CLM CLAIMS & LITIGATION MANAGEMENT ALLIANCE™

ADVANCING ETHICS, COOPERATION AND EDUCATION

2016 CLM Boston Conference
July 14-15, 2016 Boston, MA

"Cyber Attacks on Professionals-How Far Will They Raise the Standard of Care?"

I. ABA (American Bar Association) Model Rules and the Standard of Care

ABA Model Rules of Professional Conduct, Rule 1.1 states that: "Lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."

Rule 1.3 states: "A lawyer shall act with reasonable diligence and promptness in representing a client."

These rules, while dealing with the standard of care, do not answer the question whether a failure to secure the client's property reflects lack of diligence and competence.

Rule 1.15 (a) makes it clear that there is a duty to safe keep the client's property: " . . . property shall be identified as such and appropriately safeguarded. . ." Yet, this safe keeping may not be a standard of care, but merely an independent ethical duty. Preamble 20 of the Rules explains: "Violation of a Rule should not itself give rise to a cause of action against a lawyer nor should it create any presumption in such a case that a legal duty has been breached . . . They are not designed to be a basis for civil liability. . . Nevertheless, since the Rules do establish standards of conduct by lawyers, a lawyer's violation of a Rule may be evidence of breach of the applicable standard of conduct."

Accordingly, based on the Rules, while an attorney is charged with securing the client's property (which surely will include cyber data, documents and information stored on computers), failing to secure such property may not necessarily be below the standard of care, but merely an ethical violation. On the same token, discipline can be had without an attorney client relationship *State v. Martin* (Okla. 1965) 410 P.2d 49. While attorneys worry about ethical violations, it is expected that clients will also be able to add additional claims of breaches. For example, Mossack Fonseca possible concealment of the fact that the breach started in early 2015 and its notification of clients of merely an e mail hack in April, 2016 may give rise to tort claims against the law firm. In those situations, the failure to secure the client's property can be evidence of legal malpractice.

II. Is there Individual Liability?

A. The Standard of Care

An attorney is held to the standard that any reasonable attorney in possession of the same knowledge and skill that an ordinary member of his or her profession possesses. *Hodges v. Carter*, 239 N.C. 517, 80 S.E.2d 144 (1954). The attorney's standard of care is to represent the client competently. *Atkin v. Tittle & Tittle*, (Fla. 3d DCA 1999)730 So. 2d 376 . Florida Ethics Code, Rule 1.1:330. The attorney must act with a reasonable degree of care, skill and dispatch. *Crosby v. Jones*, (Fla. 1998) 705 So. 2d 1356 . "A lawyer owes to the client a duty to exercise the degree of reasonable knowledge and skill which lawyers of ordinary ability and skill possess and exercise." *Home Furniture Depot, Inc. v. Entevor AB*, (Fla. 4th DCA 2000) 753 So. 2d 653, 655. A lawyer advising a client with regard to a settlement proposal "has a duty to utilize ordinary skill and knowledge." *Sauer v. Flanagan & Maniotis, P.A.*, 748 So. 2d 1079, 1082 (Fla. 4th DCA 2000). Are members of the profession, and each and every attorney at a law firm, charged with knowledge of cyber security? Should Mossack Fonseca have realized that its web hosting software had flaws and was old? Even if yes, should any individual attorney at the law firm know that? Would it have been unreasonable to know the risks?

B. The Cyber Attack

Typically, a claim made by the client is made against the attorney representing that client and against the law firm. Yet, data breaches arise from several causes, some of which may not necessarily originate with the attorney at the law firm who directly represents the client. They can happen by rogue employees, or they can occur by mistake, when there are lost or stolen mobile devices or laptops. They can also arise from an attack on the firm's network. A cyberattack is an attack initiated by hacking from a computer against a website, computer system or individual computer or on a person, which compromises the confidentiality, integrity or availability of the computer or information stored on it. Cyberattacks occur in many forms, including: (a) Gaining, or attempting to gain, unauthorized access to a computer system or its data, (b) unwanted disruption or denial of service, including the take down of entire web sites, (c) installation of viruses or malicious code (malware) on computer a system, (d) unauthorized use of a computer system's hardware, firmware or software without the owner's knowledge, instruction or consent, and (e) inappropriate use of computer systems by employees or others. While it is possible that that a cyber attack can disrupt the business of the attorney's client, the real risk is that the client's information is stolen and then misused.

C. Individual Liability and Causation

Before suing an attorney, does the claimant need to determine what was the cause of the hack? If an attorney A at a law firm downloads a bug into the main frame which is then used to extract information from attorney B's clients, can attorney B's clients sue attorney B for malpractice for failure to secure their documents and information? What if

the law firm employs numerous defenses and fire walls, uses the most updated web hosting software and uses encrypted e mails?

Not all security breaches necessarily arise from an individual attorney's actions but the Rules do not explain what is reasonable for an individual attorney in terms of protecting the client's property. The analysis will depend on a case by case and on what attorneys in the same community are doing. The more new and young attorneys join the profession, who have much more inclination and understanding of technology and computers, the more likely that these younger attorneys will be more keenly aware of, and respond to a higher level of cyber security. Therefore, this could become the new standard of care.

III. How is Standard of Care Relevant?

Standard of care is important to prove negligence. The elements of a cause of action for breach of professional negligence are "(1) the duty of the professional to use such skill, prudence, and diligence as other members of his profession commonly possess and exercise; (2) a breach of that duty; (3) a proximate causal connection between the negligent conduct and the resulting injury; and (4) actual loss or damage resulting from the professional's negligence." *Budd v. Nixen,* 6 Cal.3d 195 (1971); *Carlton v. Quint,* 77 Cal.App.4th 690 (2000). Causation and damages are important components, as the client needs to prove it would have had a better result but for the attorney's mistake. *Sutton v. Whiteside* (1924) 101 Okla. 79

California jury instruction, CACI 600 explain: "[defendant] is negligent if he/she fails to use the skill and care that a reasonably careful [attorney] would have used in similar circumstances. This level of skill, knowledge, and care is sometimes referred to as "the standard of care." You must determine the level of skill and care that a reasonably careful [attorney] would use in similar circumstances based only on the testimony of the expert witnesses who have testified in this case."

The standard is that of members of the profession 'in the same or a similar locality under similar circumstances'. . . . The duty encompasses both a knowledge of law and an obligation of diligent research and informed judgment." *Wright v. Reed,* 47 Cal.App.3d 802 (1978). The standard is ordinary care by attorneys practicing in the same jurisdiction. *Collins v. Warner* (Okla. 1963) 382 P.2d 105. Geographical location may be a factor to be considered, but, by itself, does not provide a practical basis for measuring similar circumstances. *Avivi v. Centro Medico Urgente Medical Center*, 159 Cal.App.4th 463 (2008). This suggests that an attorney in a rural county can be charged with the same standard of a top tier law firm in a large city. It may also be irrelevant that the small law firm may not be able to afford the expensive security systems used by the wealthier law firms.

VI. How is Standard of Care Determined?

A. The Defendant's Higher Standard

In *FFE Transportation Services v. Fulgham,* 154 S.W.3rd 84 (Tex. 2004) the Supreme Court of Texas discussed the changing standard of care. *FFE Transportation Services* was a trucking injury case where the plaintiff argued that the company deviated from its own--potentially higher—standard, which inspected the trailer assemblies every 60 days. While plaintiff's expert testified that he was not aware of such industry wide standard, he commented that this standard was reasonable and therefore applied to the situation. The judge did not allow that testimony because it was not prevalent throughout the industry. The Supreme Court agreed and held that a self-imposed inspection, taken alone, did not establish the standard a reasonably prudent trucking company would follow. In fact, this self -imposed standard may have exceeded the industry standard and a party should not be penalized solely for setting its internal policies higher.

That case however dealt with a third party. In legal malpractice there can also be third party claims. The concept of privity was prevailing only until the 60s when the California Supreme Court held that an attorney could be liable to third persons who suffered economic losses as a proximate result of the attorney's negligent legal practice. *Lucas v. Hamm,* 56 Cal.2d 583 (1961). Generally speaking however, cyber claims will be made by clients who have a relationship with the lawyer. Those clients can argue that they have signed up with counsel, expecting a higher standard of care, as the plaintiff in *FFE Transportation Services* tried to do.

B. An Attorney Specialist

If the attorney is a specialist in his or her field, it will be held to the standard of care of a specialist. *Wright v. Williams,* 47 Cal.App.3d 802, 810 (1975). This suggests that if an attorney holds him/herself out as someone who is an expert in providing security to clients who especially need it (such as the Mossack Fonseca clientele) then it is possible that such law firm could be charged with having its guard down, even if the typical law firm would not. In connection with the Mossack Fonseca situation, the firm clients may be able to argue that Mossack Fonseca attracted the clients by advertising its higher security and confidentiality levels; yet third parties caught up in the breach may not be able to make a claim based on a higher standard.

While the standard of care is limited to the object of representation *Calloway v. State* (1926) 117 Okla. 43, expansion of liability is possible as a result of changes in the legal practice. The heightened complexity of the law, development of specialization and the growth of methods of communication increase exposure. This suggests that while specialists may be in a unique place today, tomorrow that will become the new standard for all attorneys.

C. Compared to Medical Standard of Care

In order to better understand how standard of care would work in data breach cases we need to examine standard of care in other contexts. Attorneys have often been compared to physicians. *Wimsatt v. Haydon Oil Co.*, 414 S.W.2d 908(Ky. App. 1967); *Cook v. Irlon,* 409 S.W.2d 475(Tex. Civ. App. 1966). Many States in fact have a much

more developed case law on medical malpractice compared to legal malpractice. Gary L. Putnam, *The State of Legal Malpractice in Oklahoma*, 9 Tulsa L. J. 129 (1973). Doctors deal with cutting edge technology to run the newest procedures, and they rely on computers to provide information such as, conflicts in medications and patient history. Doctors are charged when they fail to use the most advanced procedures and medications to cure their patients, and they are also charged when those systems fail to protect their patients. Attorneys commonly communicate over cyber space. They store client information on computers, generate documents, and communicate confidential information by e mail. Why should treating attorneys be any different, from the standard we treat our physicians?

D. Defining Standard of Care, Use of Experts and the Community Standard

The duty in a standard of care case is the hypothetical prudent person. *Ishmael v. Millington*, 243 Cal.App.2d 520 (1966). In legal malpractice the reasonable man is the customary professional "conduct;" not a person. *Cervantes v. Forbis*, 73 N.M. 445 (1964). This means that expert testimony is necessary to testify about the prudent conduct. Interestingly, this testimony is a self-evaluative opinion regarding the profession. In that regard, it can potentially protect the profession from a higher criteria that would not reflect the needs of the legal profession as a whole. In other words, we should only expect that experts will testify about measures used and applicable to attorneys. Attorneys are not advanced in technology as other professionals. That said, in some cases, where the jury can determine without expert testimony whether the client would have prevailed on a particular point, expert testimony is not required. See e.g., *Tarleton v. Arnstein & Lehr*, (Fla. 4th DCA 1998)719 So. 2d 325. Are attorneys at risk that the general population expect them to be savvy in technology as the younger population is?

Legal standard of care has been defined in many ways. Whether the standard is that of a lawyer with 'ordinary skill and capacity commonly possesses and exercises' (*Theobald v. Byers*, 193 Cal.App.2d 147 (1961)), that a client has a right to 'a fair average of professional skill and knowledge' (*Cochrane v. Little*, 71 Md. 323, 326 (1889)), that attorney must be as 'well informed members of the profession' (*Roehl v. Ralph*, 84 S.W.2d 405, 409 (Mo. App. 1935)) or that the 'skill and diligence required of an attorney is such as a man of ordinary prudence gives his own business' (*Williams v. Knox*, 10 N.J. Super. 384, 385 (1950)), it all relates in one way or another on <u>other members of the profession</u>. That is how objectivity is met. There is also a subjective component of using best judgement under the circumstances (the judgement immunity defense).

Therefore, we can expect that as technology continues to control all aspects of our lives there will be a cyber standard to attorneys as there is to doctors. There will also be some comparison to members of the profession. Yet when reviewing medical malpractice cases and legal malpractice cases one would note that the difference is that in medical malpractice the locality and school are important, but are not much of a factor in legal malpractice. *Rhine v. Haley*, 238 Ark. 72 (1964). This make it harder for attorneys.

Attorneys may not be considered proficient in technology as doctors may be, but if there is a standard of care issue the attorneys can be compared to an industry trend, even if it had not yet reached their locality or type of practice.

V. Is Data Security Part of the Standard of Care?

California Rules of Professional Conduct, Rule 3-110 (Failing to Act Competently) provides: "(A) A member shall not intentionally, recklessly, or repeatedly fail to perform legal services with competence. (B) For purposes of this rule, "competence" in any legal service shall mean to apply the 1) diligence, 2) learning and skill, and 3) mental, emotional, and physical ability reasonably necessary for the performance of such service. (C) If a member does not have sufficient learning and skill when the legal service is undertaken, the member may nonetheless perform such services competently by . . . 2) by acquiring sufficient learning and skill before performance is required."

A typical lawsuit for security breach can allege that the attorney was reckless by its lack of diligently acquiring sufficient learning skills how to protect data that is on the attorney's computer. This also relates to maintaining client's confidences. If an attorney allows a third party to be present in a client meeting or holds a client meeting at a public place where others may eaves drop, then everyone would agree that the attorney breached its duties. Hence, why would the standard be different if the issue is cyber data? Perhaps if cyber breach was new or even an unknown risk the attorney should not be charged with it, but cyber liability has become a common risk.

VI. Can Cyber Attacks Raise the Standard of Care?

As we all know, cyber attacks are ever more likely and are becoming a constant threat on the way we communicate and store information. Since attorneys' work primarily involves documents and communications and they also deal with clients' funds, they are more likely to be attacked (albeit, they are not as uninformed and naïve victims).

Because the expense of a cyber attack is huge (including, notification and interference with the business) surely attorneys are taking greater measures of protection. There is no standard of what that measure of protection should be, as there is for hospitals for example, who store patients' personal information. Therefore, when a breach occurs, the question will be whether the measure of protection taken by the attorney was reasonable conduct.

It is not obvious that a breach of security means that the attorney acted below the standard of care. First, there is no clear standard and second, because the protection of the client's property and confidences are ethical responsibilities, and not necessarily violations that would lead to a civil claim of breach.

If the claim is that a higher standard was expected, that claim should only belong to the client himself/herself. That appears to be more of a claim of breach of warranty otherwise covered by a contractual relationship. As to claims by clients, they may to

some extent relate to the legal community. As the community at large becomes better at protecting cyber data, so should every individual attorney office. The claim can be trickier when there is an intervening cause like a theft of a password by an employee. Will attorneys be charged with vetting their employees better? Having office policies as to how to use the internet? Also, what if the cause of breach was by another attorney at the firm? Obviously, the analysis will be based on a case by case. If an attorney complies with all measures of security but another attorney at the firm caused the breach, in those instances perhaps the law firm who employed the attorney that caused the breach would be responsible but not the attorney who directly represents the victim client but did not cause the breach.

To the extent that grounds exist to make a claim we should also consider how a victimized client would be able to make such claim. If the client's illegal activities were exposed then surely he/she would not be able to make a claim. If confidential information was exposed, that client may not wish to make that even more public. Also, the attorney defending him/herself will have to be able to discuss causation and damages by claiming that the more secured confidential information was not disclosed, that the information disclosed did not affect strategy or, that the client would have lost the issue--as the case may be-- irrespective of the breach. Such defenses may be impossible in on going cases without hurting the clients and therefore, clients may not jump quickly into making security breach claims.

To conclude, increased security probably will raise the standard, but the claim may not necessarily be a 'standard of care' type claim. Lawsuits alleging such breaches however, could be fewer because of the nature of the data that was leaked and the relationship with the attorney and lastly, the stronger claims will be made by the clients and not by third parties caught in the breach.