CYBERSECURITY PROTOCOL FOR VIDEOCONFERENCE MEDIATIONS

Widely reported security concerns about popular video meeting program Zoom are summarized within the following bulletin from the Boston FBI office, released March 30,2020. This issue is of particular concern to the Florida legal community, as the Florida Court System has adopted Zoom as its preferred platform for the conduct of the Court's business, as have most of the major mediation provider firms throughout the state:

FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic

As large numbers of people turn to video-teleconferencing (VTC) platforms to stay connected in the wake of the COVID-19 crisis, reports of VTC hijacking (also called "Zoom-bombing") are emerging nationwide. The FBI has received multiple reports of conferences being disrupted by pornographic and/or hate images and threatening language….

As individuals continue the transition to online lessons and meetings, the FBI recommends exercising due diligence and caution in your cybersecurity efforts. The following steps can be taken to mitigate teleconference hijacking threats:

- Do not make meetings or classrooms public. In Zoom, there are two options to make a meeting private: require a meeting password or use the waiting room feature and control the admittance of guests.
- Do not share a link to a teleconference or classroom on an unrestricted publicly available social media post. Provide the link directly to specific people.
- Manage screensharing options.

- Ensure users are using the updated version of remote access/meeting applications.
- Lastly, ensure that your organization's telework policy or guide addresses requirements for physical and information security.

To address the security concerns as summarized above, and assure compliance with the recommended steps necessary to assure security and privacy, the mediator provider firm of Upchurch Watson White & Max, Inc. has adopted the following set of principles to govern all videoconference mediations conducted by members of the firm, regardless of the platform in use for a particular case:

UWWM MODEL CYBERSECURITY PROTOCOL

It shall be our policy to utilize the following baseline security measures in all videoconference mediations:

1. **We will only host the mediation from a private, hard-wired site, and never host using a shared or public Wi-Fi network.**
2. **Multi-factor authentication: We will use a unique Meeting Identification Number; in addition, we will establish a unique one-time password for each mediation.**

3. **We will gather participants in a virtual waiting room and admit them upon authentication of legitimacy, and lock the meeting to new entrants once all expected attendees are accounted for.**
4. **We will disable the Record function for the host and all attendees, and reiterate to all that recording a mediation is illegal and subject to severe sanctions by the court.**
5. **We will only use enterprise programs that offer data encryption. We will make available all commonly used videoconferencing applications, including Zoom, GoToMeeting and WebEx; as well as any others required by a client's institutional requirements.**
6. **Video platforms are constantly updating their applications and strengthening security settings. We will constantly monitor this activity, and promptly install all software updates and patches for all video platforms within our portfolio.**
7. **We will verify at the beginning of every mediation or arbitration that only authorized people are physically present with attendees at their respective locations.**