VOLUME 9, ISSUE 4

PROFESSIONAL LIABILITY DEFENSE QUARTERLY

FALL 2017

INSIDE THIS ISSUE:

OUR 2017-2018 MISSION LEVEL SPONSOR:

SPECIAL POINTS OF INTEREST:

- Young Professionals Committee Formed
- Board of Directors Meet January 18-19, 2018 Hollywood, Florida
- Committees are Reformed—See Website
- Use Website to Make Blog Posts—Showcase Expertise

LAW FIRM CYBER BREACH AVOIDANCE TIPS, BY: DEBORAH BJES, J.D., C.P.C.U.

The Cyber Breach

Unfortunately, law firms are still regarded as "soft" in the comparative world of cyber targets. Many law firms use systems that are easier to penetrate than those of their more sophisticated clients. This imbalance in technology leaves the law firm as the weakest link in the data chain and an obvious target for cyber criminals.

Further, lawyers, even if employed at firms with sophisticated systems, are vulnerable to socially engineered attacks. Lawyers must work efficiently, look for new opportunities, and look to assist and procure potential clients. Many lawyers will therefore click the links contained in unsolicited emails and continue to fall for phishing scams.

Indeed, a 2015 Legal Technology Survey found that at least 80 of the 100 biggest law firms in the country had been hacked. Smaller firms are also increasingly subject to incidents involving ransomware and pay bitcoin ransoms to recover data.

Competence and Confidentiality

In addition to a financial and a practical problem for lawyers, a cyber incident may lead to ethical problems as well. The ABA Model Rules have evolved to address technology and it is no longer acceptable for a lawyer to simply claim technological ignorance. What follows is a reminder of how the ABA Model Rules speak to technology:

<u>ABA Model Rule 1.1: Competence, Comment [8]</u>

"To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject."

<u>ABA Model Rule 1.6, Confidentiality</u>

"(c) 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] and [19]

No lawyer wants to be the subject of a grievance or law suit as a consequence of technological incompetence and/or the failure to protect confidential client information.

Tips for Maintaining Confidentiality in the Cyber World

1. <u>Find/Cure Your Weakest Links</u>

All attorneys, staff, and vendors must exercise the utmost level of cybersecurity care, awareness and diligence. Training in cyber breach prevention and mitiga-

Continued on page 2

LETTER FROM THE PRESIDENT, BY: ERIN K. HIGGINS, ESQ.

The cold weather is finally arriving in Boston, and a trip to New Orleans next fall is starting to seem very appealing! Please mark your calendars now for our next PLDF Annual Meeting, on October 3-5, 2018, at the Westin Canal Park. The Board and the Program Committee will be working hard over this next year to assemble another terrific slate of programming, and more of our memorable field trips and group dinners.

Thank you to those who attended the 2017 Annual Meeting in Chicago. We had a record number of attendees, and the member feedback has been terrific. If you have any thoughts about how to make next year's meeting even better, please e-mail Chris Jensen, or anyone on the board, with your thoughts and suggestions.

One idea that came out of the 2017 Annual Meeting was to start a Young Professionals Committee, for those lawyers and claims professionals who have been in the industry for ten years or less. Molly Eiden of Minnesota Lawyers Mutual is spearheading

Erin K. Higgins of Conn Kavanaugh Rosenthal Peisch & Ford LLP of Boston, Massachusetts, is President of PLDF. She may be reached at ehiggins@connkavanaugh.com.

Continued on page 16

CYBER BREACH AVOIDANCE TIPS, CONT'D

Θon should be mandatory for everyone in every law ļrm, including founding partners and recepΘonists. Employing a technologically proļcient team is the best prevenΘon.

2. Enforce Polices to Curtail Human Error

The majority of all security incidents are caused by human error. Consequently, the most sophisΘcated security system in the world is irrelevant if the potenΘal for human error is unaddressed. For example, one law ļrm with a strong security system discovered someone had accessed client ļles. AŌer performing numerous systems checks, the law ļrm ulΘmately discovered that an employee kept her passwords on a notepad in her unlocked desk drawer. A member of the cleaning staī found the notepad and was able to access client ļles.

Further, many law ļrm partners sΘll send conļdenΘal informaΘon from personal email accounts, use public Wi-Fi systems while waiΘng for Ňights or having coī ee, and take other risks, such as failing to password protect their smartphones. Training and enforcement of cyber policies for everyone in the ļrm is necessary to avoid these common human errors that rouΘnely lead to cyber breaches.

3. Send Fake Emails

To further provide cyber security training, a number of corporaΘons now rouΘnely send fake phishing emails to test their employees' cybersecurity awareness and to gather open rates. These corporaΘons then advise their employees of the open rate percentage and instruct them regarding the red Ňags that were ignored. For example, employees may ignore a change in the senders email address protocol, fail to hover over a link before clicking it (the name displayed may indicate that the link is not as represented), and may ignore other inconsistent informaΘon that would indicate that the email is a fraud. CorporaΘons hope that this type of feedback is eī ecΘve in encouraging employees to exercise more care before opening the next link or providing their informaΘon to a potenΘal thief. CorporaΘons also encourage staī to share any phishing emails that they receive for analysis and discussion.

4. Pause Before Sending Text Messages and Emails

The "reply to all' key has been responsible for conļdenΘality breaches, embarrassment and awkwardness. Further, accidentally sending to the wrong "Mary" or not realizing the actual plainΘī has been copied on a document can cause further problems. Disabling the "reply to all" buΣon and pausing an extra second before pushing "send" to review the distribuΘon list is obviously good pracΘce.

Further, we have all likely read about a certain athlete's aΣorney who accidentally texted a reporter a sentence that started "Heaven help us…" Perhaps simply avoiding the text message in a professional setļng is the best idea. While a text may be a great way to communicate with friends and family, it is not the ideal form of communicaΘon to use professionally due to its fast and informal nature.

5. Encrypt

EncrypΘon is the best alternaΘve for protecΘng sensiΘve data. Encrypted data is unreadable if a cell phone or computer is lost or if the data ends up in the wrong hands. EncrypΘon, however, is the least used security feature found in most law ļrms. While encrypΘon of all ļles is currently not ethically mandated, the failure to encrypt could arguably be viewed as a breach. ABA Model Rule 1.6 reads:

…This duty, however, does not require that the lawyer use special security measures if the method of communicaΘon aī ords a reasonable expectaΘon of privacy. Special circumstances, however, may warrant special precauΘons. Factors to be considered in determining the reasonableness of the lawyer's expectaΘon of conļdenΘality include the sensiΘvity of the informaΘon and the extent to which the privacy of the communicaΘon is protected by law or by a conļdenΘality agreement. Comment [19]

Lawyers should therefore evaluate the security needs of the actual data for each engagement to make sure that the conļdenΘality needs of their clients are adequately protected. Obtaining the client's wriΣen consent before using email or text messaging to communicate with them, while advising of potenΘal conļdenΘality issues, is also advisable. If your law ļrm does not encrypt data, disclose that to the client and provide them with the opportunity to refuse email communicaΘons from your ļrm.

6. Passwords

Law ļrms should encourage strong passwords. The password should contain leΣers, both upper and lower case, characters, and numbers. Passwords should be changed regularly (every 90 days) and never repeated. One idea is to anchor your password to a phrase instead of a word. For example "She Loves to travel to Warm Weather and go swimming" can translate to the following password by using just the ļrst leΣer of every word, with capitalizaΘon every so oŌen: SLΣtWWags. The value to this new password is that it is very hard to guess without knowing the original sentence, but yet easy to remember. Adding numbers and characters will then create a stronger password. Another opΘon is to use a secure password generator.

7. The Cloud

While many aΣorneys conceptually understand that informaΘon stored in a cloud is stored oī site, many have no idea that depending upon the vendor, cloud data could be stored internaΘonally, governed by foreign law, and subject to search and seizure. Further, if an aΣorney places data in the cloud that is subject to

> "[A] number of corporaΘons now rouΘnely send fake phishing emails to test their employees' cybersecurity awareness."

CYBER BREACH AVOIDANCE TIPS, CONT'D

state or federal privacy laws, the client should first provide their informed and written consent for such storage (adding this item to the engagement letter may be an option). Finally, the attorney should check with the bar association for their respective state's ethical opinions that govern cloud storage.

8. Update Your Systems

Law firms should update their systems, including the VPN, antivirus, anti-spyware and spam filters routinely. Class action lawsuits arising out of data violations are exploding and the first public data security class action complaint against a law firm was recently filed in Federal Court in Chicago. The plaintiffs allege that the firm's outdated systems failed to protect client data. Damages are sought for the threat of a breach and the "diminished value" of the law firm's services. Law firms should periodically update systems.

9. Vet Vendors

Vendors have been identified as the weak link in certain large exposure hacking incidents. Recall that the Target hackers were able to access the chain's security systems by stealing credentials from a vendor. Examine all vendors' cyber security protocols (does the vendor encrypt data, use a VPN system) as well as the vendor's insurance policy and all controlling contracts. Understand where the vendor will store the information – international storage may present problems. Examine indemnification clauses and provisions regarding who will be expected to pay in the event of a data breach.

10. Have a Plan

Every law firm should establish a plan to follow in the event of a cyber breach. Further, like fire drills, law firms should practice cyber drills. Are documents routinely backed up? Are copies of the most important documents at an off-site, secure location? In the event of a hack or a ransom, does everyone know who to call? Vendors should be selected ahead of time so that in an emergency, the law firm is not panicked and scrambling. For example, privacy counsel, to establish immediate privilege and provide notice requirement advice, can easily be researched ahead of time. Selecting or creating a list of professionals to assist with restoring data or handling a ransomware incident should also be researched. Finally, cyber liability coverage can help to not only cover the costs related to a data breach, such as notification expense and regulatory fines, but can also provide professionals to assist in case of an emergency.

Deborah Bjes is a dedicated risk manager for the Lawyers Professional Liability Group with Swiss Re Corporate Solutions. Deborah is a licensed Illinois attorney and a graduate of Loyola University Chicago School of Law, where she received her J.D. cum laude. She may be reached at deborah_bjes@swissre.com.

PLDQ's Winter 2018 Issue

We encourage member submission of articles pertinent to professional liability claims administration, defense trial advocacy, or professional liability substantive law. The manuscript deadline for the next issue is:

February 1, 2018.

"[C]reating a list of professionals to assist with restoring data or handling a ransomware incident should also be researched."

WEAKENING MEDIATION CONFIDENTIALITY: PROS AND (MOSTLY) CONS, BY LOUIE CASTORIA, ESQ.

In mythology, Pandora opened a forbidden box, loosing all the world's woes upon humankind. One might think we would have learned not to look into forbidden boxes or to kick hornets' nests, but our pointless curiosity sometimes gets the best of us.

California's Law Review Commission (the "California Commission") has proposed an amendment to the state's Evidence Code, carving out a substantial exception to the near-absolute confidentiality of communications during and preparatory to mediations.

In 2012 the California Legislature directed the California Commission to analyze "the relationship under current law between mediation confidentiality and attorney malpractice and other misconduct," in response to a California Supreme Court decision, Cassel v. Superior Court, 244 P.3d 1080 (S.Ct. Cal., 2011), which had strictly construed the state's mediation statutes in its Evidence Code to require confidentiality of all mediation communications, except as expressly excluded.

The proposed change would allow communications into evidence in attorney malpractice cases, disciplinary proceedings, and fee disputes when "relevant to prove or disprove an allegation that a lawyer breached a professional requirement when representing a client in the context of a mediation or a mediation consultation[.]"

Proponents of the statute, which would become California Evidence Code 1120.5, if enacted into law, focus on a perceived unfairness to clients who sue their lawyers for malpractice, and to lawyers defending themselves against such suits, when the alleged misconduct occurs within the sanctum sanctorum of mediation.

The potential impact of the proposed statute extends beyond the Golden State. This article addresses the current inconsistency among state and federal laws governing the inviolability of mediation communications, and argues against opening Pandora's box, even just to take a peek inside.

Inconsistency of Mediation Confidentiality Laws

The Uniform Mediation Act ("UMA"), drafted by the National Conference of Commissioners on Uni-

WEAKENING MEDIATION CONFIDENTIALITY, CONT'D

form State Laws, provides broad conţ denęality for all communicaęons made in mediaęons, but carves out communicaęons "sought or oī ered to prove or disprove a claim or complaint of professional misconduct or malpracęce" ţ led against a mediator, party, paręcipant, or representaęve at a mediaęon. Other excepęons exist in the UMA, such as communicaęons during pretextual mediaęons, such as ones held to advance criminal schemes.

The UMA has been enacted in eleven states and the District of Columbia, with some modiţ caęons. (Those states are: Hawaii, Idaho, Illinois, Iowa, Nebraska, New Jersey, Ohio, South Dakota, Utah, Vermont, and Washington. It has been proposed in New York and MassachuseΣs.) The California Commission's proposal does not track the UMA, though it shares a similar carve-out for malpracęce cases.

Surveying other states' laws and judicial rulings, the California Commission concluded:

> The statutes and rules protecęng mediaęon communicaęons vary widely from state to state. Among other things, they diī er in whether, and to what extent, they permit the use of mediaęon communicaęons in resolving an allegaęon of aΣorney misconduct. In seven states (plus the UMA states), a statute or rule protecęng mediaęon communicaęons has one or more excepęons that expressly addresses alleged aΣorney misconduct or alleged professional misconduct more generally (thus encompassing aΣorney misconduct). Those states are Florida, Maine, Maryland, Michigan, New Mexico, North Carolina, and Virginia.

The California Commission's full survey of the states' laws and judicial ruling on mediaęon conţ denęality may be downloaded at: hΣp://www.clrc.ca.gov/pub/2017/MM17-30.pdf. Please see pages 57 through 70, and the numerous footnotes therein for speciţ c states' laws.

In contrast, the Federal Rules of Evidence do not include a "mediaęon privilege," as such. Rule 408 excludes evidence of seΣlement communicaęons from being introduced to show a party's liability or lack thereof in an underlying claim, but provides no protecęon for other uses of such evidence. Some federal courts have used Rule 501, which states that they shall "be governed by the principles of the common law as they may be interpreted by the courts of the United States in the light of reason and experience," to protect mediaęon conţ denęality, recognizing that it generally exists in other jurisdicęons. However, a court-by-court approach provides neither lięgants nor lawyers suĸ cient guidance as to what they may say in a mediaęon with conţ dence that it will not be repeated.

California's current mediaęon statutes are found in its Evidence Code, secęons 1115 through 1128. They create a comprehensive structure for mediaęons, including conţ denęality, but also conclusively answering quesęons that have vexed other states, and are not resolved by the UMA. The following is an abbreviated summary of the key points as to conţ denęality in California:

- Conţ denęality applies to all communicaęons, oral and wriΣen, in a mediaęon and in preparatory mediaęon consultaęons.
- It is not necessary for the paręes to agree in wrięng that the mediaęon is conţ denęal, though they may waive conţ denęality by mutual, wriΣen agreement.
- No one may be subpoenaed to tesęfy about, in any non-criminal proceeding, or produce records of communicaęons made in a mediaęon.
- Conţ denęality does not apply to certain informaęon exchanged in family law cases, nor to judicial seΣlement conferences.
- Noncommunicaęve conduct during a mediaęon is not conţ denęal. As an example, a derogatory comment regarding an opposing party's parentage is conţ denęal, but a physical assault or baΣery is not.
- Any reference to a mediaęon communicaęon at trial is treated as an irregularity, potenęally leading to a mistrial and/or sancęons. In other noncriminal proceedings such a reference is grounds to vacate or modify a ruling made in such hearings.
- A wriΣen, signed seΣlement agreement that is created at a mediaęon is admissible to prove that a seΣlement was reached and on what terms.

(Comment: it is common in California, though not required, that the paręes use a Sępulaęon for SeΣlement under California Code of Civil Procedure secęon 664.6 to memorialize the seΣlement terms. This document may be ţ led with the court in which the case is pending to enforce its terms, without any party needing to inięate a separate acęon for breach of contract. If the seΣlement terms are complex or open-ended on any point, a 664.6 sępulaęon may not be feasible.)

With potenęally conÑicęng standards in state and federal courts, it is important to know which state's law applies and what it provides, rather than assuming conţ denęality. Many mediators thus require the paręes and counsel to sign mediaęon conţ denęality agreements at the beginning of mediaęon sessions.

Courts generally uphold such agreements, as famously occurred in Facebook, Inc. v. Paciţ c Northwest SoÕware, Inc., 640 F.3d 1034, 1041 (9th Cir. 2011), and recounted in the ţ lm, "The Social Network." Mark Zuckerberg's college collaborators, the Winklevoss brothers, sought to undo their signed seΣlement agreement with him based on communicaęons during

> "The [Uniform Mediaęon Act] has been enacted in eleven states and the District of Columbia, with some modiţ caęons.."

WEAKENING MEDIATION CONFIDENTIALITY, CONT'D

a mediaϴon that resulted in the seΣlement. The parϴes had signed a conĮdenϴality agreement in advance of the mediaϴon, which the court upheld as valid. However, such agreements do not bind persons who are not in the room and may have an interest in the seΣlement amount or terms.

Indisputably SeΣled?

Imagine the following situaϴon: a securiϴes broker leaves a brokerage Įrm in New Mexico to join a similar Įrm in Colorado, taking a client list with her, and claiming that she generated the list before she joined the New Mexico Įrm. The broker and the two Įrms agree to mediate their dispute in neutral territory, California, and to use a private, solo pracϴϴoner mediator in Santa Barbara.

At the end of a twelve-hour mediaϴon the parϴes agree on a seΣlement amount and sign a term sheet that uses the term "the Subject Accounts" to describe the scope of the mutual release. Later, a dispute arises as to which of two account lists consϴuted the Subject Accounts. The broker and Colorado Įrm Įle suit in Denver for breach of contract against the New Mexico Įrm (assume proper jurisdicϴon). The broker's estranged husband, who used to be her partner in her original brokerage, gets wind of the seΣlement and sues in New Mexico, claiming rights to the seΣlement amount under his partnership agreement with the broker and New Mexico's community property law.

Here are three issues that arise from this fact paΣern—there are several others that could be posed:

- Does California law govern the admissibility of communicaϴons during the mediaϴon regarding which list contained the Subject Accounts?
- If the parϴes signed a conĮdenϴality agreement at the mediaϴon, does it bar the husband from obtaining through discovery the parϴes' mediaϴon briefs, or deposing the mediator?
- The broker later claims that the aΣorney who jointly represented her and the Colorado Įrm failed to disclose a conŇct of interest, and urged her to seΣle at an unreasonable number to beneĮt the lawyer's other client, the Įrm. She Įles a third-party complaint against the aΣorney in the Colorado acϴon, seeking to void the seΣlement agreement, and money damages. Can the aΣorney's advice to her during the mediaϴon be introduced in evidence?

My views on the above quesϴons:

- Neither Colorado nor New Mexico is bound to follow California law, unless the parϴes to the mediaϴon all agreed in wriϴng that California law would govern. However, both states recognize mediaϴon conĮdenϴality to a lesser degree than California.
- The mediaϴon parϴes' conĮdenϴality agreement does not bind the husband, a non-signatory. New Mexico law would govern his rights to discovery, if any.
- The Colorado aΣorney was not a party to the California conĮdenϴality agreement, and should not be bound by it. To defend himself against the malpracϴce claim he should be able to introduce evidence of what he recommended, as can the broker in prosecuϴng her third-party complaint against him. Note that the husband's subpoena to the mediator in Santa Barbara can probably be quashed by a California court on the basis that he conducted the mediaϴon in California.

Please note that these views are debatable under present law. The draϴers of the UMA recognized a beneĮt of uniform mediaϴon conĮdenϴality statutes, and posed an even more perplexing scenario: "Mediaϴon sessions are increasingly conducted by conference calls between mediators and parϴes in diī erent States and even over the Internet. Because it is unclear which State's laws apply, the parϴes cannot be assured of the reach of their home state's conĮdenϴality protecϴons." (Prefatory Note to the UMA)

The California Proposal

The California Commission seems to be ready to muddy the currently clear waters of California's mediaϴon conĮdenϴality. Proposed Evidence Code secϴon 1120.5, if adopted by the Legislature and signed into law, would diminish the nearly absolute conĮdenϴality rule in civil cases, eī ecϴve on January 1, 2019, under a two-pronged test:

- The evidence must be relevant to prove or disprove an allegaϴon that a lawyer breached a professional requirement when represenϴng a client in the context of a mediaϴon or a mediaϴon consultaϴon
- The proceeding in which the evidence is proī ered must be an acϴon for damages based on alleged malpracϴce, a disciplinary proceeding, or a fee dispute between lawyer and client.

A pleading that meets these tests must be served by mail on all mediaϴon parϴcipants whose whereabouts can be idenϴĮed. The court may use a sealing order, a protecϴve order, a redacϴon requirement, an in camera hearing, or a similar judicial technique to prevent public disclosure of mediaϴon evidence, but is not required to do so.

The proposed law would make mediators exempt from providing tesϴmony or documents in a mediaϴon malpracϴce case, except in criminal cases and a few other kinds of cases. Mediators are not made immune

> "The proposed law would make mediators exempt from providing tesϴmony or documents in a mediaϴon malpracϴce case …"

PLDF AND DIVERSITY

The Professional Liability Defense FederaϴϴOn supports diversity in our member recruitment eī orts, in our commiΣee and associaϴon leadership posiϴons, and in the choices of counsel, expert witnesses and mediators involved in professional liability claims.

WEAKENING MEDIATION CONFIDENTIALITY, CONT'D

from liability by the proposed law, nor is any exis€ng mediator immunity revoked. (In some situa€ons mediators may have quasi-judicial immunity.)

Sec€on 1120.5, as currently dra©ed, does not limit the gathering or use of media€on evidence in a malprac€ce case to the client and a∑orney in ques€on. As the requirement of service by mail upon all par€cipants hints, the plain€ ī and defendant may introduce evidence from other par€cipants (except the mediator), thus resurrec€ng a dispute that those par€cipants considered se∑led, and poten€ally revealing their con¦ den€al communica€ons with the defendant-a∑orney at the media€on.

One can easily imagine a law-and-mo€on morass for a trial court judge, umpiring the calls of "fair" and "foul" in discovery requests and depsi€on ques€ons among par€es and nonpar€es, all over a case that, by de¦ ni€on, was se∑led or that the par€es tried to se∑le.

If It Ain't Broke: Public Comments on the Proposal

As the California Commission candidly noted about the public comments on its proposed statute, "The 155 pages of comments include sca∑ered words of praise or appreci€on for the Commission, its staī , its process, and its work on this study. In general, however, they do not have much posi€ve to say about the Commission's proposal."

The main arguments advanced by those suppor€ng the proposal are that it allows plain€ ī s and defendant-a∑orneys to introduce evidence that may be crucial to their respec€ve cases, and that a malprac€ce excep€on to media€on con¦ den€ality would bring California more in line with other states.

Against the proposal is an array of judicial, legal, and media€on organiza€ons, including the California Judges Associa€on, and the Academy of Professional Family Mediators, the California Dispute Resolu€on Council, and the Center for Con Ñ ct Resolu€on. The proposal accomplished one thing that no one would have predicted: the Consumer A∑orneys of California and the California Defense Counsel submi¦ ng a joint le∑er opposing it—a rare example of something they agree upon.

Both sides of the debate advance a "why ¦ x it" argument, the proponents saying that in states where there is no malprac€ce excep€on to media€on con¦ den€ality there appears to be no reluctance to mediate, and the opponents poin€ng out that there is li∑le evidence that media€on-malprac€ce cases are more prevalent in those states than in California.

In this writer's opinion, both sides miss the point: media€on-malprac€ce cases are few and media€on use is high not because of statutes governing media€ons, but because media€ons have become a principal and eī ec€ve way of resolving civil disputes. Once thought "novel," media€ons have become de rigueur in modern li€ga€on. Media€ons work because they allow li€gants a chance to step away from the brink, to see the case from the other side's or sides' viewpoints. For counsel, media€ons provide a neutral messenger, someone with an aura of authority to deliver hard facts to all par€es, without being thought a traitor to any client, because the mediator has none.

There are cases of "se∑ler's remorse," in which a party gets cold feet a©er signing a se∑lement agreement. California puts a par€cularly high burden of proof on such cases, proof to a "legal certainty" that a be∑er result would have been obtained if the case had bee tried to verdict. (Filbin v. Fitzgerald, 343 P.2d 118 (Cal. Ct. App. 2012).) California imposes a high threshold on the admissibility of media€on communica€ons, I believe for the same reason: the ¦ nality of mediated se∑lements is essen€al to the func€oning of the most populous state's underfunded judicial system. Forcing overcrowded courts to consider Mulligans on se∑led cases, under the guise of se∑le-and-sue or media€on-malprac€ce, is a waste of scant judicial resources. Cases se∑le at media€on because media€ons work.

Another argument that appears in the public comments on proposed sec€on 1120.5 is the par€es' "right to choose" con¦ den€ality. Exactly where this right springs from is unclear, but if it does exist, the burden to explain it would fall upon counsel on a case-by-case basis, whereas under current law it is a given, like the statute of limita€ons, the rule against perpetui€es, and the in¦ eld Ñ y rule. Public policy dictates that some rules be made by the Legislature and be uniform, elsewise every decision is arguable.

"Media€on privilege," as it is some€mes called, is a rule of evidence, not an immunity from liability. A∑orneys can s€ll be sued from malprac€ce during media€ons, but neither side can rely on the he said/she said evidence of what is said during those hours of nego€a€on. Other evidence—communica€ons before and a©er a media€on, such as privileged emails and pre-se∑lement tes€mony—can be introduced. If the pre-media€on evalua€on by counsel says the case is worth $500,000 and it se∑les for $5,000, those facts get into evidence.

We rou€nely accept eviden€ary restric€ons in other communica€ve contexts—penitent/confessor, doctor/pa€ent, spouse/spouse. In those contexts the privacy of the communica€on is only of interest to its two par€es, but in a media€on all par€es, even adverse ones, share the same interest that none of their con¦ den€al communica€ons be disclosed. Disclosure by one opens the door to disclosure by all.

As dra©ed, sec€on 1120.5 allows any "relevant" inform€on into evidence, not only the communica€on between the client (now plain€ ī) and the a∑orney (now defendant). In a real sense, all par€cipants in a media€on are the holders of the privilege, which ex-

PLDF COMMITTEES

PLDF's 11 substan€ve com-mi∑ees include:

- Medical
- Legal
- Accoun€ng
- Investment
- Corporate Governance
- Insurance
- Real Estate
- Construc€on Design
- Cyber Security
- Employment Prac€ces
- Miscellaneous PL

> "'Media€on privilege,' as it is some€mes called, is a rule of evidence, not an immunity from liability."

WEAKENING MEDIATION CONFIDENTIALITY, CONT'D

plains why they are all entitled to written notice of a mediation-malpractice suit.

There is a value to uniformity, but also to diversity and experimentation. California has a stronger mediation confidentiality statute than other states because it needs one. It may not be the answer for all, any more than its three-year statute of limitations for fraud needs to be universal. But it works. It ain't broke.

Louie Castoria is a professional liability defense and coverage attorney, and is the Co-Managing Partner in Kaufman Dolowich & Voluck LLP's San Francisco office. He is California-certified mediator and a Hearing Officer under contract to the City and County of San Francisco. Louie may be reached at lcastoria@kdvlaw.com.

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

CONTRACTOR LICENSURE REQUIREMENTS: BEWARE!, BY: GLEN OLSON, ESQ. AND ARI BARUTH, ESQ.

California law allow for harsh results when contractors and/or owners overlook state licensure requirements. The issue most often hits the radar screen too late – after a dispute arises and the parties are in litigation. A recent California decision addresses this particularly dangerous area for contractors, in which even creative pleading by the plaintiff can sometimes not save the day. Design professionals need to be aware of the current state of the law in this area in the event they are in litigation with unlicensed contractors.

California Business & Professions Code § 7031(a) requires a party to maintain an active contractor's license throughout the project at issue in order to maintain or defend an action for compensation for services performed for which a contractor's license is needed. In Phoenix Mechanical Pipeline, Inc. v. Space Exploration Technologies Corp., (Cal. Ct. App. June 13, 2017), California's Second Appellate District Court of Appeal interpreted this statute in denying, in part, Phoenix Mechanical Pipeline, Inc.'s ("Phoenix Pipeline") appeal of a trial court ruling granting Space Exploration Technologies Corporation's ("SpaceX") demurrer to Phoenix Pipeline's second amended complaint, without leave to amend.

Phoenix Pipeline contracted with SpaceX to provide plumbing, concrete removal and electrical services. Phoenix Pipeline alleged SpaceX paid for such services from 2010 to October 2013, but failed to pay Phoenix for just over $1,000,000 in services performed from October 2013 to August 2014. Phoenix Pipeline contended this work was performed pursuant to a series of invoices constituting individual agreements between SpaceX and Phoenix Pipeline and alleged causes of action for breach of contract and breach of the covenant of good faith and fair dealing.

SpaceX demurred to the initial complaint, arguing Phoenix Pipeline was not licensed. Phoenix Pipeline elected to file a first amended complaint and added allegations that it had a licensed "responsible managing employee" on the job. This individual owned a separate entity, Phoenix Mechanical Plumbing, Inc., which "oversaw all services" provided by Phoenix Pipeline.

SpaceX filed another demurrer, arguing the employee's license failed to satisfy the requirements of section 7031(a). SpaceX's demurrer was sustained with leave to amend.

Phoenix Pipeline then filed a second amended complaint with two modifications. It recast the licensed "responsible managing employee" as a "responsible managing officer" and expanded the description of the employee's role on the project. The second amended complaint also distinguished between "subcontracting services" for which a license was required and "non-contracting services" for which no license was needed.

SpaceX again demurred based on Phoenix Pipeline's continued failure to allege it held a contractor's license. The court sustained the demurrer without leave to amend, prompting an appeal.

The appellate court weighed whether Phoenix Pipeline's allegations were sufficient to overcome the requirement in section 7031 that it must have had a valid license to recover in an action for payment for services for which a contractor's license is necessary. The Court of Appeal found Phoenix Pipeline's pleading failed to meet that standard.

First, the Court held that Phoenix Pipeline failed to allege that Phoenix Pipeline – as opposed to another entity - held a contractor's license, and cited various decisions interpreting section 7031 to provide that the failure to comply with the licensing requirements of the statute bars a person or entity from recovering compensation for any work performed under a contract that requires a contractor's license. We examine those decisions in the following section below in evaluating the potentially draconian results for a contractor working without proper licensure.

Second, the Court held that alleging a "responsible managing officer" fails to meet section 7031's requirement that Phoenix Pipeline cannot pursue a claim without a valid contractor's license. Several

> "Design professionals need to be aware of the current state of the law in this area in the event they are in litigation with unlicensed contractors."

CONTRACTOR LICENSURE REQUIREMENTS, CONT'D

California cases have held that licenses held by partners, managing ok cers and/or owners of contracEng enEEes were insuk cient to saEsfy secEon 7031. Thus, the fact that Phoenix Pipeline alleged it had a licensed "responsible managing ok cer" at the scene, without more, did not meet the requirements of the statute.

Third, however, the Court held Phoenix Pipeline did plead suk cient allegaEons to maintain a cause of acEon for recovery for services it performed (including maintenance, repair, clean-up, hauling, disposal, etc.) which did not require a license. Since each of those invoices was alleged as consEtuEng an individual contract between Phoenix Pipeline and SpaceX, the Court overruled the trial court to the extent that Phoenix Pipeline sought compensaEon under those alleged invoices for tasks performed for which no contractor's license is required.

This decision illustrates that California courts will interpret the condiEons of secEon 7031 quite strictly, as the statute represents a "legislaEve determinaEon that the importance of deterring unlicensed persons from engaging in the contracEng business… can best be realized by denying violators the right to maintain any acEon for compensaEon." The license must be held by the contracEng enEty itself; licenses held by employees, partners, individual owners, or other ancillary individuals are not suk cient to support a claim for recovery of payment. This public decision illustrates the importance of licensure for a contractor making an ak rmaEve claim, but secEon 7031 also requires suk cient licensure in order for a contractor to defend an acEon. As outlined below, a contractor (deļ ned to also include subcontractors) cannot defend itself in an acEon for fees absent proper licensure.

Other ImplicaEons of California's Strict Contractor Licensure Requirements

California law requires that any person engaged in the business of a contractor, or that acts in the capacity of a contractor, must be properly licensed by the Contractors State License Board ("CSLB"). A contractor is deļ ned broadly, as follows:

> . . . a contractor is any person who undertakes to or oī ers to undertake to, or purports to have the capacity to undertake to, or submits a bid to, or does himself or herself or by or through others, construct, alter, repair, add to, subtract from, improve, move, wreck or demolish any building, highway, road, parking facility, railroad, excavaEon or other structure, project, development or improvement, or to do any part thereof, including the erecEon of scaī olding or other structures or works in connecEon therewith, or the cleaning of grounds or structures in connecEon therewith, or the preparaEon and removal of roadway construcEon zones, lane closures, Ňagging, or trak c diversions, or the installaEon, repair, maintenance, or calibraEon of monitoring equipment for underground storage tanks, and whether or not the performance of work herein described involves the addiEon to, or fabricaEon into, any structure, project, development or improvement herein described of any material or arEcle of merchandise. "Contractor" includes subcontractor and specialty contractor. "Roadway" includes, but is not limited to, public or city streets, highways, or any public conveyance.

Cal. Bus. & Prof. Code § 7026.

Phoenix Pipeline illustrates that an unlicensed contractor performing work in California requiring a license will likely be subject to a harsh penalty. Courts explain these requirements are designed to protect the public against incompetency and dishonesty in those who providing construcEon services. Hydrotech Systems, Ltd. v. Oasis Waterpark, 2 Cal. 3d 988, 995 (1991). For example, an unlicensed contractor may be subject to both civil and criminal penalEes. See, e.g., Cal. Bus. & Prof. Code § 7027.3 (one year imprisonment and/or $10,000 ļ ne for intenEonal use of another person's license with intent to defraud), Cal. Bus. & Prof. Code § 7028 (contracEng without a license is a misdemeanor; penalty for second oī ense is $4,500 minimum and 90 day county jail Eme), Cal. Bus. & Prof. Code § 7028.7 (CSLB citaEon and ļ ne of $200-$15,000), Cal. Bus. & Prof. Code § 7117 (CSLB disciplinary acEon); and Cal. Lab. Code §§ 1021-1023 (civil penalty of $200/day per employee performing work for unlicensed contractor).

> "[A] contractor (deļ ned to also include subcontractors) cannot defend itself in an acEon for fees absent proper licensure."

The penalEes resulEng from non-compliance with secEon 7031 include the unlicensed contractor's inability to maintain a lawsuit to recover compensaEon for its work. Moreover, a potenEally even more onerous penalty is that an unlicensed contractor may be required to disgorge any compensaEon it has previously been paid for performing work requiring a license. Cal. Bus. & Prof. Code § 7031(b). Under secEon 7031(b), "[a] person who uElizes the services of an unlicensed contractor may bring an acEon . . . to recover all compensaEon paid to the unlicensed contractor for performance of any act or contract." There is liΣle case law interpreEng the so-called "disgorgement" penalty since its addiEon to SecEon 7031 is relaEvely recent (added by amendment in 2001). Below is a discussion of the four opinions published to date addressing the topic.

PLDF Amicus Program

Please let us know of appeals in your jurisdicEons implicaEng important professional liability issues that might have naEonal signiļ cance.

CONTRACTOR LICENSURE REQUIREMENTS, CONT'D

In Wright v. Isaak (2007) 149 Cal.App.4th 1116, a contractor sued two homeowners for unpaid amounts in connecƟon with a home remodeling project. The homeowners responded with a cross-complaint against the contractor seeking, among other things, the return of all amounts they had paid him on the ground he did not have a valid contractor's license. Although the contractor was licensed, he grossly underreported his payroll to the State CompensaƟon Insurance Fund, and never obtained workers compensaƟon for his crew working on the home remodeling project.

Both the trial court and Court of Appeal agreed with the homeowners that, under California Business & Professions Code § 7125.2, the contractor's license was automaƟcally suspended for his failure to obtain workers compensaƟon insurance for his employees. The courts each rejected the contractor's argument that the suspension could not take eī ect unƟl the contractor received a noƟce of suspension from the registrar of contractors. Because the contractor failed to properly report his payroll and obtain insurance for his workers before, during and aÕer the home remodeling project, the contractor was out of compliance. Despite a seemingly draconian result, the court held that the homeowners were enƟtled to recover all amounts paid to the contractor under Business & Professions Code § 7031(b).

In Goldstein v. Barak ConstrucƟon, 164 Cal. App. 4th 845 (2008), homeowners entered into a contract with Barak ConstrucƟon to remodel their home. Barak began work on the project but failed to obtain a contractor's license for several months. The homeowners paid Barak $362,629.50 before Barak abandoned the incomplete project. The homeowners then ļ led suit under Business and Professions Code § 7031(b), seeking resƟtuƟon of the full amount paid, plus an amount for aΣorneys' fees and costs. The superior court ruled in favor of the homeowners.

In conļ rming the trial court ruling the appellate court rejected Barak's contenƟon that the recoupment acƟon was puniƟve in nature rather than a claim for money based upon a contract. It also rejected Barak's contenƟon that the amount of the recoupment was improper and excessive because Barak had passed along most of the money it received to laborers or material suppliers for the project. Though the court recognized the draconian nature of the recoupment acƟon, California law clearly allows recovery of all compensaƟon paid to the unlicensed contractor regardless of whether the amounts paid are ulƟmately retained by it. And the Court of Appeal rejected the contenƟon that the amount of the monies returned should be reduced by the amount earned by Barak aÕer it became a licensed contractor. The court reiterated that to recover for work performed on a project, a contractor must be licensed at all Ɵmes during which it performs the contractual work.

A third unlicensed contractor scenario was discussed in Oceguera v. Cohen, 296 Cal. App. 2d (2009). There, the contractor was a partnership consisƟng of three partners. Only one of the partners, Golen, was licensed. Golen executed a disassociaƟon noƟce in accordance with secƟon 7076(c) of the California Business & Professions Code which provides that "partnership license shall be canceled upon the disassociaƟon of a general partner or upon the dissoluƟon of the partnership . . . [T]he remaining general partner or partners may request a conƟnuance of the license to complete projects contracted for or in progress prior to the date of disassociaƟon or dissoluƟon for a reasonable length of Ɵme . . ."

AÕer Golen ļ led his disassociaƟon noƟce the two remaining partners began a residenƟal project. Following compleƟon, the project owner sued the partnership for defecƟve construcƟon. In addiƟon to seeking damages for repair of the defecƟve work, she also sought disgorgement of the $32,000 paid under secƟon 7031 (b). The issue on appeal was limited to whether the trial court erred in entering a judgment in favor of the owner on the refund of the $32,000. The Court of Appeal ak rmed that defendants did not establish that the substanƟal compliance doctrine applied because they were never licensed before entering into and performing work, and because Golen's associaƟon with the partnership ended on the date stated in the applicaƟon for replacing the qualifying individual. Neither of the other individuals in the partnership could saƟsfy the substanƟal compliance doctrine because neither was licensed before entering into the contract.

More recently, in White v. Cridlebaugh, F053842 (July 29, 2009), the Whites retained a contractor to build them a log cabin. Due to concerns over the contractor's billing and competency, the homeowners terminated the construcƟon contract. The parƟes ļ led complaints against one another including the homeowners' request for disgorgement of amounts paid to the contractor. The Court of Appeal considered, among other things, "whether the Whites properly brought a claim for reimbursement under secƟon 7031(b)."

The appellate court concluded that the contractor was not qualiļ ed to be licensed because it did not have a qualiļ ed responsible managing ok cer or employee in place, and that its license therefore was suspended by operaƟon of law. Hence, the Court ordered reimbursement of all monies paid to the contractor under secƟon 7031(b). The Court further considered whether "the recovery of compensaƟon authorized by secƟon 7031 (b) [may] be reduced by oī sets for materials and service provided or by claims for indemnity and contribu-

"The ...court conduded that the contractor was not qualiļ ed to be licensed because it did not have a qualiļ ed responsible managing ok cer ..."

CONTRACTOR LICENSURE REQUIREMENTS, CONT'D

Θon?" The Court concluded that it may not, and that under the express terms of the statute, "unlicensed contractors are required to return all compensaΘon received without reducΘons or oī sets for the value of the materials or serviced provided."

The requirement of SecΘon 7031 that a license be maintained "at all Θmes" conveys the California Legislature's obvious intent to impose a sΘī all-or-nothing penalty for unlicensed work by specifying that a contractor is barred from all recovery for such an "act or contract" if unlicensed at any Θme while performing it. This all-or-nothing philosophy demonstrates that contractors with lapses in licensure may not recover even parΘal compensaΘon by segmenΘng the licensed and unlicensed porΘons of their performance.

Licensure Issues Arising From Unlicensed Subcontractors

Contractors and subcontractors must be extremely careful about their licensure status. California Labor Code § 2750.5 creates a presumpΘon that a worker (such as a subcontractor) performing work for which a license is required is an employee and not an independent contractor. "Any unlicensed subcontractor is the employee of the general contractor; consequently, as a maΣer of law, the employee of an unlicensed subcontractor is the employee of the principal contractor." Neighbours v. Buzz Oates Enterprises (1990) 217 Cal.App.3d 325, 330; See also Sanders ConstrucΘon Co. Inc. v. Cerda (2009) 175 Cal.App.4th 430 (general contractor is liable for unpaid wages, worker's compensaΘon insurance, withholding taxes, and other liabiliΘes arising from retaining an unlicensed subcontractor).

Contractors retaining unlicensed subcontractors must have worker's compensaΘon insurance covering individuals deemed employees of the contractor as a maΣer of law. If not, the contractor will not saΘsfy all licensure requirements, will not saΘsfy the "at all Θmes" language explained above, and may be required to disgorge all payments made on the project. Moreover, a contractor cannot recover on a mechanic's lien for money voluntarily advanced to an unlicensed subcontractor. Holm v. Bramwell (1937) 20 Cal.App.2d 332. Holm and its reasoning was discussed at length in MW Erectors, Inc. v. Niederhauser Ornamental and Metal Works Co. Inc. (2005) 36 Cal.4th 412. There, the California Supreme Court reasoned that "Holm held that because a subcontractor was unlicensed..the subcontract was illegal, void, and unenforceable; hence, the general contractor could not recover, under a mechanic's lien, compensaΘon aΣributable to the subcontractor's work. Signiļ cant in Holm's reasoning was the wording of the predecessor statute to secΘon 7031, as then in eī ect."

This reasoning raises two quesΘons answered perhaps by common sense but not by law: (1) may a contractor recover on a breach of contract theory from an owner fees incurred for work performed by an unlicensed subcontractor, and (2) does the law leave open the possibility that a licensed contractor could hire all unlicensed subcontractors, collect money from the owner for the unlicensed work, and then seek reimbursement from the unlicensed subcontractors per secΘon 7031?

As to the ļ rst quesΘon, a contractor cannot recover on a mechanic's lien from an owner for work performed by an unlicensed subcontractor, but there is no clear law on whether a licensed contractor may pursue the funds on a breach of contract acΘon. The logical extension of the cases discussed above would appear to be that a contractor cannot recover on either a mechanic's lien or a breach of contract theory.

On the second quesΘon, a loophole does appear to exist in the law allowing a licensed contractor to hire unlicensed subcontractors, collect funds from the owners for work performed by the unlicensed subcontractors, and then sue the same subcontractors under secΘon 7031. Hiring unlicensed subcontractors violates Business and Professions Code § 7018, but a violaΘon does not implicate any potenΘal disgorgement of funds from the unlicensed contractor. An owner may never know about the licensure of the subcontractor and it is conceivable a contractor, under the law as currently wriΣen, could proceed with this approach unΘl a complaint were raised with the state licensing board. This raises an interesΘng potenΘal loophole in the law and illustrates the need for increased cauΘon from an owner in ensuring that all contractors and subcontractors are licensed.

PROFESSIONAL LIABILITY DEFENSE QUARTERLY
is published by:
Professional Liability Defense FederaΘon
1350 AT&T Tower
901 MarqueΣe Avenue South
Minneapolis, MN 55402
(612) 481-4169

"Contractors and subcontractors must be extremely careful about their licensure status."

Glen R. Olson is a partner of Long & Levit LLP, in San Francisco, specializing in professional liability and insurance coverage liΘgaΘon. He defends lawyers, real estate agents, insurance agents and brokers and escrow agents. Glen may be reached at golson@longlevit.com.

Ari Baruth pracΘces with Long & Levit, LLP in San Francisco. He represents architects, design professionals, owners and other professionals in the construcΘon industry in design and constructed related maΣers. Ari may be reached at abaruth@longlevit.com.

ELDER ABUSE AVOIDANCE: COUNSELING PROFESSIONALS, BY: JEFF C. HSU, ESQ. AND ANGELA S. RHO, ESQ.

According to the U.S. Census Bureau, as of July 1, 2015, 47.8 million people in the United States are age 65 and older, accounting for 14.9 percent of the total population. The senior population grew 1.6 million from 2014, and is steadily growing. U.S. Bureau of the Census. Older Americans Month: May 2017 (CB17-FF.08). Washington: Government Printing Office, 2017. (Profile America Facts for Features). (CB17-FF.08). As of November 2016, U.S. seniors numbered approximately 50 million, and the projected population of seniors in 2060 is 98.2 million; nearly one in four U.S. residents will be in this age group, and of this number, 19.7 million will be age 85 or older. Id.

With such a dramatic spike in the senior population, both the government and private sector face a challenging landscape. Not only will government programs and resources be taxed and overstrained, but those in the private sector also face real challenges in working with/representing senior citizens. All 50 states and the District of Columbia have laws designed to protect older adults. www.justice.gov/elderjustice/prosecutors/statutes. These laws vary considerably. They started out to protect seniors who are neglected or exploited by caregivers, however, many states have enlarged the definition of elder abuse to include "financial elder abuse." This is generally when someone takes advantage of an older person's vulnerability or dependent condition to deprive them of their assets. In some states, elder abuse laws apply to people 60 years or older; in others, it's 65 or older. Both criminal and civil penalties can apply to all forms of elder abuse.

California has arguably the most far-reaching elder abuse laws of any state. In California, financial elder abuse laws apply to anyone 65 or older regardless of whether they have any diminished physical or mental capacity. Financial elder abuse is defined as: when any person or entity "takes, secrets, appropriates, obtains or retains real or personal property of an elder for a wrongful use or with intent to defraud." It also includes "assisting" in the taking of any property of someone 65 or older. The definition of "wrongful use" is: if the person "knew or should have known that this conduct is likely to be harmful to the elder." Cal. Welfare & Institutions Code §15610.30

This language is so broad that it may apply to virtually every business transaction with someone who is 65 years or older. For example, leading up to and during the recent hurricanes which have ravaged parts of Texas and Florida, there have been numerous reports of price gouging, including reports of up to $99 for a case of water, hotels that are tripling or quadrupling their prices and fuel going for $4 to $10. If someone unwittingly sold a bottle of water to an elder for fifty cents more than its fair market value and the elder can prove you knowingly sold the water for that price, you may have just engaged in financial elder abuse. Situational price gouging, deliberate or inadvertent, may be limited to times of natural disaster, however broad financial elder abuse laws like those in Texas or California apply to nearly every financial transaction and may turn an otherwise innocuous sale into a nightmare. One such precautionary tale is that of Glenn Neasham, an insurance broker in California who was arrested and charged with felony theft from an elder in December 2010, facing up to four years in prison.[2] He was ultimately convicted for selling an indexed annuity to an elderly client with Alzheimer's-like dementia. In the process, he lost his license, annuity business, and his house. After years of battling in court, Mr. Neasham's conviction was overturned on October 8, 2013 by the Court of Appeals, yet he continues to struggle putting his life and career back together.[3]

Mr. Neasham's ordeal began in February 2008, when met with Fran Schuber, an 83-year old client referred to him by her friend, an existing client. They discussed how Ms. Schuber could earn a better return on her money than she was currently earning from bank certificates of deposit. After discussing options, Mr. Neasham sold Ms. Schuber an indexed annuity for $175,000. This caused Ms. Schuber's bank manager to express concern that Ms. Schuber was being unduly influenced by her friend. Mr. Neasham had similar misgivings, but after further investigation, determined that his concerns were unfounded. Unfortunately, it later became apparent that Ms. Schuber had Alzheimer's-like dementia at the time of the transaction. According to Mr. Neasham and his assistants, although they did not notice any signs of impairment from Ms. Schuber, her friend had done most of the talking during the sale. [4]

The bank manager reported her concern to the California Department of Insurance, causing the district attorney to investigate. Mr. Neasham was subsequently arrested for: (1) selling a complex and inappropriate product to an elderly woman who lacked the mental capacity to assess the recommendation to buy the indexed annuity; and (2) that "the terms and conditions of the annuity contract were not in her best financial interest." Worse, he was reported to be an "unscrupulous agent" who preyed on seniors.[5]

Mr. Neasham maintained that he did nothing wrong by selling the annuity. Namely, that Ms. Schuber showed no signs of the Alzheimer's-like dementia she

> "[M]any states have enlarged the definition of elder abuse to include 'financial elder abuse.'"

ELDER ABUSE AVOIDANCE, CONT'D

had been diagnosed with, that she appeared to comprehend the annuity, that the annuity appreciated in value by the time of the trial, and that it was legal to sell such annuities to people under the age of 85. He was nonetheless convicted of a felony count of theft and sentenced to prison. Immediately after the verdict was returned, a juror stated that two jurors voted to convict to "send a message" to caution insurance agents from selling products to the elderly.[6]

Since the reversal of Mr. Neasham's conviction, the California Supreme Court declined the request to review the decision. Moreover, a recently discovered video of Ms. Schuber from 2008 shows her speaking lucidly of the annuity she purchased. Yet Mr. Neasham's reputation and business are still harmed despite reissuance of a license to sell insurance again.[7]

While this ordeal played out in the criminal courts, the potential liability had it involved a civil lawsuit could have been equally daunting. In any action for financial elder abuse, in addition to any actual economic damages, the elder is entitled to attorneys' fees if he/she prevails. California Welfare & Institutions Code § 15657.5. Further, if the plaintiff can show "by clear and convincing evidence" that the defendant was guilty of "recklessness, oppression, fraud or malice," the plaintiff can also recover punitive damages. Id. Even if the action is frivolous or the elder does not prevail, they are not required to pay the other side's attorney's fees.[8] This motivates lawyers to file lawsuits with the fee provision driving the litigation.

So What Can You Do?

First of all, continue to do business with seniors. Do not refuse to do business with older people out of fear it may be easy for them to sue you. Not only is this illegal, but as explained above, senior citizens are a tremendous market for legitimate and fair business.

Second, take the time to know your clients. Before recommending the purchase of a product or service, obtain a full picture of the client's individual needs. Evaluate the client's income and expenses including liquidity and net worth. Understand the client's goals, including when the client may need to access funds in the future. Make sure that your product or service is suitable for the senior's needs at the time of the transaction. To gauge suitability, consider whether or not your product/service confers a benefit to the client. If you are recommending the replacement of an existing policy, provider or product, transactions involving a replacement should not be made unless it is in your client's best interest. That is, the replacement must be appropriate to your client's needs and must provide them with a benefit that is not otherwise available in their existing product. Also consider whether or not the client is in a financial position to allow the recommended product/service to function as desired, in order for the client to access the full benefit.

Third, provide your client with copies of all sales material used or discussed. All clients, but in particular, senior clients, require a full explanation of their options to make informed decisions. Encourage your client to carefully read all documents and disclosures for the product/service you are recommending. Discuss this information in detail and respond to any questions to ensure that your client understands. Frequently ask questions and pay close attention to older clients to make sure they understand the product or service you are presenting. Space out the time between when a product/service is presented and when the client is asked to commit or purchase the product or service. Encourage your client to use the time to engage family members who may be impacted by this transaction. In some cases, it may be appropriate to suggest your client discuss the proposed transaction with a tax advisor or independent legal professional.

Fourth, consent, decision-making capacity, and undue influence are critical issues in many elder abuse cases. When these issues are raised, other forms of evidence besides the alleged victim's testimony may be necessary to analyze the elder's state of mind and to defend against such claims. While it may seem extreme, consider video-taping or recording transactions where decisions are made or documents are signed to evidence the elder's understanding and consent. Modern technology gives us the ability to document or record communications with ease. However, the use of recording devices has serious implications on people's right and expectation of privacy. Many states, including Califor-

> "This motivates lawyers to file lawsuits with the fee provision driving the litigation ...."

Jeff C. Hsu is with Murphy Pearson Bradley & Feeney in its Los Angeles, California office. Jeff's defense practice includes professional liability, construction defect and design cases. He may be reached at jhsu@mpbf.com.

Angela S. Rho is with Murphy Pearson Bradley & Feeney in its Los Angeles, California office. She defends employers against claims of wrongful termination, retaliation, discrimination, harassment and other claims. She may be reached at arho@mpbf.com.

Google

Analytics
PLDF Website Data
October 2017

Sessions: 949, Users: 736, Page Views: 3,032, Visit Duration (mins:secs): 2:27, Pages/Visit: 3.19, New Visits: 66%

Have you uploaded your bio data and photo yet?

nia, have strict laws regarding the recording of conversaeons. See California Penal Code § 632. Therefore, before you start recording, be mindful of the laws of your respeceve state regulaeng recording of communicaeons.

Lastly, to protect yourself from any poteneal legal aceon, obtain errors and omissions insurance coverage. When purchasing coverage, pay close aΣeneon to the limits and exclusions. Read and fully understand the rules of your coverage, especially regarding the eemely noeicaeon of a poteneal claim. Failure to follow the guidelines in your coverage may result in a loss of coverage for a claim.

Endnotes

1.hΣps://www.cnbc.com/2017/08/28/price-gouging-during-hurricane-harvey-up-to-99-for-a-case-of-water-texas-ag-says.html.

2. Leslie Scism, Annuity Case Chills Insurance Agents, The Wall Street Journal, March 18, 2012, available at hΣps://www.wsj.com/areicles/SB10001424052702303863404577288480158320286.

3. Sanders Wommack, Found Innocent AÕer Being Sentenced to Jail for Alleged Bilking of An Old Lady, Glenn Neasham Struggles to Rebuild His Career, March 20, 2015, available at hΣps://riabiz.com/a/2015/3/20/found-innocent-aÕer-being-sentenced-to-jail-for-alleged-bilking-of-an-old-lady-glenn-neasham-struggles-to-rebuild-his-career.

4. Id.; Steve Morelli, Court Upholds Reversal of Neasham TheÕ ConviceOn, Insurancenewsnet.com, January 15, 2014, available at hΣps://insurancenewsnet.com/innareicle/Court-Upholds-Reversal-Of-Neasham-TheÕ-ConviceOn-a-446461#.WbcGObKGOos.

5. Id.

6. Sanders Wommack, footnote 3, supra.

7. Id.; Steve Morelli, footnote 4, supra.

8. Bates v. Presbyterian Intercommunity Hospital, 204 Cal. App. 4th 210, 216 (2012).

LAW FIRM CYBERSECURITY: LIABILITY AND ETHICAL CONSIDERATIONS, BY: BARRY R. TEMKIN, ESQ.

Cybersecurity events, including hacking, are on the rise at law ¡rms. A major professional liability insurer eseimates that as many as 80% of the largest law ¡rms in the U.S. have experienced data breaches recently. Nor is external hacking the only threat faced by law ¡rms. Some data breaches may be aΣributable to employee negligence, such as a law ¡rm employee leaving a laptop, cell phone or other electronic device in a taxi, car trunk, coï ee shop or other public place. Moreover, informaeon stored in the cloud, or transmiΣed via unsecured servers may be vulnerable to unauthorized intrusions.

As explained below, recent law ¡rm data breaches have included the outside hacking by Chinese naeonals into the computers of the mergers & acquisieons groups at two major law ¡rms, resuleng in signi¡cant insider trading and an enforcement case by the U.S. Securiees & Exchange Commission against the overseas naeonals (but not the law ¡rms). In addieon, former clients of a Chicago law ¡rm have ¡led a federal class aceon against the law ¡rm alleging that they were injured because of the ¡rm's failure to maintain data security.

These alarming developments have been accompanied by an increase in government scrueny of regulated industries and the lawyers who serve them. In addieon, the organized bar has issued recent ethics opinions which may presage a trend toward enhanced vigilance by lawyers on encrypeon and other cybersecurity requirements. This areicle will analyze recent developments in lawyer cybersecurity and explain the nascent but growing trend toward stepped-up scrueny of law ¡rm data proteceon, including by state ethics regulators and the organized bar.

Recent Law Firm Data Breaches

The year 2016 abounded with news of law ¡rm data breaches, none of it happy. The data breach of Panamanian law ¡rm Mossack Fonseca made interneonal headlines, embarrassing the ¡rm's roster of an¡uent and polieically powerful clients. See American Lawyer, April 4, 2016, "Panama Papers Put Spotlight on Law Firm Data Security." This infamous data breach shined an unwelcome spotlight on the Mossack Fonseca ¡rm and its interneonal clients, whom the Panamanian lawyers had apparently helped set up oï -shore eneeies to evade their respeceve countries' income taxes on eye-popping wealth.

In March 2016, the Wall Street Journal reported that two major U.S. law ¡rms had been hacked by outsiders running an insider trading scheme seeking to bene¡t from non-public con¡deneal informaeon about poteneal mergers and acquisieons by the ¡rms' clients. Wall Street Journal, March 29, 2016, Bloomberg BNA, March 30, 2016. The ¡rms were ideneied as Cravath, Swaine & Moore and Weil, Gotshal & Manges. On December 27, 2016, the U.S. Securiees & Exchange Commission announced an enforcement aceon in U.S. District Court against three Chinese naeonals charged with insider trading based on hacked non-public informaeon stolen from two New York based law ¡rms. U.S. Securiees & Exchange Commission, Lieigaeon Release 22711/ December 27, 2016, U.S. Securiees & Exchange Commission v. Hong. According to the SEC complaint, the Chinese hackers targeted the mergers and acquisieons departments of the ¡rms, where they installed malware on the ¡rm's networks, compromised accounts that enabled access to all

> "These alarming developments have been accompanied by an increase in government scruEny of regulated industries and [their] lawyers ..."

LAW FIRM CYBERSECURITY, CONT'D

email accounts at the ļrm and accessed dozens of gigabytes of emails from remote internet locaϴons. Armed with the data, the Chinese naϴonals went on a trading frenzy in the stocks of the M&A targets, reaping proļts in excess of $1 million, then moving the markets by trading in up to 25% of all trades.

And as if 2016 didn't contain enough bad news for lawyers, on April 15, 2016, a former client of Chicago law ļrm Johnson & Bell ļled a federal class acϴon alleging that the ļrm engaged in malpracϴce by its failure to maintain adequate standards of cybersecurity. See Al Faikali, Data Security Law Journal, "Law Firm Data Security: The First Class Acϴon," December 12, 2016. The class acϴon alleges malpracϴce in that the ļrm, which portrays itself as an expert in advising clients about cybersecurity, was itself negligent in protecϴng its own clients' data security, by its failure to encrypt an online aΣorney ϴme tracking system and the use of a virtual private network known as VPN. See Andrew Strickler, "Law Firm Hacking to Breed New Kind of Malpracϴce Suit," Insurance Law 360, December 12, 2016. According to the complaint, "Johnson & Bell has injured its clients by charging and collecϴng market-rate aΣorney's fees without providing industry standard protecϴon for client conļdenϴality." Id.

Aside from the fact that this is apparently the ļrst client class acϴon against a law ļrm alleging cyber-insecurity, the Johnson & Bell suit is noteworthy in that the law ļrm was not hacked and there were no actual known data breaches. Rather, the purported class representaϴves alleged that they were damaged by the risk that their conļdenϴal informaϴon might be compromised at some point in the future. AÕer denial of the law ļrm's moϴon to dismiss, the court directed the parϴes to parϴcipate in arbitraϴon, thereby reducing the likelihood that there will be addiϴonal reports on the case in the short term.

New Cybersecurity Regulaϴons

As will be explained in the following two secϴons of this arϴcle, primary regulators, parϴcularly in health care, insurance and ļnancial services, have begun to regulate companies in these industries to require speciļc cybersecurity protecϴons. These industry regulaϴons will indirectly, and in some instances, directly, aī ect lawyers as service providers to companies in regulated industries. In addiϴon, law ļrms themselves are directly subject to regulaϴon by courts and the organized bar, which have begun to impose ethical requirements on lawyers to adhere to standards of cybersecurity in order to maintain client conļdenϴality. As will be seen, the trend is growing toward enhanced scruϴny of lawyers' cybersecurity measures.

According to ļnancial services aΣorneys Jeī Kern and Christopher Bosch, ļnancial ļrms have been obligated to implement cybersecurity measures since enactment of the Gramm-Leach-Bliley Act of 1999. See Jeī Kern & Christopher Bosch, "New York State Department of Financial Services Cybersecurity Regulaϴon Poised to Reshape Exisϴng Regulatory Landscape," Sheppard Mullin Government Contracts and Invesϴgaϴons Blog, January 31, 2017. Kern and Bosch write that the Gramm-Leach-Bliley safeguards rule "sets forth high-level cybersecurity direcϴves, but mainly delegates rule-making authority to various government regulators to promulgate informaϴon security rules applicable to enϴϴes under their respecϴve jurisdicϴons." Kern & Bosch, supra. In the ļnancial services sector, informaϴon security regulaϴons are promulgated by the Ok ce of the Comptroller of the Currency, the Federal Reserve System, the Federal Deposit Insurance Corporaϴon, and other agencies. Federally-regulated broker-dealers, investment companies and registered investment advisors must comply with SEC Regulaϴon S-P, which requires regulated enϴϴes to "adopt policies and procedures that address administraϴve, technical and physical safeguards for the protecϴon of customer records and informaϴon." SEC Regulaϴon S-P, Privacy of Consumer Financial Informaϴon, 17 CFR §238.40. In addiϴon, the Naϴonal Insϴtute of Standards and Technology has issued a non-binding Framework for Improving Criϴcal Infrastructure Cybersecurity, a voluntary risk-based cybersecurity framework.[2]

Nor have state regulators been idle. MassachuseΣs enacted a pioneering data protecϴon law in 2010 known as "Standards for the Protecϴon of Personal Informaϴon of Residents of the Commonwealth," which requires companies doing business in MassachuseΣs to encrypt personal data and to retain digital and physical records and implement network security controls, such as ļrewalls, to protect consumer informaϴon. See 201 CMR 17.00, Standards for Protecϴon of Personal Informaϴon of Residents of the Commonwealth.

The MassachuseΣs regulaϴons established minimum standards for safeguarding of personal informaϴon in order to ensure the conļdenϴality of customer informaϴon and protect against threats or hazards to such informaϴon. 201 CMR 17.01, www.mass.gov/ocabr/docs/idtheÕ/201cmr1700.

The MassachuseΣs standards are unique in that they reach across all industries and are not restricted to a single industry. Rather the MassachuseΣs law broadly applies to: "Every person that owns or licenses personal informaϴon about a resident of the Commonwealth," and requires such persons to develop "a comprehensive informaϴon security program that it is wriΣen in one or more readily accessible parts," and contains safeguards to protect and encrypt conļdenϴal consumer informaϴon. Id. at 17.03, Duty to Protect and Standards for Protecϴng Personal Informaϴon. The MassachuseΣs law requires secure user authenϴcaϴon protocols, control of data security passwords, restricted access to acϴve users, unique and complex passwords and encrypϴon of all transmiΣed records and ļles.

> "[V]endors who do business with regulated ļnancial service companies will soon be expected to comply with cybersecurity standards …."

LAW FIRM CYBERSECURITY, CONT'D

New York Governor Andrew Cuomo, in December 2016, announced the promulgaϴon of cybersecurity regulaϴons by the New York Department of Financial Services, eī ecϴve March 1, 2017. The new DFS rules apply to all enϴϴes under its jurisdicϴon, including insurance companies, insurance agents, banks, charitable foundaϴons, holding companies and premium ļnance agencies. The New York DFS regulaϴons require encrypϴon of all non-public informaϴon held or transmiΣed by the covered enϴty, and require each regulated company to appoint a chief informaϴon security oĸ cer ("CISO"), who must report directly to the board of directors and issue an annual report, setţ ng forth an assessment of the company's cybersecurity compliance and any idenϴļ able risks for potenϴal breaches. New York 23 NYCRR §501 et. seq.; see also Barry R. Temkin, "New Cybersecurity RegulaϴonΣ: Impact on RepresenϴΣng Financial InsϴtuϴonΣ," New York Law Journal, December 15, 2016.

Of parϴcular interest to law ļrms who represent ļnancial insϴtuϴons is §500.11 of the new DFS regulaϴons, which requires each covered enϴty to "implement wriΣen policies and procedures designed to ensure the security of informaϴon systems and nonpublic informaϴon that are accessible to, or held by third-parϴes doing business with the covered enϴty." 23 NYCRR §500.11. Thus, covered enϴϴes, including insurance companies, who provide access to personal idenϴfying informaϴon to third-party vendors must cerϴfy not only that their own informaϴon systems are adequate, but that the informaϴon security systems of vendors with whom they do business are also secure and protected. In other words, vendors who do business with regulated ļnancial service companies will soon be expected to comply with the cybersecurity standards of their represented clients. Nor does the New York DFS rule appear to be an isolated outlier. To the contrary, the organized bar is already advising lawyers to exercise care and scruϴny in proteceϴng client's conļ denϴal data.

Regulatory Enforcement

ParϴcularΣ in the ļnancial services industry, regulators have been stepping up their enforcement of cybersecurity breaches, oĈen with signiļ cant ļnes and penalϴes. For example, the SEC, in 2016, announced a seΣlement with Morgan Stanley Smith Barney in a case in which over 700,000 customer accounts containing personal idenϴfying informaϴon (PII), such as social security numbers and dates of birth, were accessed by a single ļnancial advisor, who decided that it would be a good idea to store these data on his own personal website. The ļnancial advisor sustained a data breach, compromising the conļ denϴal customer informaϴon, whereupon he was terminated by the ļrm. Although Morgan Stanley contacted the FBI within two weeks of learning of the breach, the SEC claimed that the ļrm was responsible for the breach and extracted a $1 million ļne.

In a recent ļnancial industry regulatory enforcement acϴon, registered broker dealer Sterne Agee agreed to pay a ļne of $225,000 for its failure to encrypt conļ denϴal data on a laptop that was leĈ in a restaurant, thereby exposing the personal idenϴfying informaϴon of 350,000 customers. This conduct was found by FINRA to violate regulaϴon SP and FINRA Rules 3010 and 2010. Thus, there has been a deļ nite upϴck in regulatory enforcement of data breaches.

The Organized Bar and Cybersecurity

Law ļrms' clients are not the only enϴϴes subject to regulatory scruϴny of their cybersecurity measures. The organized bar is now starϴng to look carefully at lawyers' ethical and professional liability responsibiliϴes to ensure the security of client data. Moreover, some jurisdicϴons, notably Florida, are imposing mandatory conϴnuing legal educaϴon requirements for lawyers to learn technology. Lawyers' duϴes of competence and conļ dence are embodied in ABA Model Rules 1.1 and 1.6. ABA Model Rule 1.1 provides that: "A lawyer shall provide competent representaϴon to a client." ABA Model Rule 1.1, Competence.

> "A lawyer's duty of technological competence may include having the requisite … knowledge to reduce the risk of disclosure of client informaϴon …."

New York's counterpart is similar, and further provides, in a comment, that: "To maintain the requisite knowledge and skill, a lawyer should..keep abreast of the beneļ ts and risks associated with technology the lawyer uses to provide services to clients or to store or transmit conļ denϴal informaϴon." New York RPC 1.1, comment [8]. A lawyer's ethical duty of conļ denϴality is imposed by ABA Model Rule 1.6 which provides broadly that: "A lawyer shall not reveal informaϴon relaϴng to the representaϴon of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representaϴon or the disclosure is permiΣed by paragraph (b)." ABA Model Rule 1.6(a). The New York Rules of Professional Conduct further require lawyers to "make reasonable eī orts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, informaϴon relaϴng to the representaϴon of a client." NYRPC 1.0. (c); at ABA Model Rule 1.6 (c).

California's Standing CommiΣee on Professional Responsibility and Conduct issued an ethics opinion in 2015 concluding that an aΣorney lacking required e-discovery competence to handle a complex liϴgaϴon must either acquire the requisite skill or associate with technical consultants or competent counsel to bring her up to speed on technology. California Standing CommiΣee on Professional Responsibility and Conduct Formal Opinion 2015-193. Eī ecϴve January 1, 2017, Florida has mandated conϴnuing legal educaϴon on maintaining technological competence, including use of encrypϴon and other technology to preserve client conļ denϴal data. See FL Rule 6-10.3(b), hΣps://

LAW FIRM CYBERSECURITY, CONT'D

Ňbridabar.org (requiring CLE in "approved technology programs").

In March 2017, the New York County Lawyers Associaeon issued its opinion on lawyers' ethical duty to ensure technological competence. See NYCLA Ethics Opinion 749, March 2017, www.nycla.org/NYCLA/Lawyersethicsopinions. According to NYCLA ethics opinion 749, lawyers are required by the Rules of Professional Conduct to keep up with technological developments, "cannot knowingly reveal client conĮdeneal informaeon, and must exercise reasonable care to ensure that the lawyers, employees, associates and others whose services are uelized by the lawyer not disclose or use client conĮdeneal informaeon." Id. at p. 4. SigniĮcantly, the NYCLA ethics opinion recognizes a duty on the part of lawyers to prevent data breaches:

> The risks associated with transmission of client conĮdeneal informaeon electronically include disclosure through hacking or technological inadvertence. A lawyer's duty of technological competence may include having the requisite technological knowledge to reduce the risk of disclosure of client informaeon through hacking or errors in technology where the pracece requires the use of technology to competently represent the client.

NYCLA Ethics Opinion at 4, www.nycla.org/ethics. Thus, the NYCLA ethics opinion suggests that lawyers have more at stake than poteneal loss of business, embarrassment or professional liability when it comes to maintaining the conĮdeneality of client conĮdeneal informaeon. While this is just a recent development, and there have been no known prosecueons of lawyers or law Įrms, lawyers should be mindful of their ethical obligaeons to maintain client conĮdeneal data, whether in the cloud, in an email or in a portable device.

On May 22, 2017, the ABA Standing CommiΣee on Ethics and Professional Responsibility issued Formal Opinion 477R, which addressed the ethics of "Securing Communicaeon of Protected Client Informaeon." In its opinion, the ABA eschewed bright line rules, adopeng instead "a fact-speciĮc approach to business security obligaeons that requires a "process to assess risks, ideneefy and implement appropriate security measures responsive to those risks, verify that they are eī ecevely implemented, and ensure that they are coneenually updated in response to new developments." ABA Standing CommiΣee on Ethics and Professional Responsibility, Formal Opinion 477R, May 22, 2017, at 4 (quoeng from ABA Cybersecurity Handbook).

The ABA opined that the decision whether to use encrypted e-mail is fact-speciĮc, and that "lawyers must, on a case-by-case basis, constantly analyze how they communicate electronically about client maΣers," based upon a number of enumerated factors, including the sensieivity of the electronically-communicated informaeon, the risk of cyber-intrusion and the needs of the client. Id at 7-8. In addieon, the ABA advised lawyers to understand clients' needs for cyber-security, to vet outside vendors and conspicuously to label e-mail communicaeons as privileged and conĮdeneal.

Conclusion

As we have seen, law Įrm data breaches are on the rise, running the gamut from an unencrypted cell phone or laptop leŌ in a taxi or restaurant, up to organized hacking by insider trading rings trading in clients' stocks. In 2016, we saw the public disseminaeon of conĮdeneal law Įrm data used to humiliate lawyers and their clients, the Įrst client class aceon against a law Įrm alleging malpracece for inadequate data security, and the Įrst Securiees & Exchange Commission enforcement aceon against overseas naeonals for hacking into and trading on conĮdeneal data pilfered from law Įrm computers.

The year 2017 has brought us a comprehensive new regulaeon from the New York Department of Financial Services which appears to be a harbinger of things to come, as well as new ethics opinions from the organized bar suggeseng that lawyers now have an ethical duty to maintain technical competence in order to maintain the security of client conĮdeneal informaeon. These developments are forcing law Įrms to be cognizant of the very real and signiĮcant risks they face in the 21st century, and to acquire the technology suĸcient to keep abreast with their clients' cybersecurity needs.

Endnotes

1. CNA Professional Counsel, Safe and Security: "Cybersecurity Pracece-es for Law Firms," hΣp://www.CNA.com/web/wcm/connect/61
2. hΣps://www.nist.gov/sites/default/Įles/documents/cyberframework/cybersecurity-framework-021214.pdf

Barry R. Temkin is a partner at Mound CoΣon Wollan & Greengrass LLP, and a Member of the N.Y. County Lawyers Associaeons CommiΣee on Professional Ethics. The views expressed are those of the author alone. He may be reached at btemkin@moundcoΣon.com.

LETTER FROM THE PRESIDENT, CONT'D

this eī ort. If you would like to join the YPC, or Įnd out more about it, please e-mail Chris Jensen so that she can connect you with the group. We also have open leadership posieons available on our D&O/Investment Professionals Liability CommiΣee. If you or one of your colleagues represents directors, oĸ cers, or investment professionals, this is a great opportunity to promote your experese.

FIELD TRIP FUN!

Board Members

PLDF Fans

We hope you enjoy this issue of the PLDF Quarterly. The next issue of the Quarterly will be published in February and the deadline for areicles is February 1, 2018. Please consider wrieng an areicle, or co-authoring an areicle with one of your younger colleagues. We welcome areicles on developments in the law that are of interest to the professional liability bar, as well as areicles about trial eips and taceics.

Finally, if you are looking to refer a case to a lawyer in another jurisdiceon, or to assign a professional liability claim to a defense aΣorney, please THINK PLDF! The website has a "member search" feature that will enable you to Įnd a defense aΣorney in a pareicular state or city. The ability to help your client, or your insured, to Įnd capable defense counsel is one of the key beneĮts of a PLDF membership.

Wishing each of you a happy Thanksgiving, Erin Higgins