Law Office of Edward E. Sharkey LLC

Unsubscribe | Update your profile | Forward to a friend

February 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 February 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

While many businesses are proud that they have never wired money to a Nigerian prince, e-mail scammers have refined their game. Here is a summary of a new, more subtle, scheme to divert payments that could trap even a prudent business. It includes a list of very simple, free steps that can effectively protect a business from payment hijacking.

Maryland High Court Re-Affirms Legality of Parental Waivers for Children

Lots of businesses that serve children ask parents to sign a waiver of liability. In a surprise ruling last year, Maryland's intermediate appellate court said they are not effective. A few months later, Maryland's high court said "not so fast." So get out the old permission forms. Parental waivers for kids do work.

One Hurdle in Suing for an Online Review: Finding Out Who Posted It

Most business owners dream of maintaining a positive online reputation. They wish for no negative reviews on websites like Yelp and TripAdvisor. If they do receive a disparaging and inaccurate review, they often question whether they can pursue the reviewer for libel. A case recently decided by the Virginia Court of Appeals reminds us of one of the challenges in taking action against a negative online posting: how to figure out the identity of an anonymous poster [1].

The Virginia case arose when a business sued anonymous reviewers and subpoenaed Yelp for information about the reviewers. Yelp objected to the subpoena. The trial court overruled the objection and entered an order compelling Yelp to produce information concerning the anonymous users. Because Yelp continued to withhold the information, the trial court held Yelp in contempt. Yelp appealed the order of contempt.

On appeal, Yelp contended that the trial court's decision contravened the users' First Amendment rights to free speech. Although it recognized that the right to commercial speech is limited, Yelp argued that the trial court applied the wrong standard to determine whether the reviewers' rights to free speech were outweighed by the business's right to prosecute claims against the reviewers in this particular case.

Yelp endorsed a standard that requires the business to, among other things, proffer evidence of its claims against the reviewers. That would mean offering proof that the posts were, in fact, libelous. The appellate court rejected the standard endorsed by Yelp. In doing so, it relied upon a Virginia law that deems the business's good faith belief in the unlawfulness of the online posting to be enough.

Although the legal standards governing free speech on the Internet are still developing, the standard endorsed by Yelp is more consistent with those emerging from courts in most other jurisdictions. The majority of courts require more than a good faith belief in the unlawfulness of anonymous posts before compelling the disclosure of information concerning the posters.

Some courts apply a standard that requires the business to state a claim that would survive a motion to dismiss [2]. That means filing a complaint against the anonymous reviewer that contains allegations of fact that, if true, would support the conclusions that the review was false, defamatory, and, in some cases, caused harm to the business. In other courts, including those in Delaware and New Jersey, a party seeking to discover the identity of an anonymous poster is required to state a *prima facie* claim against the poster [3]. Stating a *prima facie* case requires more than just alleging

facts that support each element of a defamation claim. It calls for the submission of evidence supporting each element.

Like those in Delaware and New Jersey, Maryland's highest court deemed the *prima facie* standard appropriate for balancing a reviewer's First Amendment right to anonymous speech against a business's right to prosecute tortious speech. It gave the following instruction to Maryland trial courts deciding whether to compel disclosure of information concerning anonymous posters:

- Require the party seeking the information to identify and set forth the exact statements purportedly made by each anonymous poster that are alleged to be actionable;
- Determine whether the complaint has set forth a *prima facie* case against each poster; and
- Balance each poster's First Amendment right to free speech against the strength of the *prima facie* case and the necessity of the disclosure [4].

Even with this guidance, the issue of whether a business will be able to discover the identity of an anonymous poster is complex. Not only does it require the assessment of evidence to determine whether a *prima facie* case has been made, but it also calls for a balancing of the poster's First Amendment right against the strength of the case. When deciding whether to file suit against negative online reviewers, businesses should take into account the time and cost associated with the complexity.

We will continue to monitor the law concerning anonymous speech on the Internet. If you have a question about this or a related issue, please contact our office.

---

[1] At tinyurl.com/k944y3b.
[2] *Columbia Ins. Co.* at tinyurl.com/lcmm46l.
[3] *Cahill* at tinyurl.com/ntolf9j; *Dendrite* at tinyurl.com/q689z9w.
[4] *Independent Newspapers* at tinyurl.com/cd3xcd.

Data Security Basics Every Company Should Know

In the closing weeks of 2013, the massive retail chain Target suffered a data breach. The incident was newsworthy primarily for two reasons: the scope of the breach (an estimated 70 million customers [1] were affected) and the size of the company (Target's revenues exceeded $70 billion in 2012 [2]).

Target's size and wealth led most law and technology experts to assume that its data security measures were robust and cutting-edge. To paraphrase the attitude of those experts: if this can happen to Target, it can happen to just about anyone. Therefore, it is imperative that every business that handles customers' personally identifying information ("PII") implement a data security policy. Target's experience provides a great backdrop for a discussion of how small business owners can protect their companies from the devastating consequences that often follow from a data breach.

Data breach, broadly speaking, refers to a compromise of PII: social security numbers, credit card or bank account numbers, or private health information [3]. In rare cases it can result from a physical trespass, such as the theft of a laptop or storage device, but more frequently, as in Target's case, the breach results from an intentional cyber trespass.

Since the Target data breach was made public, countless lawsuits [4] have popped up all over the country. Though the suits are not identical, most share common theories of recovery, including

negligence and unjust enrichment.

Due to the relative novelty of cyber crime, the law is still evolving with respect to data breach claims. For example, courts in some federal districts have been hostile to unjust enrichment claims (a legal theory that lawyers have used to hold businesses liable for data breaches in cases where negligence would be difficult to prove), while other courts have allowed such claims to proceed. For the time being, businesses should be aware that courts are willing to consider novel theories of liability when it comes to data breach lawsuits and may be willing to hold companies responsible even when their customers have suffered no damages [5].

Lawsuits filed by consumers are far from the only concern for businesses that have suffered a data breach. The businesses' insurers might disclaim coverage under the relevant policies, which would require the business to sue the insurer for coverage. Businesses may also face civil penalties from federal and state government authorities. There also is the prospective cost of legal fees for any claim or investigation not covered by insurance. Finally, there is the potential loss of customer goodwill, which can manifest itself in a shrinking bottom line.

The single most important thing a business can do in order to protect itself is to make sure it is insured against all the harm a data breach might cause. There are various types of insurance policies that might cover businesses in the case of a data breach. Specialized policies, such as crime or cyber insurance, as well as general business liability policies, might offer varying degrees of coverage to a business that has suffered a breach. Small business owners should discuss their policies with their broker to ensure that they will be covered.

Businesses also should implement "reasonable" security measures and policies to prevent against data breaches in the first instance. What is "reasonable" depends on the particular circumstances of the business, including its industry and the sensitivity of the information it maintains. Businesses must have some physical and digital security to guard against the theft of consumers' PII, as well as solid employee training programs in place. For example, in one recent data breach case [6] that settled out of court, the defendant agreed to revise its company-wide information security policy, require its employees to undergo security awareness training, upgrade the physical security at its offices, and upgrade the data security on its devices through the use of encryption software. These steps alone will not immunize a company from suit, but they are a good starting point.

Finally, one of the most interesting aspects of the Target lawsuits will be how the courts address the plaintiffs' claims that Target waited too long to notify them of the breach. This is perhaps the trickiest aspect of the data breach framework. If a business notifies customers too quickly, it risks stifling law enforcement efforts to catch the perpetrators. If it waits too long, it may increase the likelihood that it will be found liable for negligence.

There are many factors that business owners need to consider when seeking to protect their companies. Finding the right insurance policies and establishing training and security measures are important, as are a company's first steps in addressing a breach immediately after it happens. Our firm advises businesses concerning data security. If you have any questions, please give us a call.

---

[1] See tinyurl.com/llr6q8v.
[2] See tinyurl.com/nhcmfjx.
[3] See tinyurl.com/q5o4adq.
[4] See tinyurl.com/o4vj53u.

[5] See tinyurl.com/m3yal4f.
[6] At tinyurl.com/kweh8f2.

Avoiding a New Payment Hijacking Scam

In December, the Seattle office of the FBI issued a warning [1] against a new type of e-mail fraud after three Washington-based businesses were victimized by the scam. The FBI has taken to calling the new type of fraud the "man-in-the-E-mail," which derives its name from the criminals' modus operandi: intercepting e-mails between established business partners and inserting themselves into the e-mail chain. Ultimately, the fraudsters will divert payment from its intended destination – an account belonging to the victim's business partner – to the criminals' own accounts.

The FBI went public with the details of the scam to help businesses avoid being victimized, as well as to collect information from the e-mail data of businesses that think they are being targeted.

The perpetrators that victimized the three Washington businesses were able to intercept e-mails between those businesses and an "established supply partner in China." After they acquired the e-mails, the scammers created a new account that was almost indistinguishable from that of the Chinese supplier and wrote to the Washington businesses pretending to be the supplier. The fraudsters requested that the targets send payment to a new account and averted any suspicion by claiming that they were dealing with an audit. As instructed, the three Washington businesses sent their payments to the foreign bank, and, of course, they never received the goods they were expecting.

In total, the three businesses suffered losses of over $1.5 million. The FBI warns that it is not only buyers that can be victimized: if a supplier routinely sends goods before receiving payment, it can just as easily fall victim to this scam by sending out goods before the fraudsters divert the payment. Thus, *all* companies who communicate via e-mail need to be wary of this scheme and know how to protect against it.

There are simple ways businesses can protect themselves against this type of fraud:

- Ensure that your business has solid employee training and oversight practices in place. They provide built-in checks which can catch simple but very easy to overlook details such as a supplier e-mailing from a new address or asking for payment to be sent to a different account;
- Verify significant transactions, especially those involving business partners outside the U.S., using the "second-factor authentication" method: in addition to e-mail communications, a phone call, or other medium of contact, should be used before completing a transaction;
- Create a company domain (for example, sharkeylaw.com) from which all your business-related e-mail should be sent. Free, web-based e-mail services are often easier to intercept and are easier for criminals to imitate;
- Avoid replying directly to e-mails. Instead, use the "forward" option and enter the recipient's address manually or by copying and pasting from your existing address book; and
- Beware of sudden changes in business practices. If, for example, a longtime business partner suddenly asks you to send a payment to a new account, that should raise a red flag and necessitate a verification – using the second-factor authentication method – that the instructions are legitimate.

The FBI has set up a law enforcement group to collect information to protect against these threats. If you suspect that your business is being targeted, contact law enforcement and report the details of the e-mails to the Internet Crime Complaint Center [2].

Finally, businesses also need to be vigilant when it comes to insuring themselves against these types of losses. Not all insurance policies – even those that are cyber-based or crime-based – will cover this type of fraud, and those that do may be subject to lower policy limits, leaving the business on the hook for a significant portion of the loss.

If you have any questions about how best to protect your small business from scams or fraud of any kind, please give us a call.

---

[1] At tinyurl.com/mkgu2bf.
[2] At www.ic3.gov.

Maryland High Court Re-Affirms Legality of Parental Waivers for Children

There was a big win for businesses that provide services for children. It happened in litigation concerning the enforceability of a parent's release of a child's potential injury claim. We previously wrote [1] about the litigation, which arises out of a child's fall in a play center at BJ's Wholesale Club ("BJ's").

In an August 30, 2012 opinion [2], Maryland's intermediate appellate court held that a release is not enforceable against a child if it is (1) presented by a for-profit, commercial entity that principally serves private interests and (2) is executed by a parent on the child's behalf before the child is injured. The court reasoned that enforcing such releases would contravene the public interest because:

- It might remove businesses' incentive to act with reasonable care;
- Such releases are most often imposed unilaterally without a real opportunity to negotiate;
- Commercial enterprises are more able than children to eliminate hazards and insure against risks that cannot be eliminated; and
- The State has an interest in protecting children.

BJ's petitioned for review by Maryland's highest court, the Court of Appeals. The Court of Appeals agreed to review the matter and recently issued an opinion [3] overturning the decision of the lower court.

The Court of Appeals noted that determining the public interest requires consideration of all of "the circumstances of any given case against the backdrop of current societal expectation." Societal expectation is manifest in the law. The law pertinent to parent-child relationships (1) obligates parents to provide care and support for their children and (2) recognizes that parents' decisions are generally in their children's best interests. For these reasons, the Court concluded that the societal expectation is that parents' decision making with regard to their children is not limited. Accordingly, the Court held that a parent's release of a child's potential injury claim against a commercial entity is valid and enforceable.

Among the pertinent law identified by the Court of Appeals is a statute which authorizes a parent to settle a child's existing claim without judicial interference. The Court of Appeals characterized the first

two considerations identified by the lower court as attempts to distinguish a parent's decision to settle a child's existing claim, which is authorized by statute, from a parent's decision to waive a child's prospective claim. The Court of Appeals opined that, if the two circumstances are to be treated differently, it is up to the legislature to create laws that call for disparate treatment.

Similarly, the Court of Appeals admonished that the lower court's choice to distinguish commercial enterprises like BJ's from non-profit entities is not based in law and, if such a distinction is warranted, it must be created by the legislature. Finally, with regard to the lower court's reliance on the State's interest in protecting children, the Court of Appeals noted that the interest is generally invoked only in situations where a child's parent is unfit or incapable of performing the duties of a parent. This case does not concern such a situation.

Unless it is changed by the legislature, the Court of Appeals' decision is now the controlling law in Maryland, and business owners who provide activities for children may rely upon releases executed by parents.

---

[1] A blog post is available at tinyurl.com/nt3o75h and a newsletter article at tinyurl.com/mavr2qm.
[2] At tinyurl.com/d7ef7cy.
[3] At tinyurl.com/oj9zb3o.

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.

Disclaimer: This message and any attachments hereto cannot be used for the purpose of avoiding penalties that may be imposed under the Internal Revenue Code.

This publication is provided for information purposes. It should not be taken as legal advice for a specific situation. If you need legal advice concerning a business or litigation matter, please seek legal counsel or contact us for a consultation at (301) 657-8184.

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

Attorney Bios

Publications

Resources