PROACTIVE CYBER LIABILITY PROTECTIONS, BY ALICE SHERREN, ESQ., JODY HARRIS, RPLU, AND DONALD PATRICK ECKLER, ESQ.

Cyber liability exposure is among the largest risks for lawyers and their clients. Law firms, big and small, are targeted by hackers seeking personal and other information to exploit for criminal purposes. Since no security system can entirely eliminate the potential for such exposure, law firms should consider including a limitation on liability in their engagement letters.

The Ethical Obligation to Mitigate Cyber Risks

The Model Rules of Professional Conduct obligate lawyers to mitigate as much as possible the risk of exposure of confidential information. Model Rule 1.6(c) requires that "[a] lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." See also Comment 18 to Model Rule 1.6. The comments to Model Rule 1.1 specifically require lawyers to "keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology…." This plainly includes the risks of cyber attack.

Lawyers need to ensure that all firm members and employees are mitigating cyber risks. Model Rule 5.1 (b) requires those lawyers supervising other lawyers to "make reasonable efforts to ensure that the other lawyer conforms to the Rules of Professional Conduct." Model Rule 5.3(b) expands this responsibility to the supervision of non-lawyers, which would include in-house or contract information technology professionals, and states that a "lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer." Comment 2 to Model Rule 5.3 particularly addresses the importance of protecting confidential information: "A lawyer must give such assistants appropriate instruction and supervision concerning the ethical aspects of their employment, particularly regarding the obligation not to disclose information relating to representation of the client, and should be responsible for their work product."

In addition to the Model Rules, there are numerous resources to guide lawyers in compliance with their ethical requirements. A very good list of steps to take is included in "Preventing Law Firm Data Breaches," Law Practice Magazine, John Simek and Sharon Nelson, Vol. 38, No. 1. https://www.americanbar.org/publications/law_practice_magazine/2012/january_february/hot-buttons.html One of the steps taken by many law firms to protect client data is to do away with in-house servers to store client data and to use cloud based services which provide more robust security for client data. Cloud based services are administered by third-parties who have expertise in managing and securing data that is far more robust that the in house systems previously used. This practice has been countenanced by many bar associations that have looked at the issue. See ISBA Professional Conduct Advisory Opinion No. 16-06 citing Alabama Ethics Opinion 2010-2 (2010) (lawyer may outsource storage of client files through cloud computing if the lawyer takes reasonable steps to make sure data is protected); Iowa Ethics Opinion 11-01 (2011) (lawyer should conduct appropriate due diligence before storing files electronically); Tennessee Formal Ethics Opinion 2015-F-159 (2015) (a lawyer may allow client information to be stored in the cloud provided the lawyer takes reasonable care to assure that the information remains confidential and that reasonable safeguards are employed to protect the information from breaches, loss or other risks). "Cloud Ethics Opinions Around the U.S.", American Bar Association, Legal Technology Resource Center, www.americanbar.org.

Nevada Formal Opinion No. 33 (2006) discussed a lawyer's use of an outside agency to store electronic client information and stated: "[t]he use of an outside data storage or server does not necessarily require the revelation of the data to anyone outside the attorney's employ. The risk, from an ethical consideration, is that a rogue employee of the third party agency, or a 'hacker' who gains access through the third party's server or network, will access and perhaps disclose the information without authorization. In terms of the client's confidence, this is no different in kind or quality than the risk that a rogue employee of the attorney, or for that matter a burglar, will gain unauthorized access to his confidential paper files. The question in either case is whether the attorney acted reasonably and competently to protect the confidential information." In other words, simply foisting the responsibility of maintaining client documents onto a third-party provider does not end the lawyer's obligation, it merely focuses that responsibility.

Limitation of Liability by Attorneys

Attorneys often use engagement letters to negotiate terms that allow the law firm to limit its financial, ethical, and malpractice risks. Such terms include arbitration clauses, interest on late paid fees, forum selection clauses, and scope limitation provisions. Generally, such terms present little or no ethical issue so long as the client agrees to the terms. Many clients, especially sophisticated institutional clients and insurance companies, negotiate terms favorable to the client. These terms often involve detailed requirements that must be met by

"Attorneys often use engagement letters to negotiate terms that allow the law firm to limit its financial, ethical and malpractice risks."

Contact PLDF:
Christine S. Jensen
Managing Director
Professional Liability Defense Federation
1350 AT&T Tower
901 Marquette Avenue South
Minneapolis, MN 55402
(612) 481-4169
cjensen@pldf.org

CYBER LIABILITY PROTECTIONS, CONT'D

the law firm and include robust audit rights. Institutional clients also often require that law firms adopt specific cyber security measures to secure client data, and impose penalties on law firms if they fail to satisfy these requirements. (As an aside, for law firms that do insurance defense work, it is a good practice to review the various requirements of insurers to not only make sure that the guidelines are being followed by the law firm but to make sure that requirements from different insurers are not in conflict).

In the cyber liability context, assuming that the guidelines of a particular client do not forbid it, law firms may look at including a limitation on liability in their standard engagement letter. Courts have not specifically addressed limitations on cyber liability in lawyer engagement letters, but cases that have addressed limitations on cyber liability in other contexts seem to imply that the negotiability of lawyer engagement letters may allow lawyers to limit their exposure. In *In re Yahoo! Inc. Customer Data Security Breach Litigation*, 16-MD-2752, the court first held that Yahoo's terms of service did not shield it from liability because it had made affirmative security promises in other parts of those same terms. Yahoo's terms of service also included a limitation on liability which provided:

> YOU EXPRESSLY UNDERSTAND AND AGREE THAT YAHOO! SHALL **NOT BE LIABLE TO YOU FOR ANY PUNITIVE, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES**, INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS, GOODWILL, USE, DATA OR OTHER INTANGIBLE LOSSES (EVEN IF YAHOO! HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES), RESULTING FROM UNAUTHORIZED ACCESS TO OR ALTERATION OF YOUR TRANSMISSIONS OR DATA OR ANY OTHER MATTER RELATING TO THE YAHOO! SERVICE.

However, the court found that the limitation on indirect, incidental, or consequential damages, including for "loss of data or other intangible losses" foreclosed the plaintiff's breach of contract claims against Yahoo that sought out-of-pocket mitigation costs.

Notwithstanding that dismissal, the court allowed the plaintiff to replead to allege that the limitations on liability were unconscionable. The court found that the provisions of Yahoo's take-it-or-leave-it terms of service to be procedurally and substantively unconscionable. *In re Yahoo! Inc. Customer Data Security Breach Litigation*, 16-MD-2752 (N.D. Cal., March 9, 2018).

In the case of a law firm servicing a business or a sophisticated individual client, the unconscionability present in the Yahoo terms of service will rarely be present because the differences in bargaining position and control over contract terms are absent. This is because engagement letters are negotiated between lawyers and clients as a matter of routine, and terms, including rates, staffing, scope, and limitations provisions, are appropriately matters for discussion and revision. An engagement letter is never a take-it-or-leave-it proposition like the terms of service in *Yahoo*. Among the terms that law firms may look at including in their engagement letters are limitations on damages provisions in the event of a cyber attack. In order to avoid some of the problems experienced by Yahoo it would be advisable to include information about the steps taken and the procedures implemented by the firm to protect client data from a cyber attack.

Insurance Considerations

When negotiating engagement letters with clients to protect against cyber liability risks, law firms should be cognizant of their cyber liability and professional liability insurance contracts. While an engagement letter is an agreement between the law firm and the client, the insurance contract is between the law firm and the insurer; the client is not a party to the insurance contract. Cyber liability and professional liability policies usually specify that the insurer controls the defense, and contain provisions dictating the obligations of the insurer and the law firm. Law firms need to be certain the terms of their engagement letters do not conflict with or otherwise impact coverage under the law firm's insurance policies.

Cyber Policy

This is language from one cyber policy under the Assistance and Cooperation Clause:

> …The Insured will not admit liability, make any payment, **assume any obligations, incur any expense, enter into any settlement, stipulate to any judgment or award or dispose of any Claim without the written consent of the Underwriters**, except as specifically provided in the Settlement of Claims clause above. …. (emphasis added)

If a law firm with such a policy provision is asking clients to agree to arbitration, the firm should have the agreement of their insurance carrier. Plus, the firm should consider that policy language changes between carriers and every time the firm changes insurance carriers, the firm would have to secure confirmation from the carrier of the carrier's approval to agree to arbitration. It is not necessarily a given that all insurance carriers would want arbitration.

Clients of law firms sometimes also ask for the firm's insurer to waive subrogation rights. A law firm cannot agree to waive subrogation rights for an insurance company. If that request is received, an endorsement would be needed on most policies.

In addition, law firms may request other items to

"Courts have not specifically addressed limitations on cyber liability in lawyer engagement letters."

PLDF Amicus Program

Please let us know of appeals in your jurisdictions implicating important professional liability issues that might have broad-based significance.

CYBER LIABILITY PROTECTIONS, CONT'D

meet client demands, that may not be reimbursed on cyber policies. Examples are credit reporting services for periods greater than the policy allows and reimburses firms for, and notice to the client of a breach in no more than 24 hours, which may not give a firm enough time to investigate a cyber incident. It's best to carefully discuss any such cyber requirements with the broker and insurer so you know what is and isn't covered by your cyber policy.

Lawyers Professional Liability Policy

Most lawyers' professional liability policies provide coverage for third party cyber claims, depending on the allegations and circumstances of the claim. If third party cyber claims are covered by both policies, the "other insurance" clause in those policies would dictate which policy provides primary coverage, and which policy provides only excess coverage. The other insurance clause in a cyber policy can often be amended.

Whatever a firm agrees with clients – whether in engagement letters, outside counsel guidelines or requests for proposals, or otherwise – if it affects how liability claims are paid or an insurer's rights under a firm's policies, it is important to ensure the carrier is in agreement with those terms as well.

Conclusion

The best defense is knowing where you are vulnerable. Once lawyers understand their ethical obligations surrounding cyber security, they can take steps to protect their clients' data and their own malpractice risks. Being aware of and reviewing the available insurance coverage for such claims is also a wise step to take to reduce exposure should a breach occur. Since implementation of even the strongest cyber security system is not fool-proof, negotiating limits on cyber liability in engagement letters with clients is appropriate so long as the agreement also is in compliance with a firm's insurance policies.

Jody Harris is the Managing Director of **Arthur J. Gallagher** & Co.'s Law Firm Practice. Jody is responsible for the insurance placement of LPL insurance, as well as risk management for mid-size to large law firms. She may be reached at jody_harris@ajg.com.

Alice M. Sherren is a Claim Attorney with **Minnesota Lawyers Mutual Insurance Company.** Since joining MLM in 2009 Alice directs the defense of LPL claims and speaks on risk management and ethics matters. Alice may be reached at asherren@mlmins.com.

Donald Patrick Eckler is a partner at **Pretzel & Stouffer,** Chartered, in **Chicago**. Pat defends doctors, lawyers, architects, engineers, appraisers, accountants, mortgage and insurance brokers, surveyors and others. He may be reached at deckler@pretzel-stouffer.com.