AHERN INSURANCE BROKERAGE

AHERN Update

As provided by Hinshaw & Culbertson, LLP— leaders in risk management.

AXA XL is the #1 global commercial property & casualty insurer, with gross written premium of $19 Billion in 2018. AXA XL's core operating insurance and reinsurance companies have one or more of the following financial strength ratings: A.M. Best A+, S&P AA-.

SAN DIEGO COUNTY BAR ASSOCIATION

AHERN Insurance Brokerage, San Diego County Bar Association's Premier Member Benefit Provider since 2004, is pleased to offer SDCBA members an exclusive Professional Liability Program with AXA XL. **SDCBA members can save up to 20%.**

Call (800) 282-9786 to speak with an AHERN Professional or visit us online at aherninsurance.com/associations/sdcba.

Video Conferencing Risk Management Considerations

The Covid-19 pandemic has altered how we interact with our clients, third parties and each other. It has required the legal profession to begin working from home virtually overnight. Naturally, this has led to a search for effective video conferencing technology that will allow lawyers to remotely hold meetings and conduct depositions. As with any technology, the use of video conferencing technology has its risks, especially for lawyers who have never used it before. Our duty of competence, however, requires that we be aware of both the risks and the benefits of this technology, and to implement reasonable measures to mitigate those risks.

Understand the Privacy and Security Risks

- **Review Policies.** Before using any free or licensed version of any video conferencing technology, consider reviewing its terms of service and its privacy policy. It's helpful to know what information the app collects about you and any attendee to your conference.

- **Understand and Utilize Settings.** Review the available settings and apply them in a way that will maximize the privacy and security of your conferences. Some settings should be a "no brainer." Why in the world would anyone want to log into a video conference using Facebook or Google? Others will be more nuanced and if you are unsure, ask for assistance from an IT professional. Recent news reports indicate an alarming trend of what's been called "Zoom Bombing," where uninvited individuals are able to gain access to video conference meetings. This risk can be mitigated by the user's choice of settings. For instance, only the conference host should be able to share access to the screen. A meeting can be set up so that participants remain in a waiting room and cannot join the conference until authorized by the host. The use of passwords and meeting IDs when available can further enhance the security of a video conference. Depending on the video conference technology, there may be other settings that can be applied such as locking the meeting once all invited participants have joined so others cannot drop without an invitation, blocking the ability to engage in file sharing and private chat, kicking out disruptive users, and stopping troublemakers from coming back.

San Diego Corporate Office
9655 Granite Ridge Drive, Suite 500
San Diego, CA 92123

Toll Free | 800.282.9786
Telephone | 858.571.9030
Fax | 858.571.9010

AHERNINSURANCE.COM

CA LIC 0K07568 | AZ LIC 1800012964

- **Encryption.** Inquire whether the technology offers end to end encryption.

- **Understand Storage Risks.** Consider the security risks relating to storage. For instance, if recording a video conference would result in storing your discussions or any information shared during the conference in the Cloud, ask yourself would you or your attendees want that information stored there? Do you want any of your privileged discussions with a client stored in the cloud? Are you jeopardizing attorney-client privilege by doing so? Do any of your clients' security standards or guidelines prohibit the storage of their information on a third party's servers? If any of the information discussed during a conference is "highly sensitive" in nature, check the ethics opinions in your state on the use of the Cloud. Have you evaluated the security of any Cloud storage options? Have you considered whether state law where you and any attendees are located permits recording or requires the consent of any or all participants? If any of these questions lead you to "No", then disable to recording feature and not have your conferences stored in the Cloud.

- **Check the Version and if Necessary, Update.** As with any other technology, you want to try to be using the latest version of the video conferencing you have chosen. Later versions of technology typically include patches to close vulnerabilities that existed in earlier versions. If your video conferencing technology has automatic updating available, consider using that feature. Some technology may also have on-line tutorials on how to check the version you are using and how to upgrade to the latest. If not, and if automatic updates are also unavailable, then have your IT vendor monitor the release of patches, which typically occur on the second Tuesday of the month, aptly called Patch Tuesday.

- **Duty of Competence May Require Consultation.** Finally, consider consulting with someone who has used the technology before and has a good working knowledge of its features and how to safely use it. The duty of technology competence does not require that you become an expert in the use of video conferencing technology, but you should understand the basics. Obviously, if you have an IT professional available to consult with, that may be a good place to start.

Avoid Inadvertently Creating Attorney-Client Relationships.

Providing specific advice to a specific question can be sufficient to trigger an attorney-client relationship, so please act accordingly to avoid this risk-management pothole when responding to questions during a video conference.

When holding a video conference with a potential client remember that if you receive too much information from the prospective client (typically defined as any information that could be significantly harmful to the putative client if it were ever to be used against it), even if no attorney-client relationship ensues, you and your firm could be disqualified from representing another party whose interests are adverse to the prospective client in the same or substantially related matter. This ethical rule on prospective clients requires that lawyers take reasonable measures to avoid learning more information than was reasonably necessary to determine whether to represent a prospective client. So limit the information you obtain in the initial conference to what you need to run a conflict check and to evaluate whether to accept the engagement.

Avoid Scope of Representation Creep.

Lawyers should be thoughtful when drafting engagement letters to identify the client and to carefully define the scope of the legal services to be provided in the engagement. This is to protect you and your firm against claims that you should have taken some action beyond what was called for in the engagement letter. That defense, however, could be lost by advising a client on issues beyond the scope of the services you have agreed to provide in your engagement letter. Please exercise care when answering questions on a video conference and limit your advice to the services you have agreed to provide in that engagement.

Avoid Inadvertent Waivers of Attorney-Client Privilege.

Remember that if you or your client discuss your privileged advice with third parties with whom you do not share a common interest, the privilege may have been waived. Be careful who you invite to video conferences with your client and try to remember to warn your client not to discuss your advice when third parties are on the conference.

Have a "Prover" for Certain Video Conferences.

Treat a video conference with a difficult client or third party no differently than your meetings or phone calls with the person. Remember, difficult clients can get good lawyers in trouble. Accordingly, consider having a prover present during your conference who can corroborate your advice or instructions.

Clients and third parties who fall into this category include those who: 1) come to you at the eleventh hour, 2) ask you to take ethically questionable positions, 3) appear to have engaged in financially questionable practices, 4) have unreasonable expectations about a matter or seem to be on a mission, 5) like to second guess your decisions or who have researched issues and claim to know the answers before consulting you, 6) frequently file lawsuits at the drop of a hat, 7) have fired multiple lawyers or firms in the past or have consulted with several other firms before landing on your doorstep, and 8) display erratic behavior or express conspiratorial theories.

Document Important Advice with Written or Electronic Communications.

This is risk management 101. Do not simply rely on the discussions that occur on a video conference when communicating important information to a client or third parties. Over time, even the best of memories fade. Clients or third parties may legitimately forget advice that you provided or statements that were made during a video conference. Practice defensively and follow up with an email or a written communication of any critical advice or instructions that you provide during a video conference. Consider documenting discussions you had or instructions you received from the client during a video conference (especially any directing you not take action or those with which you disagree) with a memo to the file or a letter to the client. If you advise a prospective client that you are not accepting an engagement via a video conference, handle it like you would if you communicated that message on a phone call or in-person meeting, follow it up with an "I'm not Your Lawyer" letter.

Take the Same Precautions you Would with Calls or Meetings Involving Discussions with Former Employees or Third Parties.

Your discussions may not be privileged and be aware that your comments or discussions could be disclosed to your opponent. See the point above about having a prover present. If you are invited to a Zoom conference hosted by a third party ask and confirm whether it is being recorded.

Do not Attempt to Upload Confidential Client Information or any Privileged Information via Video Conference.

You need to protect privilege and comply with any applicable outside counsel guidelines, many of which require that their information not be stored on the third party servers. Uploading information through the video conference platform potentially allows it to be stored in the Cloud in violation of those client guidelines.

Anticipate that with the growing popularity of video conference applications, such as Zoom or Google's GoToMeeting, your client may be asked in discovery if it ever participated in any video conference involving the matter, who participated in the conference and there will be attempts to subpoena any information in the video conference company's possession at some point.

Share Protected or Confidential Information with Appropriate Attendees Only Through Secure Communications.

This would include PHI (protected health information), PII (personally identifiable information), NPFI (non-public financial information) or any type of personally identifying information under the California Consumer Privacy Act or the GDPR, or any other privileged or confidential information. Do not share through the video conference application; use only secure and encrypted portals to share this type of sensitive information.

Take Care in Setting Up Video Conferences.

When you anticipate attorney-client privilege or confidential communications will occur, please indicate that in a calendar invite. Never share your share your password for accessing this technology with anyone and never share your video conference meeting ID with anyone, treat it like your password.

Be Professional and Disciplined in Your Use of Video Conferencing.

Clients will not be surprised by casual dress but please be professional. Consider where you are holding the conference in your home or apartment and how it reflects on you and your firm. Clients and third parties will be able to not only see you but what is behind you. Nothing inappropriate or offensive should be displayed. No Zombies allowed. And don't carry your computer around with you during a video conference. Don't be the next #PoorJennifer. Let's be careful out there.