Lawyers Mutual
www.lmick.com

The Risk Manager

A quarterly newsletter by Lawyers Mutual Insurance Company of Kentucky

SUMMER 2013
Volume 24, Issue 3

WHAT IS YOUR RESPONSIBILITY FOR LOSS OF CLIENT CONFIDENTIALITY AND CLIENT PRIVACY WHEN YOUR FIRM COMPUTER AND INTERNET DEVICES ARE HACKED?

Background

The scope of hacking of computer systems and Internet devices such as a Smart Phone is increasing exponentially worldwide. The legal profession is no exception to this development and, unfortunately, carries an even heavier burden for computer system security than the typical business. This is true because of a lawyer's fiduciary duty of preserving client confidentiality and the sensitive nature of the information in electronic client files vulnerable to being hacked. Hacked financial information concerning business deals, settlements, and divorce negotiations are just a few examples of how compromised client files can harm clients and expose a firm to a large liability claim.

According to the National Conference of State Legislatures, 46 states have enacted laws to protect the general public from this kind of injury by requiring those who maintain personal information of others to secure it and upon being hacked to notify all persons whose personal information is compromised. To date Kentucky has not passed such a law, but the Kentucky Legislature by resolution in its 2013 session recognized that "Kentucky is one of only four states without a security breach law requiring notification to consumers by government and private data custodians of security breaches involving personal information." The resolution directed the Interim Joint Committee on State Government of the Legislative Research Commission to study issues related to cyber security and provide a report by November 27, 2013.

Since in Kentucky the Supreme Court issues the rules governing the practice of law, it may be that any Kentucky security breach law passed by the Legislature will not be applicable to Kentucky lawyers. This point, however, does not overcome a lawyer's existing professional responsibility to protect client confidentiality and the duty to reasonably inform a client of the status of a matter and of errors in its handling. For this reason, it is recommended that lawyers risk manage computer security breaches as if any new law will apply as well as existing professional responsibility duties.

Other State Laws

There is considerable uniformity among the state laws on security breaches suggesting that any Kentucky law will be similar. The following extracts from West Virginia's law (W.V. Code §§ 46A-2A-101 et seq.) provide a good overview of what you may see in a Kentucky Law:

- "Breach of the security of a system" means the unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes the individual or entity to reasonably believe that the breach of security has caused or will cause identity theft or other fraud to any resident of this state.

- "Entity" includes corporations, business trusts, estates, partnerships, limited partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint

continued on page 2

"Sometimes questions are more important than answers."

Nancy Willard

continued from page 1

ventures, governments, governmental subdivisions, agencies or instrumentalities, or any other legal entity, whether for profit or not for profit.

- "Personal information" means the first name or first initial and last name linked to any one or more of the following data elements that relate to a resident of this state, when the data elements are neither encrypted nor redacted:

  (A) Social security number;

  (B) Driver's license number or state identification card number issued in lieu of a driver's license; or

  (C) Financial account number, or credit card, or debit card number in combination with any required security code, access code or password that would permit access to a resident's financial accounts.

  The term does not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully

- Notice of breach of security of computerized personal information.

  (a) An individual or entity that owns or licenses computerized data that includes personal information shall give notice of any breach of the security of the system following discovery or notification of the breach of the security of the system to <u>any resident of this state</u> whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person and that causes, or the individual or entity reasonably believes has caused or will cause, identity theft or other fraud to any resident of this state. (*emphasis added*)

  (d) The notice shall include:

  (1) To the extent possible, a description of the categories of information that were reasonably believed to have been accessed or acquired by an unauthorized person, including social security numbers, driver's licenses or state identification numbers and financial data;

  (2) A telephone number or website address that the individual may use to contact the entity or the agent of the entity ….

<u>Computer Security Breach Risk Management</u>

There are a number of good sources for developing a security breach risk management plan on the Internet. We recommend the following sites to begin research for determination of what is best for your practice:

- For a short review of the issues and general risk management guidance read the article "Law Firms' Obligations When Personal Information in Their Control Is Hacked — Data Breach Legislation" in the September 5, 2012 issue of Hinshaw & Culberston's *The Lawyers Lawyer Newsletter* at *http://www.hinshawlaw.com/*. (Click on Publications, Newsletters, and View All Newsletters) (*last viewed on 6/18/13*)

- For a comprehensive treatment of risk managing security breaches read "Managing the Security and Privacy of the Electronic Data in a Law Office;" a publication of Lawyers' Professional Indemnity Company at *http://www.lawpro.ca/*). (Search for the article with words "security breach") (*last viewed on 6/18/13*). The section headings for this article are:

  #1 install latest updates to eliminate security vulnerabilities
  #2 make full and proper use of passwords
  #3 antivirus software is essential
  #4 avoid spyware and adware
  #5 install a firewall on your Internet connection
  #6 be aware of and avoid the dangers of e-mail
  #7 beware the dangers of metadata
  #8 lockdown and protect your data, wherever it is
  #9 harden your wireless connections
  #10 learn how to safely surf the Web
  #11 change key default settings
  #12 implement a technology use policy
  #13 a backup can save your practice

<u>Unresolved Issues</u>

Opposing Parties and Third Parties: Fiduciary duties applicable to clients do not apply to opposing parties and third parties. Thus, it is an open question what responsibility Kentucky lawyers may have to notify them of a security breach. Kentucky Rule of Professional Conduct 4.4, Respect for the Rights of Others, can be read broadly to require notification of third parties, but that is arguable. Also consider that notification may not be in your client's best interest even though future law or rules could require you do so. Should you face this ethical issue, call the KBA Ethics Hotline for guidance.

continued on page 3

"The thing that is really hard, and really amazing, is giving up on being perfect and beginning the work of becoming yourself."

Anna Quindlen

continued from page 2

Out-of-State Clients, Opposing Parties, and Third Parties: Note that the West Virginia law protects residents of West Virginia. If you maintain electronic files of persons in West Virginia you may have a legal requirement to notify them of a security breach regardless of Kentucky law or rules. The point is that if you currently maintain files of persons in states outside of Kentucky, you need to know now the law in those states on security breaches.

Malpractice Avoidance – Client Screening

Client screening is a concept of risk management well known to most lawyers. Screening out high-risk prospective clients is a failsafe method of avoiding any risk of a malpractice claim. What is not so well appreciated is that current client screening should be part of your risk management program as well. In tough economic times, however, it can be hard to apply screening when it means declining or disengaging clients, worthy or unworthy. Nonetheless the price paid for representing a client that should be avoided can be high both in terms of cost, time, and reputation. These circumstances suggest that now is a good time to review the factors that a prudent lawyer will consider when performing prospective and current client screening.

Prospective Client Screening Checklist:

1. Beware of the prospective client who is changing attorneys.
2. Be leery of a case that has been rejected by one or more other firms.
3. Does the prospective client have a history of questionable prior litigation?
4. Does the prospective client have unrealistic expectations for the matter that cannot be altered?
5. Does the prospective client have an unreasonable sense of urgency over the matter? Beware of a case that has an element of avoidable urgency.
6. Beware of the client who has already contacted multiple government representatives to plead his case.
7. Beware of the client who wants to proceed with his case because of principle and regardless of cost.
8. Beware of a client who has done considerable personal legal research on his case.
9. If your first impression of the prospective client or his matter is unfavorable, think twice before accepting the case. It is best to avoid a prospective client who demonstrates a difficult personality along with other indications that he will be uncooperative. If your intuition tells you to avoid a prospective client, listen to it.
10. Is the prospective client difficult about reaching agreement on fees? Does he appear to be price shopping? Can he afford your services? Does he refuse to give an adequate retainer?
11. Avoid prospective clients with matters outside your firm's regular practice areas unless you are prepared to spend the time and resources necessary to develop the required competence to practice the matter. Can the prospective client afford the cost associated with this effort?
12. Avoid prospective clients when the statute of limitations is about to run or other deadline is impending on their matter unless you are absolutely sure you can meet the limitation or deadline. A good rule of thumb is that a new case should not be accepted if it is within three months of the statute of limitations. This is just too short a time to identify and name all the parties. Accepting unrealistic time pressure to represent a client is an invitation to commit malpractice (think medical malpractice suits).
13. Be leery of accepting prospective clients who are family or friends. Fee misunderstandings along with the loss of objectivity when representing family or friends can lead to bitter results.
14. Learn everything you can about the quality of a prospective client before you take the matter – not just verification of the facts of the case. Do a Google search – look for Websites, blogs, and participation on sites such as FaceBook, and MySpace. Determine whether the prospective client has:
    a. Good credit and is financially solvent.
    b. A criminal record.
    c. Frequently filed claims for injuries.
    d. Retained numerous lawyers in the past.
    e. Ever sued a lawyer for malpractice or filed a bar complaint.
15. Verify the identity of non-face-to-face prospective clients – those that contact you by phone, mail, or over the Internet. Scams targeting lawyers are everyday occurrences.

continued on page 4

"If at first you don't succeed, find out if the loser gets anything."
Yale English Professor William Lyons Phelps

continued from page 3

Current Client Screening Checklist: (From "The Impact of the Credit Crunch on Lawyer Risk Management," by Del O'Roark, *Kentucky Bench & Bar,* July 2009)

Screening of prospective clients is a well-known risk management procedure. What many lawyers fail to do, however, is screen current clients for problems that can develop during a representation. Current client screening should include:

- Conducting Interim Conflict of Interest Checks: During the course of a representation a conflict check should be made anytime a new party is named, a new entity becomes involved, new witnesses are identified, or any other development that triggers conflict issues. This is especially important in business and commercial transactions. When the deal goes bad or the business fails, lawyers involved with any whiff of a conflict are sued either for malpractice or breach of fiduciary duty. These are difficult claims to defend and juries have little sympathy for lawyers perceived as disloyal or devious.

- Monitoring for Good Clients Gone Bad: Enron's fall from grace is a good example of a good client gone bad resulting in its lawyers being accused of breaching fiduciary duties owed to third parties and aiding and abetting the client in fraud. Business and commercial transaction lawyers are at greatest risk for such a claim. To risk manage this exposure, establish policies that screen for red flags signaling that something is amiss with a client or that a client is engaged in questionable transactions.

  The following is a list of some of the factors to consider in evaluating whether a current client poses unexpected risks:

  - Change in control – Has there been a sudden change of management or has management gone into weaker hands? Are the client's employees leaving the client or being laid off?

  - Change in ownership – Has the client been acquired by a conglomerate or gone into bankruptcy? Successors, receivers, regulators, and trustees are not your friends, even if the client was.

  - Unusual transactions – Does the client want to do a transaction with no apparent business purpose?

  - Nature of client's business – Does the client owe fiduciary duties to customers and is the client dealing with other people's money?

  - Change in relationship with the client – Has the client's behavior changed as reflected in sudden urgent requests for legal advice giving little time for response? Is the client tense, erratic? Does the client want to micromanage the matter? Does the client want a reduction in fees? In bad economic times clients can become desperate.

  - Character change – Does the client expect you to bend rules, endorse a questionable scheme, cover up, or stretch the truth? Is the client uncertain of the source of funds for a deal? Is the client now willing to commit fraud?

  - Change in fee payments – A change in payment habits is a frequent sign of trouble in a client. Accounts receivable building up could be a signal that the client is in financial difficulties. Do a solvency check before the amount of arrearages becomes significant. If you are about to enter a period of intense work for the client that will involve substantial billing, get a retainer supplement and make sure the client knows what is coming. If you cannot readily work out fee payments, consider withdrawing.

Do not rely on a client's continued good will. Clients change. There are changes in ownership, control, and circumstances. Educate firm lawyers and staff to be alert to these developments. If you become concerned that a good client is going or has gone bad, withdrawal is often the best risk management. If you continue the representation, be sure that the letter of engagement accurately defines the scope of representation and any changes in scope. Carefully document the file to record significant developments and the advice given. In delicate situations it is especially important that the advice given be reflected in a letter to the client. Do not expose yourself to a claim of fiduciary breach by third parties or of aiding and abetting your client in fraud.

"I've learned that people will forget what you said, people will forget what you did, but people will never forget how you made them feel."

Maya Angelou

Scope of Engagement – Elder Adult Representation – Adding Provisions to Power of Attorney Inadvertently Enlarges Scope of Ohio Lawyer's Duty to Client *(Svaldi v. Holmes, 2012 Ohio 6161, 12/27/12)*

In 2008 lawyer Holmes assisted Svaldi, a wealthy 93-year-old client, by preparing a standard power of attorney granting J and E who managed the apartment where he lived the authority to manage, sell, and transfer his assets and to open and close bank accounts and sign checks on his behalf. In an effort to protect Svaldi, Holmes modified the POA by adding these two provisions:

> 10. The holder of this Power-of-Attorney shall within thirty (30) days of appointment, or as soon thereafter as possible make an inventory of my estate assets and list any claims or obligations which I have or may have, giving me a copy, keeping a copy for herself, and leaving a copy with my attorney, Robert D. Holmes ….
>
> 11. The holder shall also file an annual account by January 31st of each year and deliver it to Robert D. Holmes, attorney, or any attorney licensed in Ohio, designated by me or by the holder of this Power-of-Attorney for safe-keeping.

J and E did none of these things even after Holmes in 2008 sent a letter to J reminding her of her obligation to comply with these requirements. Holmes made no other follow-up effort to obtain compliance. In 2011 large withdrawals from Svaldi's bank account prompted the bank to notify the police. Investigation revealed that over $800,000 was stolen by J and E.

Svaldi then sued Holmes for malpractice claiming that by including the inventory and annual accounting requirements in the POA, Holmes assumed a duty to monitor compliance. Holmes defended by arguing that his only duty to Svaldi regarding the POA was to prepare it competently and with due care. Holmes was granted summary judgment by the trial court, but the Ohio Court of Appeals reversed this decision.

In its decision the Court wrote:

> The expert witnesses of both parties testified that provisions such as paragraphs 10 and 11 do not typically appear in powers of attorney. Holmes explained that he incorporated the inventory and accounting scheme into Svaldi's power of attorney because the designated agents were not Svaldi's relatives and, thus, lacked a familial duty to act in Svaldi's best interests. To protect Svaldi, Holmes sought to create transparency about the amount of Svaldi's assets at the origination of the power of attorney and the subsequent expenditure of those assets by Svaldi's agents.
>
> ….
>
> We conclude that, by incorporating the inventory and accounting scheme into the power of attorney, Holmes expanded the scope of his representation of Svaldi beyond the mere drafting of legal documents. By setting up the inventory and accounting scheme, Holmes assumed a responsibility to attempt to make it work. Thus, Holmes had a duty to follow up with [*J and E*] regarding their obligation to complete an inventory and the annual accountings and encourage [*J and E*] to comply with the scheme.

Risk Management Considerations

- Modifying a standard legal form such as a POA with a well understood scope of the preparing lawyer's duties must be done with extra care and appreciation for the implications to the lawyer's scope of engagement. Holmes' modification of Svaldi's POA, well intended as it was, is ambivalent on how the added terms were to be managed. In a malpractice claim a lawyer will never get the benefit of the doubt in these circumstances.

- Holmes' problem was exacerbated by the fact of Svaldi's extreme old age. Risk management of older adult representations involves the recognition of the enhanced professional responsibility duties lawyers owe older adults. In these representations a lawyer often needs to go much further than in other similar representations to assure that the older adult client is protected from family, friends, business people, and scammers. While not explicit in the Court's decision, it is not much of an extrapolation to conclude that Svaldi's 93 years factored significantly on the protection the Court saw fit to give him.

- The May 2013 issue of the KBA Bench & Bar Magazine includes the article *Kentucky Powers Of Attorney: A Necessary Planning Tool For End Of Life*, by Kenton, Dougherty, McClelland, and McFarlin. In addition to being an excellent substantive treatment of POAs, it is something of a risk management bible for avoiding malpractice when preparing a POA for

continued on page 6

Lawyers Mutual
www.lmick.com

Waterfront Plaza
323 West Main Street, Suite 600
Louisville, KY 40202

Malpractice Avoidance Update
Member National Association of Bar Related Insurance Companies

For more information about Lawyers Mutual, call ***(502) 568-6100*** or KY wats ***1-800-800-6101*** or visit our Website at ***www.lmick.com***

continued from page 5

an elderly client. It covers numerous POA considerations for elderly clients including the specificity required for powers granted to the agent, choice of agent, authority to gift real estate and other assets, and Medicaid planning. We urge you to read this article and place a copy in your POA file for ready reference whenever drafting a POA.

Beware of the Statute of Limitations in Personal Injury Cases When the Injury Occurs Outside Kentucky

In the article *"Where Did You Say The Accident Happened?"* Warren Savage of Lawyers Mutual Insurance Company of North Carolina gave North Carolina lawyers some pointers on risk managing statutes of limitation for personal injury claims that occur in states other than North Carolina.

Savage recommends that client intake forms require information that addresses whether the case may have an out-of-state statute of limitations. Specifically, the intake form should cover the:

- State in which the accident occurred.
- Identity and residence of the tortfeasor.
- Jurisdiction where the complaint will be filed if necessary.
- Statute of limitations that will apply to the claim.

Savage concludes with the advice that "the attorney who has ultimate responsibility for filing a complaint review the gathered information and make an immediate determination of the proper statute of limitations that is then properly docketed."

We heartily concur with Mr. Savage's excellent risk management advice.