AN ILLINOIS LAW FIRM

GETTING DOWN TO BUSINESS

HEYL ROYSTER
BUSINESS & COMMERCIAL LITIGATION NEWSLETTER

 Fall 2015

WELCOME LETTER

Dear Friends, Clients and Colleagues:

In this issue of our newsletter, we cover several important topics. First, Steve Ayres discusses the pitfalls of uninvited faxes. Next, Chrissie Peterson examines the risks of doing business in a digital world. Finally, Stacy Crabtree examines a recent decision rejecting Self-Critical Analysis privilege.

We are excited to announce our next seminar, "Avoiding Litigation – How to Stay Out of Court, or What to Do Now to Win Quickly Later." This two-hour seminar will cover a variety of topics on avoiding litigation and what to do to help you prepare in the case litigation arises. This seminar will initially be offered in Rockford on December 4, 2015 and will be available at our other offices around the state in the New Year.

Be sure to watch for your invitation to attend this insightful seminar at our various locations. We hope you will be able to join us to discuss these important topics.

Our Business and Commercial Litigation team at Heyl Royster hopes that you are enjoying the Fall season.

Mark A. Ludolph
Editor

A POTENTIAL BUSINESS NIGHTMARE: THE TCPA AND UNINVITED FACSIMILES

By: Steve Ayres, sayres@heylroyster.com

All businesses should be aware of the existence of the Telephone Consumer Protection Act of 1991, the "TCPA." This statute, as enforced by the Federal Communications Commission, makes it unlawful to fax an unsolicited advertisement unless the sender has an established business relationship with the recipient, the recipient consents to such communication, and the advertisement contains an opt-out notice. 47 U.S.C. § 227(b)(1)(C) (2000). The TCPA applies not only to faxed advertisements, but also to unwanted text messages and the use of an automatic telephone dialing system in a manner prohibited by the statute.

The TCPA has formed the basis for a myriad of class action lawsuits, because it allows for statutory recovery of $500 for each and every violation of the statute, with treble damages if the defendant willingly and knowingly committed the violation. Standing alone, this $500 figure appears minimal, but class action plaintiff's attorneys have "clients" on the lookout for uninvited faxes and if one is received, through the use of class action lawsuits and discovery, the TCPA allows those attorneys to seek discovery and identify each and every similar fax in an effort to expand the class of recipients. The implications can be immense-in one case, an Illinois estate planning attorney sent more than 200 CPAs a targeted monthly fax called the "Daily Plan-It," which purported to give advice but which also contained information about the attorney's services. Based on a finding that over 8000 such faxes were sent over a period of several months, the federal trial judge granted summary judgment in favor of the class plaintiffs in an amount exceeding $4 million, and that award was upheld on appeal by the 7th Circuit. *Ira Holtzman, C.P.A. & Assocs. v. Turza*, 728 F. 3d 682 (7th Cir. 2013).

continued on next page

Because many small and medium businesses cannot shoulder the effects of such a large judgment, the TCPA plaintiff's bar typically targets the faxers' insurance policies in an effort to maximize recovery and extort settlements. One strategy is for the class plaintiff's attorney to achieve a consent judgment with the insured defendant-faxer to agree not to pursue the faxer's personal assets, and then attempt to collect the agreed consent judgment from any insurance proceeds available. In 2013, the Illinois Supreme Court ruled that the $500 per violation damage provision was insurable under the "personal and advertising injury" portions of a general liability policy. *Standard Mutual Ins. Co. v. Lay*, 2013 IL 114617. In response to this decision, however, beginning in 2006, insurance companies have begun to implement exclusions into their policies that expressly exclude coverage for TCPA and other statutory claims, and such exclusions have been recently upheld in Illinois. *G.M. Sign Inc. v. State Farm Fire & Cas. Co.*, 2014 IL App (2d) 130593. Businesses should review their policies for the existence of such an exclusion.

Insurance implications aside, the TCPA can present a nightmare for unwary businesses and its implications must be kept in mind before any material which arguably might be deemed advertising is electronically disseminated to entities that have not invited such advertising.

Steve Ayres has more than 28 years of experience in a wide array of civil litigation matters, ranging from premises liability and vehicular accidents to complex construction defect and bodily injury cases, products liability cases, environmental and toxic tort claims, as well as related insurance coverage disputes. Steve has handled thousands of matters and tried many to verdict.

Cyber Liability: The Risks of Doing Business in a Digital World

By Chrissie Peterson, cpeterson@heylroyster.com

Major security and data breaches have become more prevalent in the past decade. News headlines are dominated by stories of major corporations having networks hacked and subjecting employees' and customers' personal, financial and health information to cyber threats. Perhaps one of the following from 2014 will sound familiar:

- January: Snapchat had the names and phone numbers of 4.5 million users compromised
- February: Kickstarter had personal information from 5.6 million donors compromised
- May: Ebay's database of 145 million customers was compromised
- September: iCloud had celebrity photostreams hacked
- November: Sony Pictures had the highest profile hack of the year involving email accounts, video games and movie releases

While the news headlines make it is easy to think this is an issue for large, Fortune 500 companies, the risk is equally widespread, but much less publicized, for small businesses.

While the data breaches at small businesses do not garner the same attention as the data breaches occurring at Sony or iCloud, the impact to the organization and the liability the organization incurs are largely the same.

Although there are many studies available giving analytics on the types of data breaches that occur, those most common to small businesses can be described in three general categories: unintentional/miscellaneous errors, insider misuse and theft/loss.

Unintentional and miscellaneous errors are any mistake that compromises security by posting private data to a public site accidentally, sending information to the wrong recipients or failing to dispose of documents or assets securely. For example, have any of your

employees ever accidentally sent an order (with account information) to the wrong email address?

Insider misuse is not a situation where an accidental error occurs. Rather, an employee or someone with access to the information intentionally accesses the data to use it for an unlawful purpose. For example, a disgruntled clerk in the billing department accesses customer information to obtain name, date of birth and bank account information in order to fraudulently establish a credit card in that customer's name. Consider another scenario where a third party vendor, a benefits provider, for example, handles employee information. Once transmitted, the employer loses control over information security for that data. Savvy business owners will make sure their contracts with vendors make the vendor responsible for any data breach that occurs during the engagement and that it will indemnify the business for any actions arising from such a breach.

Data breaches also result from physical theft or loss of laptops, tablets, smart phones, USB drives or even printed documents. Consider a scenario where the Human Resource director is heading to a conference and her laptop is stolen at the airport. The laptop is not encrypted or pass coded and the thief can access all the employee files the director keeps on her computer.

In the past decade, laws have been aimed at narrowing the information that can initially be collected by businesses and with whom it can be shared, as well as mitigating the breach after it occurs.

Federal regulations like the Health Insurance Portability and Accountability Act (HIPAA) limit the collection and use of protected health information, and also has requirements for entities suffering a data breach, including customer notification and damage mitigation provisions, such as mandatory credit monitoring and fraud protection for affected customers.

The Personal Information Protect Act requires government agencies, corporations, universities, retail stores or other entities that handle nonpublic personal information to notify each Illinois resident who may be affected by a breach of data security. 815 ILCS 530/1 *et seq*. Personal information is defined as: an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

1. Social security number.
2. Driver's license number or State identification card number.
3. Account number or credit card or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

The required notice to Illinois residents must include contact information for credit reporting agencies and the Federal Trade Commission, along with a statement that the individual can obtain information from those sources about fraud alerts and security freezes. 815 ILCS 530/10(a). If the data breached is data that the entity owns or licenses, the notice must be made without unreasonable delay. *Id.* If the data breached is data that the entity does not own or license, notice must be made immediately. 815 ILCS 530/10(b).

Failure to notify affected consumers is a violation of the Illinois Consumer Fraud and Deceptive Business Practices Act. 815 ILCS 530/20.

Technology is everywhere. Smart phones, tablets, laptops, the internet, online bill payments and the like have changed the way businesses operate. There is no denying that technology allows for efficient and effective commerce and communication. Unfortunately, the same technology that allows for faster and more efficient commerce and communication also subjects businesses to new forms of risk when it comes to data security.

There are risk management tools that all businesses should be aware of and using on a daily basis. Anti-virus software, passwords on all devices, frequent back up of data, encryption for sensitive information transmitted electronically are just a few.

What if a business owner takes all the steps necessary to reduce the risk of a data breach and it still occurs? There is a way to reduce damages and to shorten the recovery and restoration timeframes.

Cyber Liability insurance can protect businesses, large and small, from data breaches that result from malicious hacking or other non-malicious digital risks. This specific line of insurance was designed to insure consumers of technology services or products for liability and property losses that may result when a business engages in various electronic activities, such as selling on the internet or collecting data within its internal electronic network.

Most notably, cyber and privacy policies cover a business' liability for data breaches in which the customer's personal information (such as social security or credit card numbers) is exposed or stolen by a hacker.

As you might imagine, the cost of a data breach can be enormous. Costs arising from a data breach can include: forensic investigation, legal advice, costs associated with the mandatory notification of third parties, credit monitoring, public relations, losses to third parties, and the fines and penalties resulting from identity theft.

While most businesses are familiar with their commercial insurance policies providing general liability (CGL) coverage to protect the business from injury or property damage, most standard commercial line polices do not cover many of the cyber risks mentioned above. Furthermore, cyber and privacy insurance is often confused with technology errors and omissions (tech E&O) insurance. However, tech E&O coverage is intended to protect providers of technology products and services such as computer software and hardware manufacturers, website designers, and firms that store corporate data on an off-site basis. Cyber risks are more costly. The size and scope of the services a business provides will play a role in coverage needs and pricing, as will the number of customers, the presence on the internet, and the type of data collected and stored. Cyber Liability polices might include one or more of the following types of coverage:

- Liability for security or privacy breaches (including the loss of confidential information by allowing or failing to prevent unauthorized access to computer systems)
- The costs associated with a privacy breach, such as consumer notification, customer support and costs of providing credit monitoring services to affected customers.
- Costs of data loss or destruction (such as restoring, updating or replacing business assets stored electronically).
- Business interruption and extra expense related to a security or privacy breach.
- Liability associated with libel, slander, copyright infringement, product disparagement or reputational damage to others when the allegations involve a business website, social media or print media.
- Expenses related to cyber extortion or cyber terrorism.
- Coverage for expenses related to regulatory compliance for billing errors, physician self-referral proceedings and Emergency Medical Treatment and Active Labor Act proceedings.

While cyber liability insurance may not be right for all businesses, those that actively use technology to operate should consider the risks they would be exposed to if a data breach occurred. In addition, there are many different cyber policy exclusions and endorsements. Not all policies are created equal.

The attorneys in Heyl Royster's Business and Commercial Litigation group routinely advise clients on cutting edge technology topics such as advertising and publicity, website liability and cyber risks.

Chrissie Peterson's practice is focused on commercial litigation, public finance and government law. Before Heyl Royster, Chrissie was the City Attorney for Canton, IL, where she managed all legal aspects of a municipal corporation including oversight of construction contracts, franchise agreements, and utility infrastructure contracts; drafting of resolutions, ordinances and policy updates; and the legal aspects of economic development.

Supreme Court Confirms Exposure of Self-Critical Documents in Litigation

By: Stacy E. Crabtree, scrabtree@heylroyster.com

When faced with a lawsuit, businesses and their attorneys value the protections afforded to them under the attorney-client privilege and work product privilege. Where typically parties must disclose all information and documents relevant to the lawsuit to each other as part of the discovery process, these privileges allow the business and attorney to withhold certain information and documents that otherwise may have to be disclosed. The Illinois Supreme Court had the opportunity to decide this year whether a new privilege, the self-critical analysis privilege, would be recognized in Illinois to protect documents created by businesses during internal reviews or investigations after an accident.

Harris v. One Hope United, Inc., 2015 IL 117200, arises out of the drowning death of a seven-month-old after being placed back into custody with her biological mother by One Hope United, an Illinois Department of Children and Family Services (DCFS) contractor. The lawsuit alleged One Hope United "failed to protect [the child] from abuse or neglect, and should not have allowed [the child] to be returned to her mother because of her unfavorable history and her failure to complete parenting classes." *One Hope United, Inc.*, 2015 IL 117200. During discovery, the public guardian bringing the suit on behalf of the child's estate requested One Hope United produce its "Priority Review" report. Priority Review reports are created by a department within One Hope United that investigates cases, identifies gaps in services, and evaluates successfulness of the services. One Hope United refused to produce the report claiming the report was subject to the self-critical analysis privilege. The public guardian filed a motion to compel, which the trial court granted. One Hope United remained steadfast in its refusal to produce the report and as a result, the trial court found One Hope United's law firm "in 'friendly' contempt of court and fined it $1 per day." The law firm immediately appealed.

First recognized by the District Court of the District of Columbia in 1970, the original purpose of the self-critical analysis privilege was "to encourage candor when parties sought to improve their own procedures in providing medical care to patients." Since that time, the privilege has been applied in other factual settings to protect against the disclosure of documents with potentially damaging self-criticism that could significantly harm public interest. Although recognized at common law by some courts, many courts rejected the privilege so as not to "contravene the general rule in favor of admissibility." The Illinois legislature expressly adopted the self-critical analysis privilege in the 1980s, but within the limited scope of the Medical Studies Act, 735 ILCS 5/8-2101 *et seq*., for the purpose of improving hospital conditions and patient care.

One Hope United argued on appeal that applying the privilege in this case was consistent with the reasoning behind adoption of the privilege in the Medical Studies Act. The appellate court found the Medical Studies Act inapplicable to One Hope United and declined to extend the privilege beyond what was contemplated in the act. The appellate court affirmed the circuit court's ruling, refusing to recognize the self critical analysis privilege. It was now up to the Illinois Supreme Court to decide whether the privilege would exist at common law, extending to circumstances other than those expressly recognized in the Medical Studies Act.

Upon review, the Supreme Court noted the recognition of new evidentiary privileges as primarily a policymaking decision for the legislature and any judicial action recognizing a new privilege absent legislative action should be rare and only where supported by public policy. The court distinguished One Hope United's sought-out self-critical analysis privilege from the qualified privilege recognized in *Illinois Educational Labor Relations Board v. Homer Community Consolidated School District No. 208*, 132 Ill. 2d 29 (1989), which protects from disclosure the strategy deliberations of school boards and teachers' unions engaged in collective bargaining. *One Hope United,* 2015 IL 117200.

When deciding whether to recognize a new evidentiary privilege, the court in *Homer* identified the following requirements:

1. The communications originated in a confidence that they will not be disclosed.
2. This element of confidentiality is essential to the full and satisfactory maintenance of the relation between the parties.
3. The relation must be one which in the opinion of the community ought to be sedulously fostered.
4. The injury that would inure to the relation by disclosure would be greater than the benefit thereby gained for the correct disposal of litigation.

Id. citing Homer, 132 Ill. 2d at 34. In applying these requirements, the court in *Homer* found all four requirements satisfied and pointing to similar exemptions under the Open Meetings Act and Freedom of Information Act, and provisions under the Illinois Educational Labor Relations Act and federal labor law as evidence of the legislature's intent to keep such information confidential and a broader public policy in favor of the same. *One Hope United*, 2015 IL 117200.

In *One Hope United,* the court did not find the same legislative intent and public policy with respect to the self-critical analysis privilege. The court found the legislature's acknowledgement of the privilege limited to the Medical Studies Act, thus indicating a legislative intent to limit the scope of the privilege. Finding insufficient legislative intent and the lack of public policy in favor the new privilege, the court refused to acknowledge the self-critical analysis privilege, affirmed the appellate court's ruling, and held the Priority Review report was to be disclosed to the opposing party.

Despite the Supreme Court's rejection of the self-critical analysis privilege at common law, businesses should continue to promptly investigate any accidents. This case, though, serves as a reminder to ensure internal investigations are focused, factual, and thorough because any documents created may be subject to disclosure in a later lawsuit. Consult with your attorney today to review your internal investigation practices.

Stacy Crabtree represents clients in commercial and contract law, as well as tort litigation. Her clients include businesses large and small, and she regularly works onsite with a Fortune 50 manufacturing company assisting with vendor agreements, open-source software and freeware licenses, and compliance issues.

Email Newsletter Available

Would you like to receive the newsletter electronically? Just send an email request to newsletters@heylroyster.com. You'll be able to enjoy the most cost-effective, environmentally-friendly way of receiving our business and commercial litigation news!

SAVE THE DATE

Upcoming Seminar!

Avoiding Litigation:

How to Stay Out of Court, or What to Do Now to Win Quickly Later

FRIDAY, DECEMBER 4, 2015

Rockford, Illinois

Registration & Agenda to come!

Heyl, Royster, Voelker & Allen
300 Hamilton Boulevard
PO Box 6199
Peoria, IL 61601-6199

For More Information

If you have questions about this newsletter, please contact:

Timothy L. Bertschy
Heyl, Royster, Voelker & Allen
300 Hamilton Boulevard
PO Box 6199
Peoria, IL 61601-6199
Phone (309) 676-0400 – Fax: (309) 676-3374
E-mail: tbertschy@heylroyster.com

Peoria, Illinois 61601-6199
300 Hamilton Boulevard
PO Box 6199
Peoria, IL 61601-6199
Phone (309) 676-0400 – Fax (309) 676-3374

Springfield, Illinois 62711
3731 Wabash Ave.
P.O. Box 9678
Phone (217) 522-8822 – Fax (217) 523-3902

Urbana, Illinois 61803-0129
Suite 300, 102 East Main Street
P.O. Box 129
Phone (217) 344-0060 – Fax (217) 344-9295

Rockford, Illinois 61105-1288
PNC Bank Building, Second Floor
120 West State Street
P.O. Box 1288
Phone (815) 963-4454 – Fax (815) 963-0399

Edwardsville, Illinois 62025-0467
Suite 100, Mark Twain Plaza III
105 West Vandalia Street
P.O. Box 467
Phone (618) 656-4646 – Fax (618) 656-7940

Chicago, Illinois 60603
33 N. Dearborn Street
Seventh Floor
Chicago, IL 60602
Phone (312) 853-8700

www.heylroyster.com