crisis management, credit monitoring, and possibly extortion costs; and
- Reimbursement for costs incurred after the breach, such as business interruption and lost revenue.

These are complex issues that should be reviewed with an experienced broker. And while the final decision may be to go without special insurance coverage, it is a lot smarter to make that decision based upon an analysis of the risks and costs rather than by inaction and default.

What Data Security Practices Will Get You Sued by the FTC?

The Federal Trade Commission ("FTC"), the agency tasked with protecting consumers, considers itself the "national data security enforcement agency." It has sued multiple businesses that suffered data breaches, contending that their lax data security is legally an unfair business practice. Many dispute the FTC's authority to file such suits. That question is presently pending review in the United States Court of Appeals for the Third Circuit.

In the meantime, the FTC is continuing to sue businesses that have been victimized by data breaches, arguing that their data security was "unreasonable." LabMD, the defendant in one such suit, moved to dismiss the lawsuit because the FTC has never issued regulations to give businesses notice of what "reasonable" security entails. The court rejected LabMD's argument, but it issued an order compelling the FTC to testify about the standards it intended to use to establish that LabMD's security measures were insufficient.

Instead of providing practical information, the FTC testified that whether security measures are

reasonable requires a case-by-case analysis. Rather than directly answer questions concerning specific practices, the FTC referred generally to its publications, including consent orders with prior victims of data breach and brochures, testifying that they amount to a "body of guidance" from which businesses can deduce what is required.

The publications do identify certain practices which the FTC has found to be unreasonable. And from these, businesses can garner information to help form prudent policies concerning data security. The unreasonable practices include:

- Employing a poor username/password protocol, such as using common or known passwords and not requiring users to change passwords periodically;
- Failing to encrypt data;
- Failing to minimize the collection and processing of PII;
- Failing to train employees to safeguard data;
- Failing to manage third-party access to data;
- Disposing of data in an unsecure manner;
- Failing to limit connectivity to a network on which data is stored;
- Failing to use adequate firewalls;
- Failing to test security;
- Failing to take steps to protect against known vulnerabilities or common attacks;
- Not maintaining a system to obtain public feedback; and
- Failing to implement procedures to detect unauthorized access.

The question left open is whether avoiding these practices will be enough in every case to meet the reasonableness standard or to avoid being sued by the FTC.

SEC Sample Audit Is a Useful Tool for All Businesses to Assess Cybersecurity.

The Securities and Exchange Commission ("SEC"), the federal agency tasked with regulating broker-dealers and investment advisers, is in the midst of its own cybersecurity initiative. As part of its initiative, the SEC will examine the cybersecurity of more than fifty securities firms. The goal of the examinations is to gather information that can be used to determine additional steps the SEC should take to protect the integrity of the market system and customer data.

To help firms make their own assessments, the SEC issued a sample list of documents and information that it may request during its examinations. The list highlights data breach risks, such as fraudulent requests made through remote customer access systems, vendors' and business partners' failures to implement sufficient security measures, and internal misconduct.

It also highlights security measures that firms can take to safeguard the data in their possession, including:

- Taking inventories of hardware and software and prioritizing them for protection based on their sensitivity and business value;
- Mapping networks and connections to networks on which data is stored;
- Conducting periodic risk assessments;
- Creating a plan to mitigate the effects of a breach;
- Training employees to safeguard data and auditing compliance with information security policies;

- Restricting access to data so that only personnel who need the data to perform their job functions are able to access it;
- Encrypting data;
- Requiring customer authentication to access online accounts;
- Assessing vendors' cybersecurity policies; and
- Monitoring network and physical environments to detect unauthorized activity or threats.

Although the SEC's focus is on investment firms, all businesses that collect or maintain personally identifiable information are susceptible to the risks it has highlighted. In light of the high costs associated with a breach, every such business should take the time to assess the safeguards it has in place. The SEC's sample examination is a good starting point for a business in any industry to do just that.

ABOUT US

The Law Office of Edward E. Sharkey LLC is a firm of dedicated business and trial lawyers in Bethesda, Maryland, concentrating on business law and commercial litigation. Other areas of practice include pension, securities, negligence/professional liability, and construction law.

In This Issue

Law Office of Edward E. Sharkey LLC
4641 Montgomery Avenue
Suite 500
Bethesda, MD 20814
www.sharkeylaw.com

Tel. (301) 657 8184
Fax (301) 657 8017
Business Hours:
9 a.m. 5 p.m.
Monday Friday

ATTORNEYS

Edward E. Sharkey
Admitted to Practice in
Maryland and Washington, DC

Jeanine Gagliardi
Admitted to Practice in
Maryland and Washington, DC