Cyber Liability for Lawyers

By Gretchen Koehler Mote

Data breaches at retail stores and financial institutions grab the attention of the media. With the implementation of EMV chip credit cards and increased cyber security at entities that faced cyber theft in the past, cyber thieves are looking for new targets. Lawyers and law firms are increasingly among the low-hanging fruit for harvesting electronic data.

How can a data breach happen?

A data breach can occur when there is improper access to or disposal of a law firm's files or records, including loss or theft. This can happen with both electronic or the traditional paper variety.

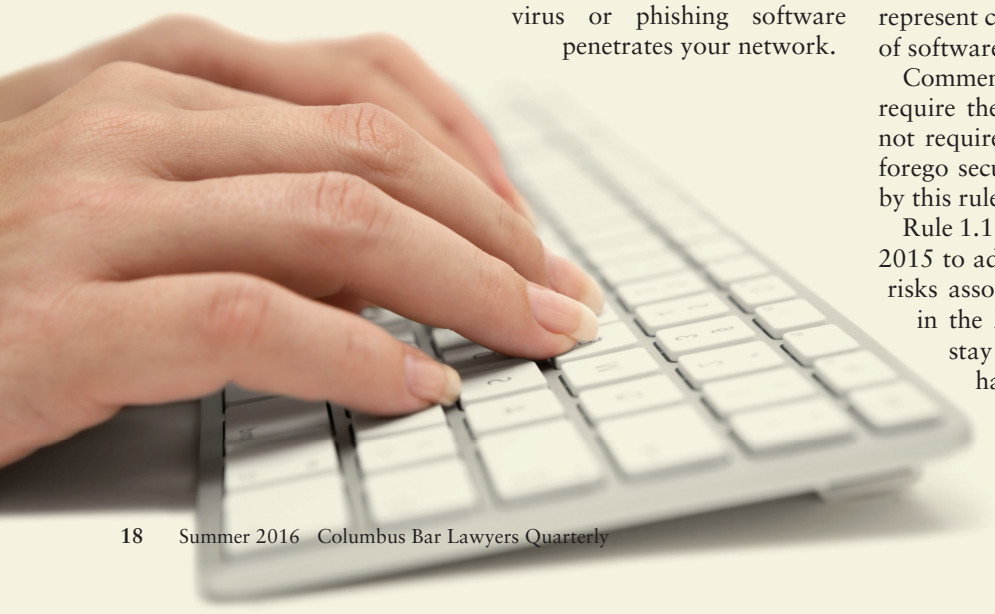
For traditional paper files or records, a breach can occur when files are not locked in a fireproof file cabinet or other secure storage when not in use. Files may be left on desks or credenzas allowing access by anyone entering the office, including cleaning crews, maintenance staff and security persons.

Improper access can also result from not regulating who can remove files from the cabinets or having unlocked doors to file storage areas that are not monitored. Improper disposal can result in a data breach when old files or records are not shredded beyond recognition using a cross-cut shredder or other means of complete destruction.

An electronic data breach can involve any device used to access and store data digitally. These devices can include a cell phone, tablet, laptop, desktop computer, server, scanner, copier or cloud and back up storage.

An electronic data breach can result from failure to log off, have adequate password protection, have established procedures on use of laptops and other electronic devices used outside the office to connect to office systems, maintain or update software including antivirus and spam software or encrypt devices, computers, servers and firewalls.

Inaction often leads to an electronic data breach. This can happen when passwords are not changed after an employee leaves or is fired, or when memory on replaced devices is not scrubbed. It can also occur when a device is stolen or lost, when a system is hacked or when virus or phishing software penetrates your network.



What happens if there is a data breach?

If there is a data breach of traditional or electronic data, there could be disclosure of client confidences. The data breach could potentially cause credit issues arising from improper access to accounts or by the use of stolen data to open new accounts. With an electronic data breach, there could also be the unintended disclosure of Personally Identifiable Information.

"Personal information," as defined in 1349.19 of the Ohio Revised Code, includes an individual's first name or first initial and last name, in combination with and linked to data elements listed in the statute. These include an individual's social security number, driver's license or state ID card number, or account number or credit or debit card number that would permit access to an individual's financial account. Personal information could be disclosed when these data elements are not encrypted, redacted or altered by technology in a manner that the data elements are unreadable.

What are a lawyer's duties relating to data breach?

Rule 1.6 of the Ohio Rules of Professional Conduct requires that a lawyer shall not reveal information relating to the representation of a client, including information protected by the attorney-client privilege. Effective April 1, 2015, Rule 1.6 (c) was amended to add new language requiring that "a lawyer shall make *reasonable* efforts to prevent the inadvertent or unauthorized disclosure of or unauthorized access to information related to representation of a client."

Comment 18 of Rule 1.6 states that such unauthorized access to or inadvertent or unauthorized disclosure does not constitute a violation of division (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards and the extent to which the safeguards adversely affect the lawyer's ability to represent clients, such as making a device or important piece of software excessively difficult to use.

Comment 18 to Rule 1.6 further notes that a client may require the lawyer to implement special security measures not required by this rule or may give informed consent to forego security measures that would otherwise be required by this rule.

Rule 1.1 Competence was also amended effective April 15, 2015 to add new Comment [8], "including the benefits and risks associated with relevant technology" to the changes in the law and its practice with which lawyers should stay current to maintain competence. Clearly, lawyers have a duty to make *reasonable* efforts to prevent the inadvertent or unauthorized disclosure of or unauthorized access to information related to representation of a client.

What can lawyers do to mitigate the risk?

The first step is to analyze compliance basics. Be sure that encryption is adequate and is actually used. Establish password protocols that require multiple passwords for data access and mandate passwords regularly be changed.

Conduct a risk assessment to determine all electronic devices in use and where the vulnerabilities lie. Establish an IRP and a WISP. If these terms are unfamiliar, get to know what they mean and plan to implement them. Implement policies and procedures and conduct training to know what to do in the event of a data breach.

Check whether data breach coverage is provided by your lawyers' professional liability carrier. If you do not have data breach coverage, look into purchasing it.

What to do if a breach occurs?

If a data breach occurs, report it *immediately* to your insurance carrier. After you report the data breach to your carrier, assess damages and implement policies and procedures set up for a data breach. Your carrier may be able to advise or assist if you have further duties imposed by ORC 1349.19.

What's the take away?

Lawyers have a duty to protect client confidential data from inadvertent or unauthorized disclosure, whether that data is kept in traditional paper files or records or in electronic format. Taking reasonable steps to implement policies and procedures to protect data in any form and having the appropriate insurance coverage can help mitigate the risks and provide peace of mind.

Gretchen Koehler Mote, Esq.
Ohio Bar Liability Insurance Company
gmote@oblic.com

BRIDGING THE GAP:
OHIO TAPS THE BRAKES ON RIDE-SHARING SERVICE COMPANIES

By Acacia M. Perko

On March 23, 2016, Ohio's House Bill 237 governing ride-sharing service companies will take effect. Now coined Transportation Network Companies, or TNCs, these companies generally provide their drivers with insurance coverage from the time they accept a customer's ride request to the time that customer exits the driver's vehicle. However, drivers are not covered by either the TNCs commercial insurance or their personal insurance while they are logged into the TNC's network and awaiting a customer's ride request. Now, 14 newly enacted statutes and an amendment to Revised Code Section 4509.103 bridge this gap period and impose new regulations on TNCs and their drivers. First, the new law mandates minimum coverage and requires TNCs to defend claims. Second, TNCs must obtain a permit to conduct business in Ohio and must require their drivers abide by zero-tolerance drug and alcohol provisions. Third, TNC drivers are specifically excluded from classification as employees under existing minimum wage laws, workers' compensation and unemployment laws. We expect the statute to impact insurance companies, TNCs and TNC drivers across the board and increase coverage litigation in the ride-share industry.

Under the new law, TNC drivers must maintain minimum coverage during the gap period in the amount of $50,000 for bodily injury or death of a person, $100,000 for bodily injury or death of two or more persons and $25,000 for property damage. They must also maintain minimum coverage of $1 million for bodily injury or death of one or more persons and property damage from the point when they accept a customer's ride request to the point when that customer exits the TNC driver's vehicle. TNC drivers must carry and provide proof of this minimum coverage to persons involved in an accident or law enforcement. Notably, the minimum coverage may be satisfied by either a policy maintained by the TNC driver personally, a policy maintained by the TNC or a combination of both.

Additionally, the new law requires TNCs to pay and defend all claims in the event a TNC driver fails to maintain the necessary coverage. TNCs are precluded from requiring a driver's private insurer to first deny coverage before providing coverage itself. In fact, the new law specifically permits private automobile insurance providers to exclude "any and all coverage afforded . . . for any loss or injury that occurs while a [TNC] driver is logged on to the [TNC's] digital network or while the driver is providing [TNC] services." Should a coverage dispute arise, TNCs and private automobile insurance providers will exchange information regarding the precise time when a driver logged on and off of the TNC's digital network in the hours before and after an accident to determine claim coverage.

In order to conduct business in Ohio, TNCs must obtain permits with the Public Utilities Commission of Ohio. TNCs must also disclose how fares are calculated, TNC rates, estimated fares, photographs of drivers and the driver's license plate. TNCs are also required to prominently display the TNC's name on the vehicle providing the service, provide customers with a receipt following service, provide proof of insurance and conduct background checks on all prospective drivers. Further, TNCs must prohibit TNC drivers from consuming any alcohol or drug of abuse, not including prescribed medications, while transporting passengers or even while logged on to the TNC digital network.

While recent court decisions in at least one state have classified TNC

Continued on page 21