Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

3 Cybersecurity Questions To Ask Before A Remote Mediation

By **F. Keith Brown and Michael Koss** (March 31, 2021, 3:45 PM EDT)

F. Keith Brown

Michael Koss

Under Rule 1.6 of the American Bar Association's Model Rules of Professional Conduct, attorneys are obliged to prevent the "unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."[1] But remote work and the pandemic have put attorneys at greater risk of exposing protected information.

Cyberattacks have amplified since before the start of the pandemic,[2] and law firms have been and will remain tantalizing targets for scammers and cybercriminals.[3] Even major law firms have fallen prey to data breaches and ransomware attacks in recent months.[4]

Simultaneously, the pandemic has normalized litigating, mediating or arbitrating disputes remotely.

Remote proceedings can be only negligibly different from in-person sessions in many cases,[5] pending a good Wi-Fi signal; however, attorneys must stay abreast of the benefits and risks associated with relevant technology[6] used to resolve disputes remotely.

Attorneys should be prepared to ask alternative dispute resolution providers a variety of questions about how remote sessions work to safeguard client information and satisfy ethical standards of the profession as they prepare to mediate or arbitrate a case remotely.

How will I access the videoconference safely?

A videoconferencing session can be accessed through a sharable link sent to the respective attendees of a remote session via email, but attorneys should not take a link sent to them at face value.

Malware, ransomware and phishing scams often ensnare users who click on links in emails masquerading as advertisements, solicitations of services[7] and videoconference invitations[8] — especially when these emails come from seemingly familiar contacts. Once latched onto a user's computer, such cyberthreats can ransom or steal confidential information and even leech onto other computer systems.[9]

When preparing for a remote session, counsel should ask their ADR provider to specify when the link will be sent, who will send it, what that sender's email is, and even what the email's subject line will be. If a new point of contact at the organization will send the link, request that the primary contact be copied on the email for easy follow-up.

Counsel should also review the beginning characters of the videoconferencing link. Links whose opening characters are https:// — with an "s" — have the cyber infrastructure in place for encrypted exchanges of information;[10] infected routers cannot change or review such information while it is being exchanged.

More importantly, counsel should scrutinize the characters in the link's domain name — the address used to locate a particular website. Are there hyphens or extra characters in the domain name, or is the domain name slightly misspelled? Once counsel receives the email and link, they can check that its contents match expectations and be confident that the email is genuine.

How are sessions regulated and safeguarded in real time?

"Zoombombing" — which involves intruders hijacking a meeting and posting disruptive content — was a pivotal part of the shift to remote work.[11] It drew national attention and compelled Zoom to require meeting passwords by default and add end-to-end encryption, which prevents the platform from viewing client information that passes through its servers during videoconferences.[12]

Most importantly, it underscored the precautions that need to be taken in order to videoconference safely.

In Zoom and similar platforms, session hosts — be they the neutral, a technical assistant or both — can moderate virtual holding rooms, close off the session, remove participants if necessary, and sort participants into virtual, private caucusing spaces for confidential deliberations.

Additionally, ADR providers can modify account settings to limit functions available to counsel, clients and other session guests, such as screen sharing and especially file sharing, which can expose unwitting participants to compromised files in extreme and rare circumstances.[13]

Counsel can contribute to virtual security by accessing the session through the most up-to-date edition of the platform, connecting to a secure, private Wi-Fi connection,[14] and running anti-virus scans prior to the session (if their device does not automatically conduct scanning).[15] Counsel should confirm that these safeguards are similarly practiced by the ADR provider and those administering the session.

How will we memorialize a settlement agreement, and how will it and other client information remain confidential?

Parties that agree to settle can memorialize the agreement in multiple ways. The neutral and counsel can cement the agreement over email or compile it into a formal, private document that can be signed electronically. Additionally, they can record a summary of the settlement agreement at the end of the videoconference, which the ADR provider can save and share with counsel as an email attachment, through cloud sharing or via an access link.

Transmitting such information over email comes with potential risks, but lawyers are generally

permitted to exchange client information over email without violating the Model Rules of Professional Conduct,[16] and are granted a "reasonable expectation of privacy"[17] in email communications, even in instances involving unencrypted email. As due diligence, though, counsel should request the use of password protections for e-signable documents or access links.

Even more so, they should also make a reasonable effort to assess the ADR provider's cybersecurity measures.

An ADR provider may retain an outside company to do a cybersecurity audit to identify if proper safeguards are in place. Similarly, law firms may retain a third-party vendor[18] to help them manage their computer network, enlist cloud-based services to store and organize matter information[19] or conduct their own cybersecurity audit. In all cases, counsel must confirm that such providers protect client information and confidentiality in accordance with the standards of the profession.

For example, the Illinois State Bar Association has developed a list of recommendations for counsel when vetting cloud-based services.[20] Those recommendations can help counsel assess the security infrastructure that an ADR provider or its third-party vendor has in place to provide safe remote dispute resolution services from start to finish. They include:

- Researching whether the ADR provider or its third-party vendors employ reasonable security precautions to protect client data;
- Investigating past breaches suffered by the ADR provider or the third-party vendor; and
- Requesting an agreement with both that they will conform to counsel's obligations to confidentiality.

Confidentiality and quality of process are crucial ethical concerns for attorneys. But these concerns are equally important for neutrals and ADR providers to address.[21] Counsel should ask a variety of questions of their ADR provider before any mediation or arbitration. By asking questions about the safety of their client's information, they will not only be serving their client well, but also become more tech-savvy practitioners in the process.

F. Keith Brown is a neutral at ADR Systems and former chief judge of the Circuit Court of Kane County in Illinois.

Michael Koss is a business development and marketing assistant at ADR Systems.

[1] Rule 1.6 - Confidentiality of Information, https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information/.

[2] Shannon Williams, Cyberattacks up 400% compared to pre-COVID-19 levels, Security Brief (Oct. 20, 2020), https://securitybrief.eu/story/cyberattacks-up-400-compared-to-pre-covid-19-levels.

[3] Ed Finkel, Cyberspace Under Siege, ABA Journal (Nov. 1 2010, 9:58 AM CDT), https://www.abajournal.com/magazine/article/cyberspace_under_siege.

[4] Xiumei Dong, Law Firms' Reported Cyberattacks Are 'Tip Of The Iceberg,' Law360 (Nov. 4, 2020, 6:25 PM EST), https://www.law360.com/articles/1326001.

[5] Michael Koss, Brigid McGrath, Remote dispute resolution is here to stay as work life changes, Chicago Daily Law Bulletin (July 30, 2020, 11:18 AM CST), https://www.chicagolawbulletin.com/mcgrath-koss-remote-adr-is-here-to-stay-20200730.

[6] Rule 1.1 Competence – Comment, ABA Model Rules of Professional Conduct, https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence/comment_on_rule_1_1/.

[7] Stephanie Francis Ward, How scams multiply during the COVID-19 crisis and why lawyers are not immune, ABA Journal (March 31, 2020, 9:30 AM CDT), https://www.abajournal.com/web/article/scams-multiply-during-covid-19-crisis-lawyers-are-not-immune.

[8] Zlati Meyer, Never click on this kind of Zoom invite. You'll thank us forever, Fast Company (Dec. 7, 2020), https://www.fastcompany.com/90582864/never-click-on-this-kind-of-zoom-invite-youll-thank-us-forever.

[9] Vincent Polley, Cybersecurity for Lawyers and Law Firms, The Judge's Journal (Nov. 1, 2014), https://www.americanbar.org/groups/judicial/publications/judges_journal/2014/fall/cybersecurity_for_lawyers_and_law_firms/.

[10] Alison Grace Johansen, What is encryption and how does it protect your data?, NortonLifeLock (July 24, 2020), https://us.norton.com/internetsecurity-privacy-what-is-encryption.html.

[11] Davey Alba, Taylor Lorenz, 'Zoombombing' Becomes Dangerous Organized Effort, The New York Times (April 7, 2020), https://www.nytimes.com/2020/04/03/technology/zoom-harassment-abuse-racism-fbi-warning.html.

[12] Joseph Marks, The Cybersecurity 202: Researchers praise Zoom's quick pledge to fix a slew of security and privacy problems, The Washington Post (April 3, 2020, 6:33 AM CDT), https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2020/04/03/the-cybersecurity-202-researchers-praise-zoom-s-quick-pledge-to-fix-a-slew-of-security-and-privacy-problems/5e860e8888e0fa101a75932b/.

[13] Will Dormann, Mindi McDowell, Brent Wrisley, Risks of File-Sharing Technology, Cybersecurity & Infrastructure Security Agency (Sept. 27, 2019), https://us-cert.cisa.gov/ncas/tips/ST05-007.

[14] Guidance for Securing Video Conferencing, Cybersecurity & Infrastructure Security Agency, https://www.cisa.gov/sites/default/files/publications/CISA_Guidance_for_Securing_Video_Conferencing_S508C.pdf.

[15] US-CERT Publications, Understanding Anti-Virus Software, Cybersecurity & Infrastructure Security Agency (Sept. 27, 2019), https://us-cert.cisa.gov/ncas/tips/ST04-005.

[16] ABA Comm. On Ethics & Prof'l Responsibility, Formal Op. 477R (2017), https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_opinion_477.authcheckdam.pdf.

[17] ABA Comm. On Ethics & Prof'l Responsibility, Formal Op. 99-413 (1999), https://www.americanbar.org/products/ecd/chapter/219976/.

[18] ISBA Advisory Opinion No. 10-01 (July 2009), https://www.isba.org/sites/default/files/ethicsopinions/10-01.pdf.

[19] ISBA Advisory Opinion No. 16-06 (Oct. 2016), https://www.isba.org/sites/default/files/ethicsopinions/16-06.pdf.

[20] Ibid.

[21] Model Standards of Conduct for Mediators, American Arbitration Association, American Bar Association, & Association for Conflict Resolution (2005), https://www.americanbar.org/content/dam/aba/administrative/dispute_resolution/dispute_resolution/model_standards_conduct_april2007.pdf#page=6.