PROGRAM MATERIALS
Program #30271
November 17, 2020

How to Ethically Protect and Secure Communication in Online Dispute Resolution

Celesq® AttorneysEd Center
www.celesq.com

5255 North Federal Highway, Suite 310, Boca Raton, FL 33487
Phone 561-241-1919 Fax 561-241-1969

How to Ethically Protect and Secure Communication in Remote Dispute Resolution

By: Leslie A. Berkoff, Moritt Hock & Hamroff LLP
&
Michael Kreitman, Esq., Senior Counsel for Macy's
&
Michael Powell, Vice President, American Arbitration Association
&
Brent Clinkscale, Clinkscale Legal & Global Dispute Resolution LLC

November 17, 2020

Introduction to Topic/Learning Points:

This webinar will review key ethical concerns related to virtual and online mediations and provide practice tips as to how attorneys can collaborate with client representatives, communicate with the other parties, and mediate in an effective and confidential fashion. The panel will review the ethical concerns raised by the foregoing and discuss Rules 1.1 and 1.6 of the Model Rules of Professional Responsibility. In the wake of the COVID-19, many practitioners are working from home offices or remote locations which presents an overlay of ethical challenges to effective confidential communication between attorney and client, among parties on the same side, and effective mediation advocacy and negotiation by parties and their attorneys. How can you work within these constraints to collaborate with your client representatives and effectively present your position to the mediator and the opposing parties? Addressing these challenges requires additional skills and techniques. The panel will explore what steps can be taken to properly and ethically prepare to mediate in a virtual and online forum and identify measures you can take to facilitate the process. The panel will also suggest means for addressing security concerns during the online dispute resolution process and what, if any, additional measures, agreements or steps counsel should be asking for and insisting on from other parties to the process, as well as their neutral to ensure fair, confidential, and ethical online dispute resolution.

Moritt Hock & Hamroff LLP
ATTORNEYS AT LAW

How to Prepare for the Virtual Session

- Setting up your physical environment
- Advance Preparation
- Dry-runs and Practices
- Discussion of Selected Commonly Used Platforms
- Some Key Security Protocols
- Ethical Rules to Consider
- Questions?

Moritt Hock & Hamroff LLP
ATTORNEYS AT LAW

Setting Up Your Remote or Actual Office

- Participants should participate in the mediation from a location with secure, reliable, high-speed internet
- Test internet speeds by searching “internet speed test” in the web browser. (The minimum Mbps download and upload speeds needed for the platform depends on several factors, including the expected number of participants and the number of locations from where they are connecting the platform)
- If internet connection is unstable, weak, or prone to outages, consider:
  - Using a Wi-Fi booster
  - Using a smartphone hotspot
  - Hardwiring the internet connection by installing a direct ethernet (T-1) connection.

Moritt Hock & Hamroff LLP
ATTORNEYS AT LAW

Microphone, Speaker and Camera

- Be sure to test to ensure you have a functional microphone and speaker to transmit and receive audio
- Beware of phone feedback
- Consider separate headset or headphones that contains a microphone (also often reduces or completely blocks ambient noise).
- Keep in mind that sound clarity is especially important for participants working from home with other people or pets present or when appliances (such as air conditioners) may generate significant ambient noise

Moritt Hock & Hamroff LLP
ATTORNEYS AT LAW

Disconnected Participants/Trouble Shooting

Develop clear guidelines for all parties so they know what to do if this occurs:

- Try to reconnect to the platform (this often resolves the problem if the mediator did not lock the session)
- Contact the mediator (and possibly others) via email or text message to alert the mediator of the connection issue, consider prior exchange of cellphone numbers
- Use provided dial-in instructions to connect by telephone

Moritt Hock & Hamroff LLP
ATTORNEYS AT LAW

Connecting to the Mediation Session/Advance Preparation

- Download the platform software application
- Choose a location that offers an adequate internet connection, quiet, and privacy – do not use public WiFi
- If desired, have two screens available so you can view other participants and documents at the same time
- Conduct a dry run of the platform and individual set-ups to test and receive feedback on a variety of different aspects, including:
  - Microphones
  - Speakers
  - Headsets
  - Sound (including feedback and background noise)
  - Lighting (avoiding backlighting and facing cameras away from windows)

Moritt Hock & Hamroff LLP
ATTORNEYS AT LAW

Common Platforms

There are many VTC platforms in the marketplace. Zoom has become a perennial favorite among many mediators and counsel. However, there are many other VTC platforms, each with their own distinct features, limitations, and security and privacy issues, such as (in alphabetical order):

- Apple FaceTime
- BlueJeans
- Cisco WebEx
- Google Meet (formerly Hangouts Meet)
- GoToMeeting
- Immediation
- Legaler
- Microsoft Teams
- Modron
- Skype for Business (being replaced by Microsoft Teams on 7/31/21)
- Sonexis

Moritt Hock & Hamroff LLP
ATTORNEYS AT LAW

Key Tips For Security

- Take advantage of other tools to limit access to mediation:
  - Ensure only invited participants are able to join your mediation
  - Passcode protect the mediation and use unique ID numbers for each mediation
  - Passcode protect the session and creating a two-factor authentication requirement by:
  - Not embedding the passcode in the link; and
  - Conveying the link and the passcode by using separate mediums (for example, emailing the link and sending the passcode by text message)
- Caution participants not to share the conference link in any kind of public forum to increase the likelihood of unwanted attendees accessing the session

Moritt Hock & Hamroff LLP
ATTORNEYS AT LAW

Key Tips For Security - continued

- Some services may give the host the option to lock the meeting once the expected participants have arrived
- Some programs provide host with ability to remove individual users from the meeting should the need arise
- Note: these features may not be enabled by default, so look carefully at what settings are available

Additional Security Tips

- When ready to join the mediation session, each participant should close unnecessary tabs and applications on the device to prevent battery drain and internet bandwidth
- Be sure to turn off email, calendar reminder, and other notifications, as well as silencing phones, also prevents unnecessary disruptions and distractions
- When you join a meeting, your video camera and microphone may be on by default. Be aware that participants may be able to see and hear you as soon as you join a meeting
- Most services allow you to mute yourself or turn off your camera. You may be able to adjust the default settings so your preferences are stored for the next meeting or – depending on the service – you may need to adjust your settings at the beginning of each call.
- Check to see if your video conference is being recorded, covered in mediation agreement and reviewed at outset of mediation
- The safest strategy is to assume you might be recorded and, if possible, avoid sharing private information via video conference
- No photos please! Remind participants of this restrictions

Moritt Hock & Hamroff LLP
ATTORNEYS AT LAW

Key Security Tips - continued

Unauthorized Attendees/Access

- The mediator needs to know who everyone is on the platform so be sure to identify all attendees
- There can be disclosure issues arising from unauthorized attendees
- This is an important to issue safeguarding information
- Family members or others who may breach the confidentiality of mediation
- Party representatives with other attorneys nearby also need to be identified

Moritt Hock & Hamroff LLP
ATTORNEYS AT LAW

Ethical Rules

ABA Model Rules of Conduct

Rule 1.1 Competence

> A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

What does this mean when it comes to virtual hearings? You must have the knowledge “reasonably necessary” to represent the client in a “ZOOM” hearing.

AAA Rule 32(c): “When deemed appropriate, the arbitrator may also allow for the presentation of evidence by alternative means ***including video conferencing***, internet communication, telephonic conferences and means other than an in-person presentation.”

Moritt Hock & Hamroff LLP
ATTORNEYS AT LAW

Ethical Rules

ABA Model Rules of Conduct

Rule 1.6 Confidentiality of Information

> (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.

What does this mean when it comes to virtual hearings? You should have an agreement in writing that specifies the VTC platform and agreement about the ground rules. Example: “no one is allowed in the room where a witness is testifying.”

Ethical complaints may arise when parties and the arbitrator agree on process and procedures on a pre-hearing status call a week before the hearings and nothing is reduced to writing. Problem: the first day of hearing the arbitrator thinks she sees an unauthorized attorney in the room with a witness?

Moritt Hock & Hamroff LLP
ATTORNEYS AT LAW

Ethical Rules

ABA Model Rules of Conduct

Rule 5.1 Responsibilities of a Partner or Supervisory Lawyer

> A partner in a law firm...shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that all lawyers in the firm conform to the Rules of Professional Conduct.

What does this mean when it comes to virtual hearings? Firms need to stay abreast of current cybersecurity measures to safeguard services it provides to its clients. Example: the firm utilizes a secure encrypted email platform to share documents.

Ethical complaints may arise when an attorney, working remotely on a different computer without encrypted email, decides to share sensitive, confidential documents because the VTC platform states it is secured with end-to-end encryption. Don't rely on VTC platform security measures, also, you want to check if the VTC platform has the ability to decrypt your meeting content.

Moritt Hock & Hamroff LLP
ATTORNEYS AT LAW

Questions?

#2388513

LESLIE A. BERKOFF

Practice Areas - Dispute Resolution / Bankruptcy & Creditors' Rights / Litigation

- Leslie A. Berkoff is a Partner with the firm where she serves as Chair of the firm's Dispute Resolution Practice Group. A skilled mediator having handled mediations in bankruptcy courts for all phases of bankruptcy-related litigation, as well as, commercial mediations in the state and federal courts and arbitration as a panel arbitrator through the American Arbitration Association. Ms. Berkoff is the past Chair of the firm's Creditors' Rights and Restructuring Department and is also involved in all aspects of creditors' rights and insolvency matters, as well as, bankruptcy cases nationwide and related litigation, including creditor, debtor, committee, and trustee representation, as well as corporate liquidations, reorganizations and out-of-court restructurings and assignments for benefits of creditors. Various concentrations including equipment and asset based lending and healthcare industries.

- Prior to joining Moritt Hock & Hamroff LLP, Ms. Berkoff served as a law clerk to the Honorable Jerome Feller, United States Bankruptcy Judge in the Eastern District of New York, from 1991 to 1993 and to the Honorable Allyne R. Ross, Federal Magistrate Judge in the Eastern District of New York, from 1990 to 1991.

- Ms. Berkoff speaks and publishes extensively and is a recognized leader in her field.

Education - Hofstra University School of Law, J.D. 1990
Editor in Chief, Hofstra Labor Law Journal
State University of Albany, B.A. 1987 *cum laude*

Admissions - Ms. Berkoff is admitted to practice in New York and Connecticut

Michael E. Kreitman is a Senior Counsel in the Macy's Law Department in New York City

Michael counsels human resources executives and senior management at the Macys and Bloomingdale's stores and support divisions on all aspects of employment and labor law, including wage and hour matters, corporate restructurings/reorganizations, internal investigations, FMLA/ADA/ADEA/Title VII issues, hiring/termination/ disciplinary actions, policy and handbook formulation, collective bargaining negotiations, union grievances, and contract interpretation. Michael also handles global employment matters for the company's overseas operations, represents Macy's before local, state and federal agencies, and handles arbitration and mediation. Michael develops and conducts individual and group training on a wide variety of employment law and human resource issues. He is also on the employment mediation panel of the United States District Court for the Southern District of New York and regularly mediates employment disputes.

Michael Powell, Vice President of AAA

Michael Powell is a vice president at the American Arbitration Association® (AAA)...the global leader in dispute resolution services, and manages the Los Angeles Regional Office. Powell, 27 years with AAA, heads up the AAA Construction Division—western region, with direct responsibility for eleven states. In this role, he interacts with AAA clients who file cases and the panelists who serve as arbitrators and mediators in those cases. He also trains commercial arbitrators and aspiring mediators in basic to advanced case management techniques.

Powell also works closely with industry organizations and associations as liaison for the AAA's *National Construction Dispute Resolution Committee* (NCDRC). In this capacity, Powell assists the corporate, legal, and public sector communities by educating them on the most current dispute avoidance and resolution techniques. He gives back to the ADR community with his service as an active Board Member and past President of the California Dispute Resolution Council.

Brent Clinkscale, Managing Member of Clinkscale Legal & Global Dispute Resolution LLC

He is a veteran litigator and advocate in both trials and arbitrations. He has tried numerous cases in both federal and state courts. Brent's concentration is in business litigation, including both domestic and international arbitrations. He has experience in the defense of complex business matters, including class actions and Multi District Litigation.

Brent is a member of the **American Arbitration Association (AAA) Domestic Panel of Commercial Arbitrators** and a member of the **International Center for Dispute Resolution (ICDR) International Panel of Arbitrators**. He is presently the President Elect of the Atlanta International Arbitration Society (AtLAS), a Vice Chair of the United States Council for International Business (USCIB) Southeastern Arbitration Subcommittee and Chair of the South Carolina Bar International Committee.

Excerpts from the ABA Model Rules of Professional Conduct

Rule 1.1 Competence

A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

Comment

Maintaining Competence

[8] 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.

Rule 1.6 Confidentiality Of Information

(a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).

(b) A lawyer may reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary:

(1) to prevent reasonably certain death or substantial bodily harm;

(2) to prevent the client from committing a crime or fraud that is reasonably certain to result in substantial injury to the financial interests or property of another and in furtherance of which the client has used or is using the lawyer's services;

(3) to prevent, mitigate or rectify substantial injury to the financial interests or property of another that is reasonably certain to result or has resulted from the client's commission of a crime or fraud in furtherance of which the client has used the lawyer's services;

(4) to secure legal advice about the lawyer's compliance with these Rules;

(5) to establish a claim or defense on behalf of the lawyer in a controversy between the lawyer and the client, to establish a defense to a criminal charge or civil claim against the lawyer based upon conduct in which the client was involved, or to respond to allegations in any proceeding concerning the lawyer's representation of the client;

(6) to comply with other law or a court order; or

(7) to detect and resolve conflicts of interest arising from the lawyer's change of employment or from changes in the composition or ownership of a firm, but only if

the revealed information would not compromise the attorney-client privilege or otherwise prejudice the client.

(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.

Comment

[17] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. The duty does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered to determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to use a means of communication or security measures not required by this Rule, or may give informed consent (as in an engagement letter or similar document) to the use of means or measures that would otherwise be prohibited by this Rule.

Rule 1.7 Conflict Of Interest: Current Clients

(a) Except as provided in paragraph (b), a lawyer shall not represent a client if the representation involves a concurrent conflict of interest. A concurrent conflict of interest exists if:

(1) the representation of one client will be directly adverse to another client; or

(2) there is a significant risk that the representation of one or more clients will be materially limited by the lawyer's responsibilities to another client, a former client or a third person or by a personal interest of the lawyer.

(b) Notwithstanding the existence of a concurrent conflict of interest under paragraph (a), a lawyer may represent a client if:

(1) the lawyer reasonably believes that the lawyer will be able to provide competent and diligent representation to each affected client;

(2) the representation is not prohibited by law;

(3) the representation does not involve the assertion of a claim by one client against another client represented by the lawyer in the same litigation or other proceeding before a tribunal; and

(4) each affected client gives informed consent, confirmed in writing.

Rule 1.8 Conflict Of Interest: Current Clients: Specific Rules

(a) A lawyer shall not enter into a business transaction with a client or knowingly acquire an ownership, possessory, security or other pecuniary interest adverse to a client unless:

(1) the transaction and terms on which the lawyer acquires the interest are fair and reasonable to the client and are fully disclosed and transmitted in writing in a manner that can be reasonably understood by the client;

(2) the client is advised in writing of the desirability of seeking and is given a reasonable opportunity to seek the advice of independent legal counsel on the transaction; and

(3) the client gives informed consent, in a writing signed by the client, to the essential terms of the transaction and the lawyer's role in the transaction, including whether the lawyer is representing the client in the transaction.

(b) A lawyer shall not use information relating to representation of a client to the disadvantage of the client unless the client gives informed consent, except as permitted or required by these Rules.

(c) A lawyer shall not solicit any substantial gift from a client, including a testamentary gift, or prepare on behalf of a client an instrument giving the lawyer or a person related to the lawyer any substantial gift unless the lawyer or other recipient of the gift is related to the client. For purposes of this paragraph, related persons include a spouse, child, grandchild, parent, grandparent or other relative or individual with whom the lawyer or the client maintains a close, familial relationship.

(d) Prior to the conclusion of representation of a client, a lawyer shall not make or negotiate an agreement giving the lawyer literary or media rights to a portrayal or account based in substantial part on information relating to the representation.

(e) A lawyer shall not provide financial assistance to a client in connection with pending or contemplated litigation, except that:

(1) a lawyer may advance court costs and expenses of litigation, the repayment of which may be contingent on the outcome of the matter; and

(2) a lawyer representing an indigent client may pay court costs and expenses of litigation on behalf of the client.

(f) A lawyer shall not accept compensation for representing a client from one other than the client unless:

(1) the client gives informed consent;

(2) there is no interference with the lawyer's independence of professional judgment or with the client-lawyer relationship; and

(3) information relating to representation of a client is protected as required by Rule 1.6.

(g) A lawyer who represents two or more clients shall not participate in making an aggregate settlement of the claims of or against the clients, or in a criminal case an aggregated agreement as to guilty or nolo contendere pleas, unless each client gives informed consent, in a writing signed by the client. The lawyer's disclosure shall include the existence and nature of all the claims or pleas involved and of the participation of each person in the settlement.

(h) A lawyer shall not:

(1) make an agreement prospectively limiting the lawyer's liability to a client for malpractice unless the client is independently represented in making the agreement; or

(2) settle a claim or potential claim for such liability with an unrepresented client or former client unless that person is advised in writing of the desirability of seeking and is given a reasonable opportunity to seek the advice of independent legal counsel in connection therewith.

(i) A lawyer shall not acquire a proprietary interest in the cause of action or subject matter of litigation the lawyer is conducting for a client, except that the lawyer may:

(1) acquire a lien authorized by law to secure the lawyer's fee or expenses; and

(2) contract with a client for a reasonable contingent fee in a civil case.

(j) A lawyer shall not have sexual relations with a client unless a consensual sexual relationship existed between them when the client-lawyer relationship commenced.

(k) While lawyers are associated in a firm, a prohibition in the foregoing paragraphs (a) through (i) that applies to any one of them shall apply to all of them.

Client-Lawyer Relationship

Rule 1.9 Duties To Former Clients

(a) A lawyer who has formerly represented a client in a matter shall not thereafter represent another person in the same or a substantially related matter in which that person's interests are materially adverse to the interests of the former client unless the former client gives informed consent, confirmed in writing.

(b) A lawyer shall not knowingly represent a person in the same or a substantially related matter in which a firm with which the lawyer formerly was associated had previously represented a client

(1) whose interests are materially adverse to that person; and

(2) about whom the lawyer had acquired information protected by Rules 1.6 and 1.9(c) that is material to the matter;

unless the former client gives informed consent, confirmed in writing.

(c) A lawyer who has formerly represented a client in a matter or whose present or former firm has formerly represented a client in a matter shall not thereafter:

(1) use information relating to the representation to the disadvantage of the former client except as these Rules would permit or require with respect to a client, or when the information has become generally known; or

(2) reveal information relating to the representation except as these Rules would permit or require with respect to a client.

Rule 1.16 Declining Or Terminating Representation

(a) Except as stated in paragraph (c), a lawyer shall not represent a client or, where representation has commenced, shall withdraw from the representation of a client if:

(1) the representation will result in violation of the rules of professional conduct or other law;

(2) the lawyer's physical or mental condition materially impairs the lawyer's ability to represent the client; or

(3) the lawyer is discharged.

(b) Except as stated in paragraph (c), a lawyer may withdraw from representing a client if:

(1) withdrawal can be accomplished without material adverse effect on the interests of the client;

(2) the client persists in a course of action involving the lawyer's services that the lawyer reasonably believes is criminal or fraudulent;

(3) the client has used the lawyer's services to perpetrate a crime or fraud;

(4) the client insists upon taking action that the lawyer considers repugnant or with which the lawyer has a fundamental disagreement;

(5) the client fails substantially to fulfill an obligation to the lawyer regarding the lawyer's services and has been given reasonable warning that the lawyer will withdraw unless the obligation is fulfilled;

(6) the representation will result in an unreasonable financial burden on the lawyer or has been rendered unreasonably difficult by the client; or

(7) other good cause for withdrawal exists.

(c) A lawyer must comply with applicable law requiring notice to or permission of a tribunal when terminating a representation. When ordered to do so by a tribunal, a lawyer shall continue representation notwithstanding good cause for terminating the representation.

(d) Upon termination of representation, a lawyer shall take steps to the extent reasonably practicable to protect a client's interests, such as giving reasonable notice to the client, allowing time for employment of other counsel, surrendering papers and property to which the client is entitled and refunding any advance payment of fee or expense that has not been earned or incurred. The lawyer may retain papers relating to the client to the extent permitted by other law.

Rule 4.4 Respect For Rights Of Third Persons

(a) In representing a client, a lawyer shall not use means that have no substantial purpose other than to embarrass, delay, or burden a third person, or use methods of obtaining evidence that violate the legal rights of such a person.

(b) A lawyer who receives a document or electronically stored information relating to the representation of the lawyer's client and knows or reasonably should know that the document or electronically stored information was inadvertently sent shall promptly notify the sender.

Rule 5.5 Unauthorized Practice Of Law; Multijurisdictional Practice Of Law

(a) A lawyer shall not practice law in a jurisdiction in violation of the regulation of the legal profession in that jurisdiction, or assist another in doing so.

(b) A lawyer who is not admitted to practice in this jurisdiction shall not:

(1) except as authorized by these Rules or other law, establish an office or other systematic and continuous presence in this jurisdiction for the practice of law; or

(2) hold out to the public or otherwise represent that the lawyer is admitted to practice law in this jurisdiction.

(c) A lawyer admitted in another United States jurisdiction, and not disbarred or suspended from practice in any jurisdiction, may provide legal services on a temporary basis in this jurisdiction that:

(1) are undertaken in association with a lawyer who is admitted to practice in this jurisdiction and who actively participates in the matter;

(2) are in or reasonably related to a pending or potential proceeding before a tribunal in this or another jurisdiction, if the lawyer, or a person the lawyer is assisting, is authorized by law or order to appear in such proceeding or reasonably expects to be so authorized;

(3) are in or reasonably related to a pending or potential arbitration, mediation, or other alternative resolution proceeding in this or another jurisdiction, if the services arise out of or are reasonably related to the lawyer's practice in a jurisdiction in which the lawyer is admitted to practice and are not services for which the forum requires pro hac vice admission; or

(4) are not within paragraphs (c) (2) or (c)(3) and arise out of or are reasonably related to the lawyer's practice in a jurisdiction in which the lawyer is admitted to practice.

(d) A lawyer admitted in another United States jurisdiction or in a foreign jurisdiction, and not disbarred or suspended from practice in any jurisdiction or the equivalent thereof, or a person otherwise lawfully practicing as an in-house counsel under the laws of a foreign jurisdiction, may provide legal services through an office or other systematic and continuous presence in this jurisdiction that:

(1) are provided to the lawyer's employer or its organizational affiliates, are not services for which the forum requires pro hac vice admission; and when performed by a foreign lawyer and requires advice on the law of this or another U.S. jurisdiction or of the United States, such advice shall be based upon the advice of a lawyer who is duly licensed and authorized by the jurisdiction to provide such advice; or

(2) are services that the lawyer is authorized by federal or other law or rule to provide in this jurisdiction.

(e) For purposes of paragraph (d):

(1) the foreign lawyer must be a member in good standing of a recognized legal profession in a foreign jurisdiction, the members of which are admitted to practice as lawyers or counselors at law or the equivalent, and subject to effective regulation and discipline by a duly constituted professional body or a public authority; or,

(2) the person otherwise lawfully practicing as an in-house counsel under the laws of a foreign jurisdiction must be authorized to practice under this rule by, in the exercise of its discretion, [the highest court of this jurisdiction].

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Video conferencing: 10 privacy tips for your business

Share This Page

Jonah Fabricant
Apr 16, 2020

TAGS: Bureau of Consumer Protection | Consumer Protection | Privacy and Security | Consumer Privacy | Data Security | Small Business

Between social distancing and COVID-19 stay-at-home orders, companies are turning to video conferencing services to get down to business. While these services help you connect, they also pose new privacy and data security risks. Here are some tips to keep in mind before hosting or joining a video conference online:

1. **Take steps to ensure only invited participants are able to join your meeting.** People may call it "zoombombing," but it's a consideration across all kinds of platforms: uninvited people showing up on video conferences. What can your company do to reduce the risk? Some services allow hosts to password-protect a meeting. Others limit access by providing unique ID numbers for each meeting or for each participant. These features may not be enabled by default, so look carefully at what settings are available. If you host recurring meetings, most services allow you to create new passwords or ID numbers for each meeting. That method is more secure than reusing old credentials, so establish that as the policy for your employees.
2. **Take advantage of other tools to limit access to meetings.** Conferencing services may give the host the option to lock the meeting once the expected participants have arrived, preventing others from joining. For the greatest level of control, hosts can enable settings allowing them to approve each participant trying to join in. You also may have the ability to remove individual users from the meeting should the need arise.
3. **When you join a meeting, your video camera and microphone may be on by default.** Be aware that participants may be able to see and hear you as soon as you join a meeting. If you don't want to share sound or video, most services allow you to mute yourself or turn off your camera. You may be able to adjust the default settings so your preferences are stored for the next meeting or – depending on the service – you may need to adjust your settings at the beginning of each call.
4. **Check to see if your video conference is being recorded.** Many services allow the host to record the meeting for future reference. The service should display some indicator you're being recorded – for example, a bright red circle or the word "recording." But remember that a meeting may be recorded even if these indicators don't appear. We've heard reports of video conferences that have been shared online without participants' knowledge. The safest strategy is to assume you might be recorded and, if possible, avoid sharing private information via video conference,
5. **Be careful before sharing your screen.** Most services have functions to allow you to share with the group what's on your screen – for example, a slide show. But before sharing your screen, make sure you don't have open documents, browser windows, or other things on your screen you don't intend for others to see. Some services have options that allow the host to turn off screen sharing or to limit its use to the host.

6. **Don't open unexpected video conference invitations or click on links.** With the upsurge in video conferencing, malicious actors are sending emails mimicking meeting invitations or other communications from conferencing services. To add authenticity, they may copy the logo and look of familiar names in the business. But instead of taking you to a conference, those links may contain viruses or install malware on your computer. The safer practice is to tell your staff or your clients in advance that you have a teleconference planned for a certain time and they should expect an invitation with your name. If they get an invitation they didn't expect, tell them not to open it and definitely don't click on any links. Another tip to help foil video conference imposters: If the service you're using requires you to download an app or desktop application, make sure you download it directly from the service's website or a platform's app store.
7. **If confidentiality is crucial, video conferencing may not be the best option.** No conferencing service can guarantee the security of your information, so consider alternatives if you need to talk about particularly sensitive topics. Evaluate whether an enterprise service would provide greater security for your company and clients, rather than free services available to the general public. If you're conferencing remotely with a health care provider, ask about dedicated telehealth conferencing services that can include more safeguards to keep information private.
8. **Before using a conferencing service, review key provisions in the service's privacy policy to understand how your information will be handled.** What information does the conferencing service collect about you? Does the privacy policy limit the company from using your information for purposes other than providing their conferencing service? Finally, does the conferencing service share your information with advertisers or other third parties?
9. **Update your video conferencing software.** As security issues arise, many video conferencing companies are updating their software with patches and fixes. That's why it's important for your business to use the improved version. Of course, only accept updates directly from the service's website.
10. **Establish preferred video conferencing practices at your business.** Your employees are doing their best to maintain productivity during a trying time. But a well-meaning staffer may inadvertently put sensitive data at risk by enabling video conferencing services that don't meet your company's privacy or security standards or that could be out-and-out malware. Share these ten tips with your team, establish company-wide video conferencing dos and don'ts, and emphasize the need to select the more secure options when hosting or joining video conferences.

AMERICAN ARBITRATION ASSOCIATION® | INTERNATIONAL CENTRE FOR DISPUTE RESOLUTION®

AAA-ICDR® Virtual Hearing Guide for Arbitrators and Parties Utilizing ZOOM

Optimizing the Virtual Hearing Experience*

1. Use a PC, laptop or large tablet for the video portion of the hearing as monitor size will be important, particularly for hearings with many participants
2. The device/screen you are using to participate in the virtual hearing will not be available for other purposes, such as taking notes or viewing documents; arrange for alternate means of doing so
   a. Use of dual monitors (or even a single monitor with a laptop screen) is recommended, with Zoom running on one screen
3. Disable any pop-up notifications within applications such as Outlook and Skype to prevent these from appearing onscreen while presenting
4. Use a good quality webcam if possible, and check lighting conditions
   a. Backlighting is generally not desirable
   b. For AAA staff, use a virtual background image provided by Marketing
5. Audio considerations
   a. Audio quality can be affected by a variety of factors and may take some experimentation to come up with the best way to connect, whether by phone, through your computer speakers/microphone, and with or without a headset; try to determine your best method prior to the scheduled event.
   b. If there are multiple participants in the same physical location, there may be an echo if their microphones/phones are not muted (this is highly dependent on the equipment being used but is obvious when it occurs)
   c. Find a quiet location
      - Minimize background noise
      - Mute yourself whenever you are not speaking
      - Take notes quietly if not muted, if necessary on paper as opposed to using a keyboard
      - Avoid multi-tasking such as checking email
6. Consider steps that may be taken to establish a high-speed internet connection (e.g., if possible, a hard-wired internet connection is generally preferable to a wireless internet connection)

---

* Please note that video hearings or proceedings are conducted through third party platforms such as Zoom are subject to the platform's terms and policies, for example: https://zoom.us/privacy-and-legal. The AAA-ICDR arranges proceedings through these third party platforms for the arbitrators' and parties' convenience. The AAA-ICDR does not endorse any one platform over another nor does the AAA-ICDR guarantee the suitability or availability of any platform. Any concerns regarding the use of a third party video conferencing platform should be raised by copying correspondence to all parties to this matter.

a. Recognize that much of the technology infrastructure involved is not in our control and there may be conditions under which a virtual hearing is not feasible

b. Consider arranging for a "lower technology" backup alternative such as an audio-only conference bridge

Zoom Technical Support

1. Zoom hardware test is available here: https://zoom.us/test
2. Zoom technical support is here: https://support.zoom.us/hc/en-us
3. Zoom Support by Chat
   a. Zoom support is available whenever you are logged into a Zoom account at Zoom.us
   b. Go to 'Help' at the bottom right
   c. Click the 'Live Chat' button

Virtual Hearing Security Considerations

See Appendix A - Default Meeting Settings for details, but generally:

1. A unique, automatically generated meeting ID must be used for each virtual hearing, not your personal meeting ID
   a. As an additional layer of security the hearing can be password-protected with a unique password, but that password should be shared with the participants via a medium other than via the Zoom invitation email
2. Participants should use secure internet connections and not attend from public locations or in circumstances where non-invitees could hear or see the proceedings
3. The host should be provided with the list of participants (including witnesses) and their email addresses for the purpose of inviting them to the online hearing
   a. Participants should be instructed to not forward or share the hearing invitation
   b. Any additional participants should be invited directly by the hearing host
4. You can use the Waiting Room feature to prevent ex parte communication with the arbitrators prior to the start of the event
   a. Give the waiting room a meaningful description such as *"AAA Case 01-20-0001-0003 with Arbitrator Jane Doe"*
   b. Do not include information that would disclose the identity of the parties to the case
   c. You may also want to consider including contact information for the AAA Zoom host in the description
5. Disable the "private" chat feature (only allow chat with "everyone")
6. Participants must decide if the recording feature will be utilized (see below Considerations for Recording a Zoom Hearing). If recording feature is not being utilized, disable all recording and emphasize that no independent recording or taking of screenshots is permitted

Preparing for the Virtual Hearing

1. At least one week before the hearing, have a trial run with the panel, representatives and any technical support people to verify their connectivity and get them familiar with some basic features of Zoom
   a. Basic features to cover
      - Overall display/tiling
      - Control Panel features
      - Participant list
      - Muting/unmuting
      - Screen sharing
      - Passing control
      - Inviting a non-participant
      - Waiting Room/Breakout Rooms
      - Locking the hearing
   b. If there are any technical issues with the panelists' equipment, take steps to get them resolved or decide whether the hearing can proceed virtually
   c. Discuss with the panel hosting/co-hosting responsibilities
   d. Each party is responsible for testing Zoom connectivity for its witnesses in advance of the hearing
2. Send the hearing invitation to the necessary participants
   a. Meeting set-up in Zoom
      - Send the hearing invitation via Outlook (not directly via Zoom) so that you can customize meeting subject line and body
      - Hearing description in Zoom should not contain full party information
        - Use the AAA case number
        - You may also use names of representatives and/or abbreviations of party names that do not allow for actual party identification
      - Include the following disclaimer in the Notice of Hearing and in the electronic hearing invitation:

        Please note that video hearings or proceedings are conducted through third party platforms. The use of such platforms for proceedings is subject to the platform's terms and policies, for example: https://zoom.us/privacy-and-legal The AAA-ICDR arranges proceedings through these third party platforms for the arbitrators' and parties' convenience. The AAA-ICDR does not endorse any one platform over another nor does the AAA-ICDR guarantee the suitability or availability of any platform. Any concerns regarding the use of a third party video conferencing platform should be raised by copying correspondence to all parties to this matter.

b. Decide if breakout rooms will be used and to the extent possible, set them up in advance; see guide here: https://support.zoom.us/hc/en-us/articles/360032752671
   - Special Considerations for Phone Only participants
     - Phone participants can be assigned to a break out room, however:
       i. If you assign them to the break out room before you "open all rooms" they will automatically be sent to the break out room upon "opening",
       ii. The only way that phone participants can rejoin the main room is if you "close all break out rooms" which ends them for everyone for the rest of the call (of course you could re-create them again).
     - Phone participants can be placed in the waiting room.

c. Document and communicate any ground rules in advance; see the model *Procedural Order for Virtual Hearings* for an extensive list of considerations, including:
   - How will document display be managed?
   - Conditions for witness participation
   - Camera use
   - Entering the hearing with full names
   - Whether the hearing will be recorded
   - How to manage panel conferences

At the start of the hearing

1. Show up early
2. Verify participants and their connectivity
3. The hearing host should use the Security Option feature on the control panel to manage settings during the hearing for items such as the waiting room, screen sharing, chat, and locking the meeting
4. The hearing moderator/host should keep the participant list open
   a. Clean up/combine virtual participant entries (names, duplicate phone/video sessions)
   b. Monitor waiting room activity and watch for participants who may drop off
   c. The host may lock the meeting but needs to be made aware of anyone who may need to join and then unlock the meeting; use of a waiting room is generally preferable to locking the meeting unless the extra level of security is warranted
5. Restate any ground rules
6. At least for the early part of the hearing, participants should state their names before speaking so other participants can easily identify the speaker

Considerations for Recording a Zoom Hearing

Should the case participants opt to use Zoom's recording features, they should be fully aware of Zoom's Terms of Service (https://zoom.us/terms/), and the conditions under which the session will be recorded should be formalized and shared with case participants in advance of the hearing (see Model Procedural Order for Virtual Hearings).

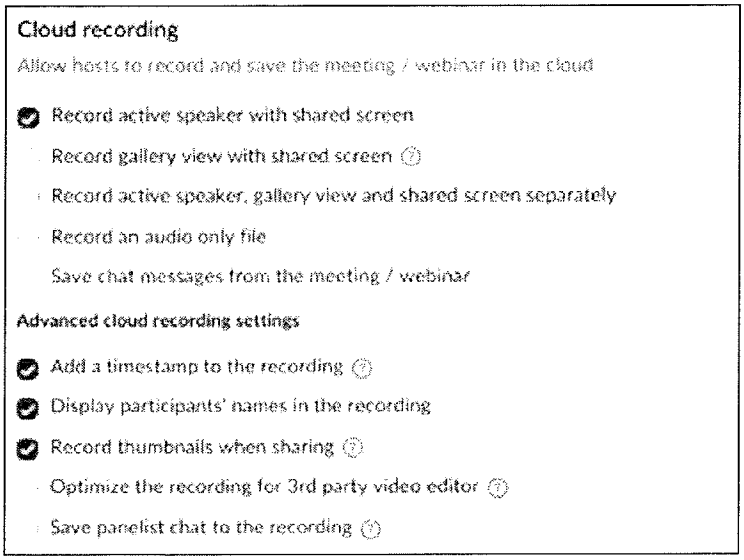
The recommended process for recorded sessions that are not conducted with AAA Zoom accounts is to use cloud storage and have the Zoom account owner send a link to the recording to case participants as directed by the arbitrator(s) or as identified in the procedural order. The link should be password protected and the password should be sent separately from the communication containing the link.

The recipients would then have seven (7) calendar days to download a local copy of the recording via the link, after which the cloud recording would be deleted. The recipients are responsible for maintaining security around and controlling access to their locally stored copies of the recordings.

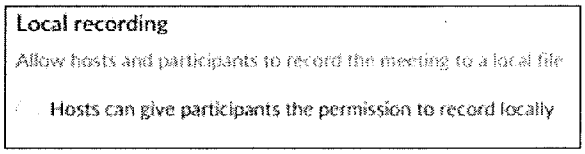
Should the case participants opt to not use cloud storage and save the recording locally, the host on whose computer the file is stored must then arrange to transmit the file to the specified case participants in a secure manner (such as via Citrix ShareFile or other file sharing tools) and also take steps to maintain the security around and control access to their locally stored copy of the recording.

Recommended Zoom Settings for Cloud Recordings

See Appendix A - Default Meeting Settings for detailed settings



Recommended Settings for Local Recording



Appendix A

AAA-ICDR Suggested Zoom Default Settings for Virtual Hearings

Schedule Meeting Settings

Configuration Section	Default Setting	Comments
Host Video	On	Allows for default to video so participants can see who is in attendance
Participants Video	On	Allows for default to video so participants can see who is in attendance
Audio Type	Telephone and Computer Audio	Allows participant to choose which has better sound quality for them
Join Before Host	Off	Keeps one party and arbitrator from being in the room together
Use Personal Meeting ID (PMI) when scheduling a meeting	Off	We must use the "generate automatically" option to randomly create a new meeting code per hearing in order to keep someone who has a link from a prior meeting from joining
Use Personal Meeting ID (PMI) when starting an instant meeting	Off	PMI not to be used
Only authenticated users can join meetings	Off	This means that the meeting participants will have to sign in to their Zoom account to join the meeting. Would require every arbitrator/party/participant/witness to create a zoom account.
Require a password when scheduling new meetings	On	
Require a password for instant meetings	On	
Require a password for Personal Meeting ID (PMI)	Off	PMI not to be used
Embed password in meeting link for one-click join	Off	
Mute participants upon entry	Off	More appropriate to be managed by host and as needed
Upcoming meeting reminder	Off	Not needed as Outlook invitations should be used

In Meeting (Basic) Settings

Configuration Section	Default Setting	Comments
Require Encryption for 3rd Party Endpoints (H323/SIP)	On	This means zoom meetings where a participant is using a different room-based solution like WebEx or Lifesize would require an encrypted connection Set to "on" in case we ever have meetings with third party endpoints, but this will not impact anything with standard Zoom meetings using the Zoom client on desktops/laptops/ mobile devices
Chat	On and check box to prevent participants from saving chat	Concern over who has access to Zoom data
Private chat	Off	Concern over who has access to Zoom data, *ex parte* communication with panel
Auto saving chats	Off	Concern over who has access to Zoom data
Play sound when participants join or leave	Off	Can be distracting; may be set to play only for the host
File Transfer	Off	Concern over who has access to Zoom data
Feedback to Zoom	Off	
Display end-of-meeting experience feedback survey	Off	
Co-host	On	
Polling	Off	
Allow host to put attendee on hold	On	Good for temporarily allowing the host to remove an attendee such as a witness

Configuration Section	Default Setting	Comments
Always show meeting control toolbar	On	
Show Zoom windows during screen share	Off	Only need to share documents/presentation
Screen Sharing	On	
Who can share?	All Participants	
Who can start sharing when someone else is sharing?	Host Only	
Disable desktop/screen share for users	Off	Needed for presenting
Annotation	On	Allows participants to mark up a document
Whiteboard	On and Uncheck Auto save white-board content when sharing is stopped	Concern over who has access to Zoom data
Remote control	On	Allows others to control shared content
Nonverbal feedback – off	Off	
Allow removed participants to rejoin – off	Off	Keeps removed people from getting back in

In Meeting (Advanced) Settings

Configuration Section	Default Setting	Comments
Breakout room	On and Check Allow host to assign participants to breakout rooms when scheduling	Only can pre-assign those with full license but n harm to allow this setting
Remote Support	Off	We do not want to get into others computers
Closed captioning	Off	
Save captions	Off	
Far end camera control	Off	
Group HD video	Off	To reduce bandwidth use
Virtual background	On	Use professional background image
Identify guest participants in the meeting/webinar	Off	Not needed as most are guests vs. someone on AAA corporate account
Auto-answer group in chat	Off	
Only show default email when sending email invites	Off	
Use HTML format email for Outlook plugin	On	
Allow users to select stereo audio in their client settings	Off	
Allow users to select original sound in their client settings	Off	

Configuration Section	Default Setting	Comments
Attention tracking	Off	Feature disabled/removed by Zoom
Waiting room	On	Can be disabled if needed (Case by case basis)
Show a "Join from your browser" link	On	Do not want to force participants to download the app
Allow live streaming meetings	Off	

Email Notification Settings

Configuration Section	Default Setting	Comments
When a cloud recording is available	On	
When attendees join meeting before host	On	
When a meeting is cancelled	On	
When an alternative host is set or removed from a meeting	On	
When someone scheduled a meeting for a host	On	
When the cloud recording is going to be permanently deleted from trash	On	

Other Settings

Configuration Section	Default Setting	Comments
Blur snapshot on iOS task switcher	Off	This setting can be used to hide potentially sensitive information on the Zoom iOS mobile app preview screen when multiple apps are open using the iOS tasks switcher Off as we don't see the need to enforce this
Direct call a room system	Off	This option enables a zoom client to directly call a room-based system instead of needing the room based system to be joined to a meeting first Off as it is not applicable to us
Invitation Email – Choose Language	English	
Schedule privilege – Assign scheduling privilege to	No one	May be used to assign privileges to other case staff

Recording Tab

Configuration Section	Default Setting	Comments
All settings	Off	See section on "Considerations for Recording a Zoom Meeting" if turning on

Telephone Tab

Configuration Section	Default Setting	Comments
All settings	On	

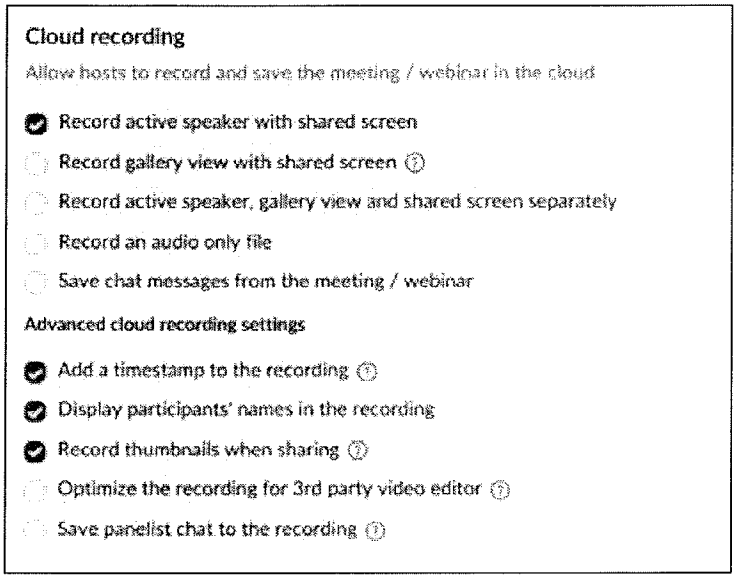
Recommended Zoom Settings for Cloud Recordings

When setting up the meeting for recording, you will need to verify these configurations.

Configuration Section	Default Setting	Comments
Local Recording	Off	If changed to yes, do not select "Hosts can give participants the permission to record locally" You must document the file distribution/retention strategy
Cloud Recording	On	See detailed settings image below
Automatic Recording	Off	
IP Address Access Control	Off	
Only authenticated users can view cloud recordings	Off	
Require password to access shared cloud recordings	On	
Auto delete cloud recordings after days	21	Set to 21 as a precaution against inadvertently premature deletion; participants should be directed to download a local copy within 7 days
The host can delete cloud recordings	On	
Recording Disclaimer	On	Set to "Ask host to confirm before recording starts"
Multiple audio notifications of recorded meeting	Off	

Detailed Cloud Recording Settings

These are the recommended settings when using cloud recording



UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

V

Civil Docket No.

CONFIDENTIALITY STIPULATION

IT IS HEREBY STIPULATED AND AGREED by and between the undersigned parties:

1. No party shall be bound by anything said or done during the Mediation, unless either a written and signed stipulation is entered into or the parties enter into a written and signed agreement.

2. The Mediator may meet in private conference with fewer than all of the parties.

3. Information obtained by the Mediator, either in written or oral form, shall be confidential and shall not be revealed by the Mediator unless and until the party who provided that information agrees to its disclosure.

4. The Mediator shall not, without the prior written consent of all parties or an order of the court, disclose to the Court any matters which are disclosed to him or her by either of the parties or any matters which otherwise relate to the Mediation.

5. The mediation process shall be considered a settlement negotiation for the purpose of all federal and state rules protecting disclosures made during such conferences from later discovery or use in evidence. The entire procedure shall be confidential, and no stenographic or other record/recording shall be made except to memorialize a settlement record. All communications, oral or written, made during the Mediation by any party or a party's agent, employee, or attorney are confidential and, where appropriate, are to be considered work product and privileged. Such communications, statements, promises, offers, views and opinions shall not be subject to any discovery or admissible for any purpose, including impeachment, in any litigation or other proceeding involving the parties. Provided, however, that evidence otherwise subject to discovery or admissible is not excluded from discovery or admission in evidence simply as a result of it having been used in connection with this mediation process.

6. The Mediator and his or her agents shall have the same immunity as judges and court employees have under Federal law and the common law from liability for any act or omission in connection with the Mediation, and from compulsory process to testify or produce documents in connection with the Mediation.

7. The parties (i) shall not call or subpoena the Mediator as a witness or expert in any proceeding relating to: the Mediation, the subject matter of the Mediation, or any thoughts or impressions which the Mediator may have about the parties in the Mediation, and (ii) shall not subpoena any notes, documents or other material prepared by the Mediator in the course of or in connection with the Mediation, and (iii) shall not offer into evidence any statements, views or opinions of the Mediator.

8. The Mediator's services have been made available to the parties through the dispute resolution procedures sponsored by the Court. In accordance with those procedures, the Mediator represents that they have taken the oath prescribed by 28 U.S.C. 453.

9. Any party to this Stipulation is required to attend at least one session and as many sessions thereafter as may be helpful in resolving this dispute.

10. An individual with final authority to settle the matter and to bind the party shall attend the Mediation on behalf of each party.

REMOTE MEDIATION AGREEMENT

11. All parties and the mediator consent to participate in an EDNY Mediation via an internet-based video conference platform provided by the mediator, and that it shall be a 'mediation' for the purposes of all applicable legislation, regulations, and rules.

12. No one shall record any portion of an EDNY Mediation to include audio, video, chat and any other aspect of the conference, and they further understand that in the event any person records any portion of a confidential EDNY mediation, that individual will be referred to the EDNY ADR Oversight Judge and may be subject to court ordered sanctions.

13. All parties will appear alone or with counsel at their location and that no one will be able to hear or observe the mediation other than the participants in the mediation. In the event any party wishes for an additional person(s)to participate in the video conference, they must disclose the identity of the additional person(s), and all parties, including the mediator, must consent to their presence. Any additional attendees must also sign this Confidentiality Stipulation and Remote Mediation Agreement.

14. All parties and the mediator affirm that they are using a secure WiFi/Ethernet connection for all conduct related to the mediation session. They further affirm that they will utilize a password or security code that will be required for entry into the video conference and that the password and/or security code will only be accessible to the participants of the mediation and will not be made available publicly.

15. An attorney of record may sign on behalf of one or more clients, and by so signing, the attorney represents that 1) the client has been fully informed of all of the terms of this stipulation, and 2) the client has affirmatively represented to be bound by the terms of this stipulation with the same force and effect as a stipulation made in open court and on the record by an attorney representing a client.

16. This document may be signed in counterparts, and once signed must be sent via e-mail to the mediator and the EDNY ADR Department at nyedadr@nyed.uscourts.gov.

Dated: _____, 2020

_____	_____
Plaintiff	Defendant
_____	_____
Plaintiff	Defendant
_____	_____
Attorney(s) for Plaintiff(s)	Attorney(s) for Defendant(s)

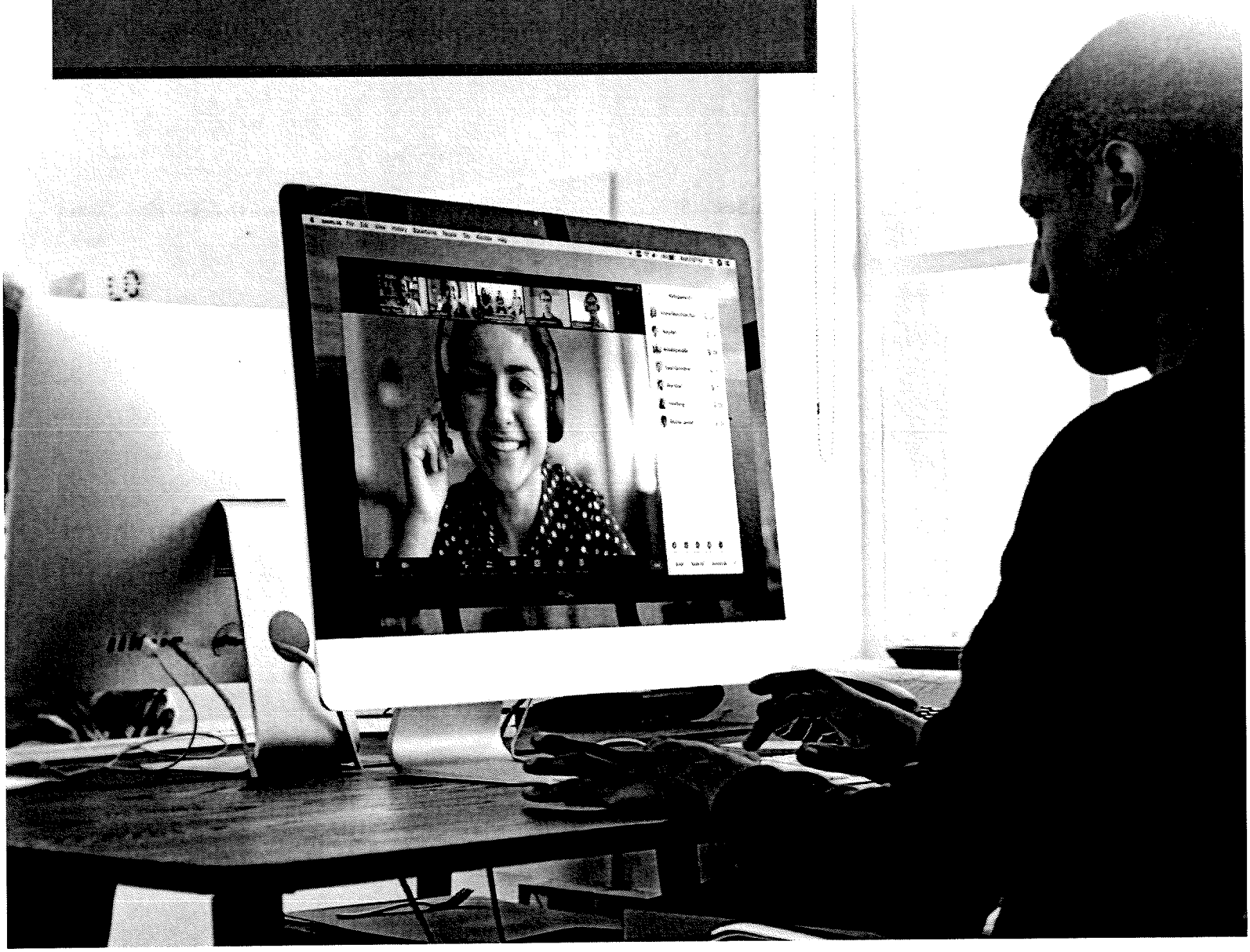
Consented to: _____
Mediator

Additional participants sign below:

_____	_____
_____	_____
_____	_____
_____	_____
_____	_____

Best Practices for Securing Your Zoom Meetings

Everything you need to keep your video meetings safe and secure.



zoom

Zoom Video Communications, Inc.

Zoom has helped thousands of businesses and organizations connect more productively, reliably, and securely with video meetings. Zoom's top priority, since the very beginning, has been to provide a safe and secure environment for all Zoom users. The Zoom platform comes loaded with host controls and numerous security features designed to effectively manage meetings, prevent disruption, and help users communicate remotely.

In this guide, learn about how you can secure your virtual meetings. The following content is separated into three distinct sections. The first section focuses on all the steps you can take to secure your meeting before it starts. The second section highlights all the controls that a Zoom Meeting host has at their disposal during a Zoom Meeting. The final section highlights a list of additional resources available to continue learning and become a Zoom Meeting expert.

About Zoom

Zoom is the leader in modern enterprise video communications, with an easy, reliable cloud platform for video and audio conferencing, collaboration, chat, and webinars across mobile devices, desktops, telephones, and room systems. Zoom Rooms is the original software-based conference room solution used around the world in board, conference, huddle, and training rooms, as well as executive offices and classrooms. Founded in 2011, Zoom helps businesses and organizations bring their teams together in a frictionless environment to get more done. Zoom is a publicly traded company on Nasdaq (ticker: ZM) and headquartered in San Jose, California.

We take security seriously and we are proud to exceed industry standards when it comes to your organization's communications.

Security questions or issues?

If you have any questions or think you may have found a security vulnerability within Zoom, please [illegible] or contact our security team directly at [illegible].

Part 1

Pre-Meeting Settings

With meeting settings in the Zoom web portal and the Zoom application, securing your Zoom Meetings can start before your event even begins.

PRO TIP: Turn on Your Waiting Room

One of the best ways to secure your meeting is to turn on Zoom's Waiting Room feature. Some Zoom users, like those in education, will have this feature turned on by default. This feature provides a virtual waiting room for your attendees and allows you to admit individual meeting participants into your meeting at your discretion.

Turn on Your Waiting Room

Users can enable Waiting Room as a default account setting, for individual meetings, or as a meeting template. Learn more about Waiting Rooms.

Customize the Experience

Once enabled, you can tailor your Waiting Room title, logo, and description, customizing what participants see when they arrive.

Add Additional Helpful Info

The description on your Waiting Room is a great place to add additional information, meeting guidelines, or rules for participants to follow.

View and Admit Participants

As meeting attendees arrive, Zoom will notify you and provide you a list of those in the meeting, and those still in the waiting room, so you have total control of who joins your meeting.

Message the Waiting Room

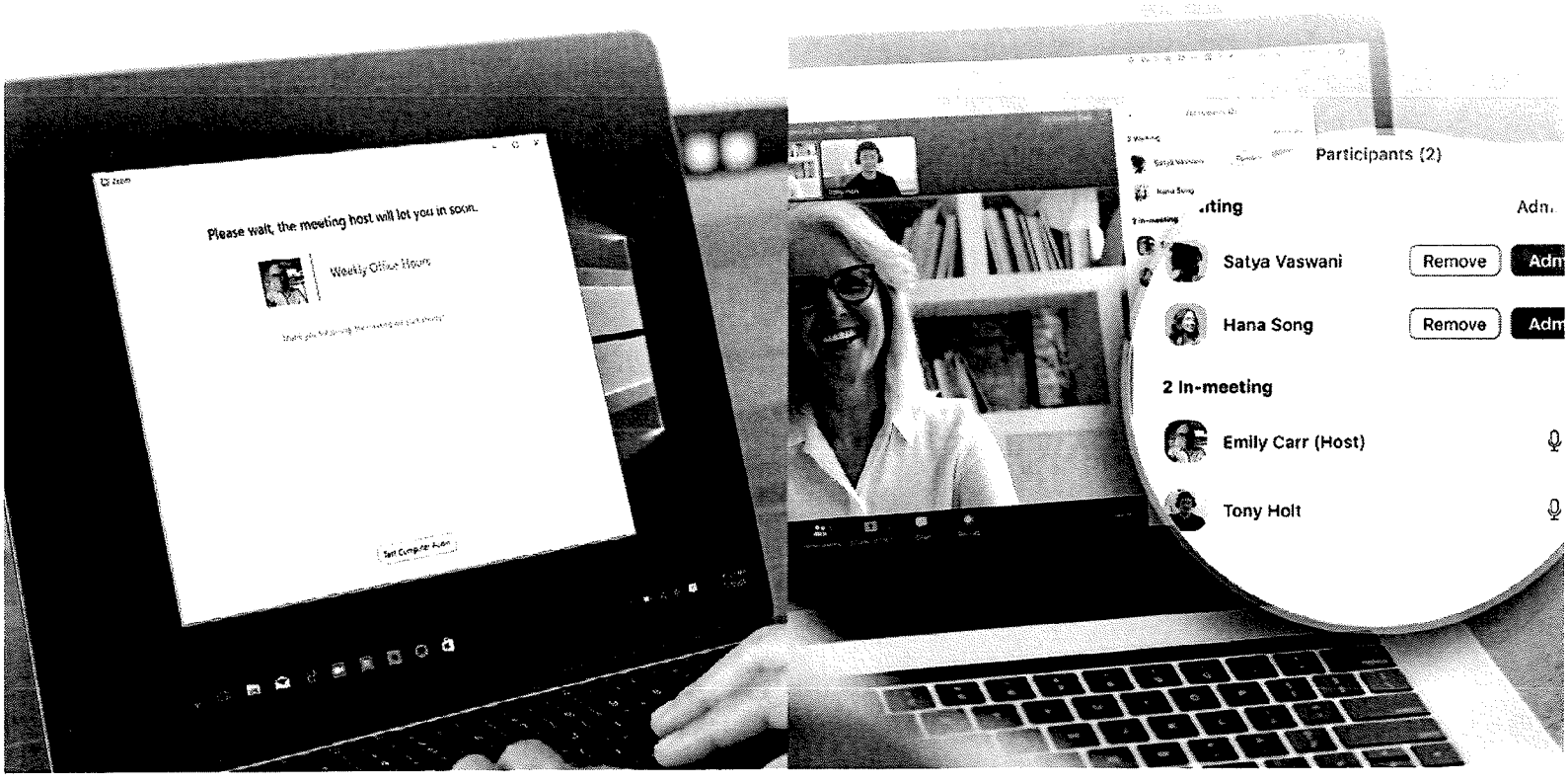
If you're meeting with a smaller group of attendees, one attendee at a time, or your previous meeting is running long, you can message everyone in the waiting room and let them know.

Remove Participants

Once you've admitted an attendee into your meeting, you can easily push them back to the Waiting Room or remove them from the meeting all together, and can even prevent their return.

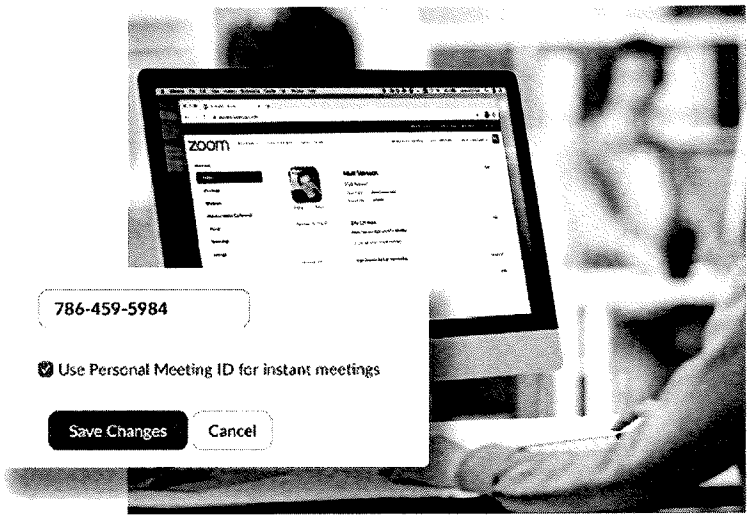
Attendee Experience

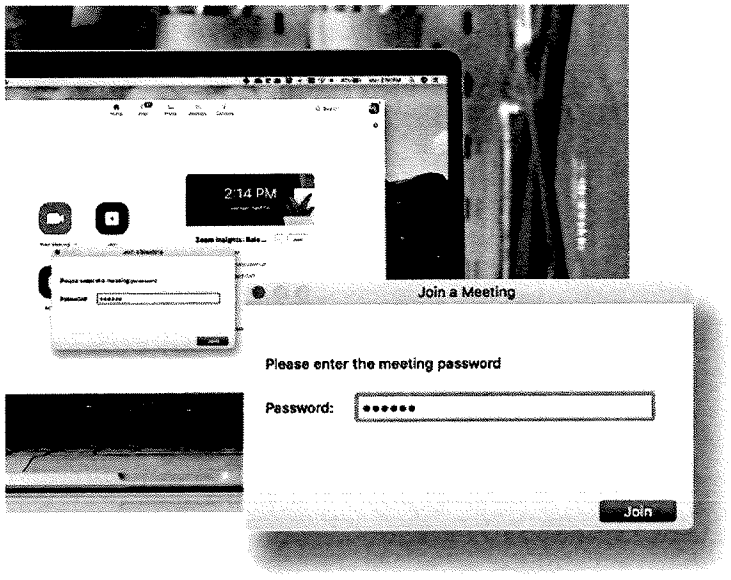
Host Experience



Don't Use Personal Meeting ID for Public Meetings

Your Personal Meeting ID (PMI) is the default meeting that launches when you start and ad hoc meeting. Your PMI doesn't change unless you change it yourself, which makes it very useful if people need a way to reach you. But for public meetings, you should always schedule new meetings with randomly generated meeting IDs. That way, only invited attendees will know how to join your meeting. You can also turn off your PMI when starting an instant meeting in your profile settings.



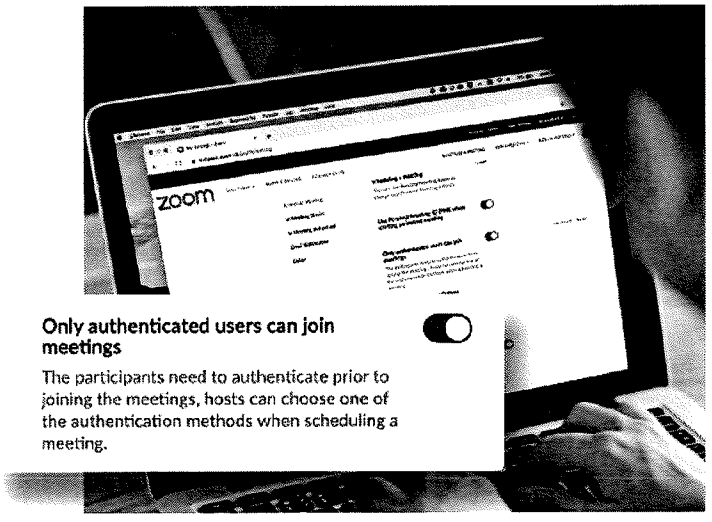


Require a Password to Join

You can take meeting security even further by requiring a password to join your meetings. This feature can be applied to both your Personal Meeting ID, so only those with the password will be able to reach you, and to newly scheduled meetings. To learn all the ways to add a password for your meetings, please view this support article.

Only Allow Registered or Domain Verified Users

Zoom can also give you peace of mind by letting you know exactly who will be attending your meeting. When scheduling a meeting, you can require attendees to register with their e-mail, name, and custom questions. You can even customize your registration page with a banner and logo. By default, Zoom also restricts participants to those who are logged into Zoom, and you can even restrict it to Zoom users who's email address uses a certain domain.



Part 2

In-Meeting Settings

Once your Zoom Meeting is off and running you'll have access to a number of helpful features that put you in total control.

PRO TIP: Master the Security Menu

Zoom now puts all your essential security options in a single button, right in the in-meeting menu. Under this menu you'll be able to lock your meeting and prevent any new participants from joining. You'll also be able to enable Waiting Room to help manage new meeting participants and be able to control any sharing and chat permissions of individuals and all attendees.

Lock the Meeting

Once all your attendees have arrived, you can easily lock your meeting from the security menu, preventing any additional attendees from joining.

Enable Waiting Room

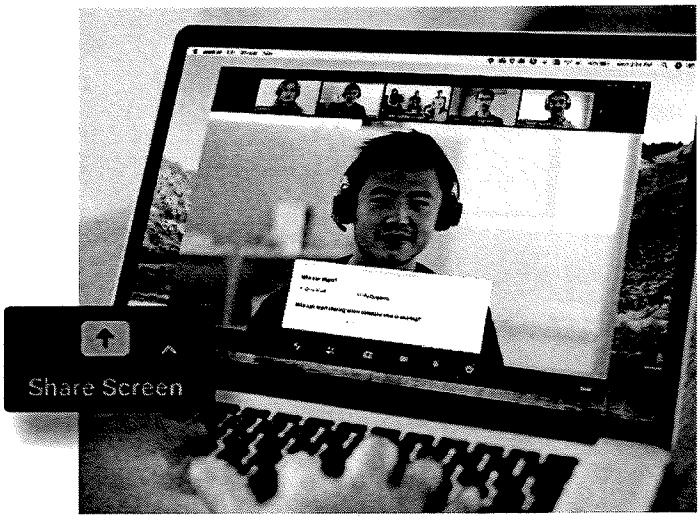
We've covered the Waiting Room in great detail already, but what if you forgot to activate it or want to turn it on mid-meeting? Now you can!

Manage Participants

In the following page, we'll dive into all the ways you can manage your participants directly from the security menu, giving you total control.

Control Screen Sharing

Allowing participants to screen share in a meeting can be a great way to collaborate, but that can also leave you open to unwanted interruptions during larger meetings. Zoom gives you the ability to determine if you want other participants in the meeting to be able to share their screens, or if you want to be the only one with that ability. You can easily toggle this feature on and off from the screen sharing menu, as well as the security menu.

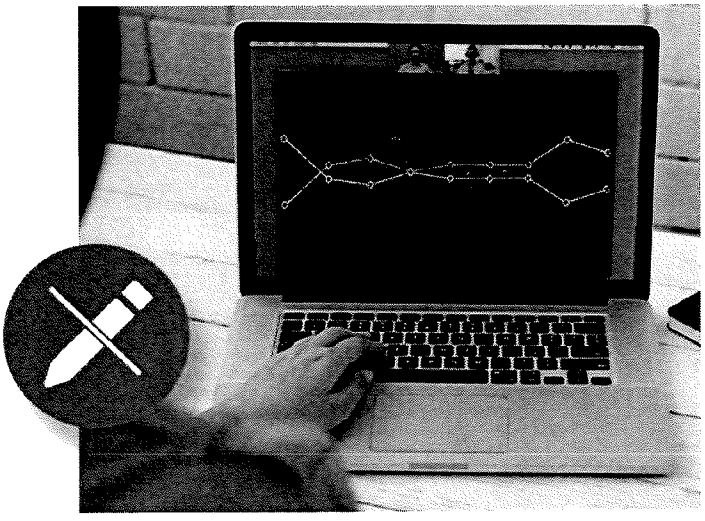


Disable Private Chat

In-meeting chat adds another dimension of collaboration to your meetings, creating a place for questions to be asked and fielded later, or for supplemental resources to be posted. But sometimes chat can become distracting or unproductive. In those cases, Zoom allows you to disable and enable chat throughout your meeting.

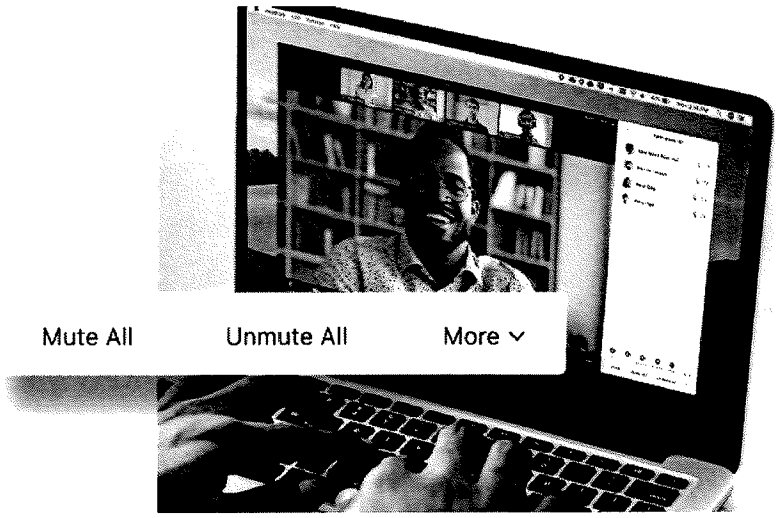
Turn Off Annotation

Like screen sharing and in-meeting chat, annotation can be a great tool when you need it, but it can also be an opportunity for mischief when you don't. To avoid unwanted annotation, Zoom allows you as the meeting host to remove all participants ability to annotate during a screen share. You can disable this for the entire meeting, or just temporarily.



Mute Participants

We've all been in meetings where somebody forgets to mute, or their microphone picks up some background noise that interrupts the meeting. Zoom allows you to solve this problem with a simple button to mute all participants. For an added layer of security, you can also disable participant's ability to unmute themselves. When you're ready to make the meeting interactive again, you can simply hit the "Unmute All" button or allow participants to unmute themselves.

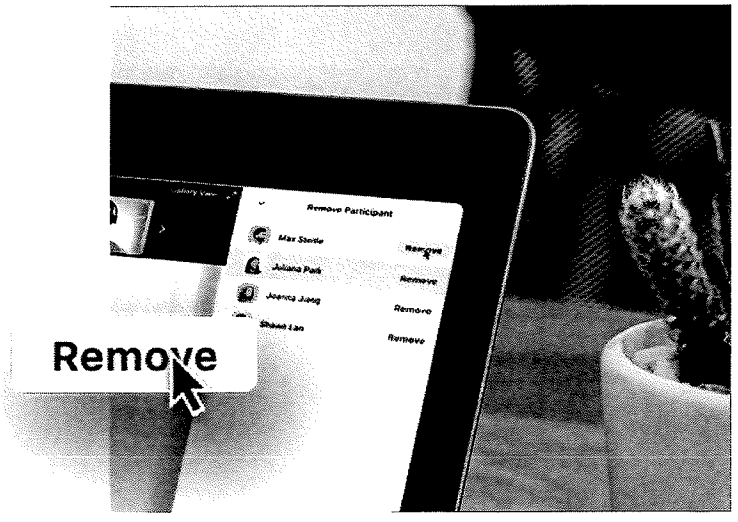


Make Someone a Co-Host

All the features we've covered so far are only accessible to meeting hosts, ensuring that hosts are the only ones with total control over a meeting. But what if you need a helping hand to manage all your participants? You can promote a trusted meeting attendee to Co-Host, allowing them many of the same privileges and control features available to the meeting host themselves. To learn about the difference between a host and co-host, view this support article.

Remove Participants

If you follow all the best practices in this guide, you should never find yourself in a meeting with an unwanted guest. But if you do need to remove an attendee from the meeting at any point, Zoom makes it easy to kick an unwanted participant out of the meeting. For additional security, you can also choose to not allow participants to rejoin once they've been removed.



Part 3

Additional Resources for Enhancing Security

When it comes to Zoom's security, our most important asset is our users and how they utilize the product.

Still have questions? We've still got you covered.

If you still have questions about specific features or functionality, we have three resources you may find helpful. The Zoom Help Center has thousands of support articles on all things Zoom. We also run weekly webinar trainings, or we have recordings you can access immediately, and the Zoom Blog is a great source of new Zoom use cases and stories.

Zoom Help Center

Whether you're looking for technical documentation or a one minute quick start video, the Zoom Help Center has you covered with thousands of resources that are updated daily, so you can get your questions answered and keep Zooming.

Visit the Help Center

Live/Recorded Trainings

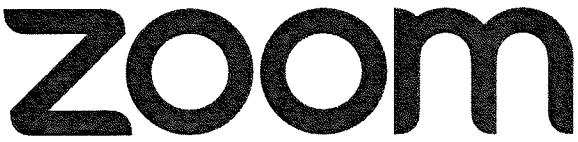
Our Zoom experts host free and interactive live training webinars daily. Get up to speed on important topics in less than an hour. Just select the time zone that fits best for you when registering for one of our live training webinars.

View Live Trainings & Recordings

Zoom Blog

Want to stay up-to-date on everything happening in the Zoom community? The Zoom blog offers daily stories on what's new at Zoom, exciting updates, and innovative customer stories and use cases to keep you inspired and on the cutting edge.

Visit the Zoom Blog


zoom

Resolve Your Dispute at JAMS via Videoconference or Conference Call

We offer a range of effective virtual options

Videoconferences and conference calls are tools that JAMS has long used to successfully resolve thousands of disputes of all kinds. JAMS mediators and arbitrators (neutrals) are adept at managing the resolution process whether they are conducting an in-person or virtual hearing. Additionally, JAMS neutrals and case managers receive ongoing training in the latest videoconferencing technology and best practices.

In addition to traditional conference calls, JAMS offers a range of videoconference options for mediations and arbitrations based on case size and complexity, client comfort level and cost considerations.

Zoom is a popular online platform that can be used for mediations and arbitrations of almost any size. JAMS provides the Zoom accounts, and there is no cost to the parties. It offers private breakout rooms for mediations. Zoom is self-administered and requires some preparation by participants, as detailed on the following page. JAMS neutrals and staff are available to assist you with this convenient and user-friendly tool.

Endispute,™ a proprietary JAMS mediation platform provided by CourtCall,® includes a high level of moderated service for a modest fee. A CourtCall representative will be available for the entire session to handle any technical aspects so that the parties can focus on settling their dispute. Endispute also allows private breakout rooms for each party and document sharing capability. This option is ideal for smaller, straightforward cases that can be resolved in a few hours. To determine if your case is appropriate for Endispute, contact a JAMS Case Manager or visit **jamsadr.com/endispute**.

How do I prepare for an online mediation or arbitration with JAMS?

- Determine which platform is best for your case *(see the following page for more information).*
- A JAMS Case Manager will provide you with the appropriate paperwork prior to your session. Parties will need to agree in advance on issues such as whether the session will be recorded and whether all participants must appear on camera.
- Just as you would with an in-person mediation or arbitration, confirm that all parties and representatives have blocked off time and are fully prepared to participate in the videoconference at any moment.
- Determine how you and your clients will communicate if you are participating from separate locations.
- Determine what documents you intend to share and ensure that they are forwarded to the neutral before the session.

Continued on the back

JAMS Online Mediation or Arbitration with Zoom

What are the technical requirements?

- Download Zoom to your computer or tablet in advance of your session at **https://zoom.us/**. Though less optimal, you may also participate via your smartphone.
- Confirm that:
  - your computer audio is enabled
  - you have a videocam on or attached to your computer
  - your internet connection is working
  - you have a suitable backdrop and good lighting
- Consider doing a test run, if possible, in advance of your scheduled conference in order to address any technical concerns.

How does the process work?

- You will receive an invitation to a Zoom videoconference. This will include both the link and the password.
- The JAMS neutral will be the host of the meeting.
- Depending on whether your videoconference involves a mediation or arbitration, the neutral may have you join parties in the main Zoom meeting room or go directly into a breakout session.
- The neutral may use the mute button at various stages during the process to eliminate background noise.
- If you are in the same location as your client, then you may also use the mute button (as appropriate) to have a sidebar conversation with your client.
- During mediation sessions, you may also have a conversation with your client – and with the mediator – in one of the breakout rooms. Conversations in that room will be limited to invitees only.

JAMS Endispute™ Online Mediation

What are the technical requirements?

- The Endispute online dispute resolution (ODR) platform is easily accessible, requiring only a phone and a computer or tablet with a webcam to participate in a mediation from anywhere.

How does the process work?

- Once you have determined that your case is appropriate for this platform, you can submit a case inquiry at **jamsadr.com/endispute**.
- An Endispute ODR case manager will then help parties select a neutral from the Endispute ODR panel and assist in the case convening process.
- Once the mediation session has been scheduled, confirmed participants will receive information about how to access the Endispute ODR mediation session, including dial-in instructions for audio as well as a link to access the video portion of the session.
- The parties will receive a fee agreement and confidentiality agreement which must be completed and returned in order to confirm the mediation session.

Disclaimer/Notice:

JAMS is providing parties with top-quality Alternative Dispute Resolution Services when in-person proceedings are not possible. Neutrals are available to conduct mediations, arbitrations and other matters via Zoom, Endispute, conference calls and any other platform agreed to by the parties.

Zoom has become a particularly popular platform for JAMS clients. While JAMS is not able to control Zoom security policies and procedures, JAMS neutrals and associates have been trained to make best use of the security protocols provided by the Zoom platform. Parties to matters at JAMS have reported good results using the Zoom platform because of its ease of use and the fact that it is cost-free to them.

For questions or concerns related to the security or privacy of any platform, please visit the website for that particular platform.

For more information, visit **jamsadr.com/online** or contact:

Western U.S. – Ed Cruz • ECruz@jamsadr.com • 415.774.2668
Eastern/Central U.S. – Shavonne Applewhite • SApplewhite@jamsadr.com • 212.607-2712

VIRTUAL ADR AND HIPAA COMPLIANCE

JAMS uses the Zoom HIPAA-compliant platform for all scheduled virtual proceedings, including mediations and arbitrations. This Zoom platform incorporates the necessary security features to satisfy the requirements of the Health Insurance Portability and Accountability Act (HIPAA).

Here are some ways that this Zoom platform ensures HIPAA compliance:

- Requires that all devices accessing the Zoom platform connect via strong encryption.
- Prevents recording of sessions from being saved to the Zoom cloud. Session recordings may only be saved to a local device. As such, personal information will not be saved to the cloud.
- Personal health information (PHI) or personal identifiable information (PII) will not be collected or reported. This includes personal identification numbers (e.g., driver's license numbers, social security numbers, passport numbers, etc.); medical records; and IP addresses, to name a few.
- The chat feature is secured with the strongest available encryption. This means that no message will be read by anyone outside of the meeting. Messages saved outside of the meeting will only be made available with explicit permission by all parties.

We all play a critical role in ensuring that virtual sessions are secure and satisfy HIPAA requirements. In order to maintain HIPAA compliance, parties must refrain from capturing any images or screen shots of the sessions, and sharing of information.

For specific information regarding Zoom's HIPAA compliant platform and its related security features, please go to https://zoom.us/docs/doc/Zoom-hipaa.pdf.

April 20, 2020

FREQUENTLY ASKED QUESTIONS – VIRTUAL ADR AND SECURITY

What steps is JAMS taking to protect security and privacy while using Zoom?

At every step of the proceeding JAMS employs processes to help protect security & privacy:

Step One – Invitations and Joining the Proceeding:

- JAMS provides a unique meeting ID for each mediation session and arbitration hearing.
- JAMS begins every proceeding by using the "waiting room feature." This feature ensures that only participants invited to the proceeding are granted access to the actual meeting.
- A JAMS moderator is assigned to every Zoom proceeding.
    - The moderator troubleshoots technical issues.
    - The moderator controls entry of the participants to the proceeding.
    - The moderator facilitates the use of break out rooms where needed or appropriate.

Step Two – The Proceeding:

- Once all participants have joined the session, the neutral and moderator have the ability to lock the meeting to prevent anyone else from joining.
- The neutral and moderator have the ability, and will, disable the recording function.
- The neutral and moderator will control the screen sharing function.

Step Three – Continuous Review and Training:

- JAMS provides ongoing training to neutrals and associates on best practices for virtual proceedings using Zoom.
- JAMS IT department monitors security developments regarding the use of virtual platforms such as Zoom and will update our processes as needed.

What alternative remote options are available for my case other than Zoom?

While JAMS is not able to control Zoom security policies and procedures and understands some clients have concerns with this platform, JAMS neutrals and associates have been trained to make the best use of the security protocols provided by the Zoom platform (see above). Parties to matters at JAMS have reported good results using the Zoom platform because of its ease of use and the fact that it is cost-free to them. However, should clients prefer another virtual option, JAMS has its own platform - Endispute™, operated by CourtCall™.

Endispute™ via CourtCall™

JAMS offers Endispute™, a mediation platform provided by CourtCall™, for a modest additional fee. Endispute™ is a browser-based video and audio application that is easily accessible through a phone, computer or tablet. A CourtCall™ representative is available for the entire session to resolve any technical aspects.

Endispute™ also allows private breakout rooms for each party and document sharing capability. Endispute™ application security is the strongest encryption standard. Only authenticated callers are let into the call and each meeting ID is unique.

Other Platforms

Should clients prefer another virtual platform, JAMS will work with the parties to accommodate the request. There are several alternative platforms available, including the following:

- Microsoft Teams (and Skype) - Users can host audio and video conferences with anyone. This platform provides features such as meeting note taking, screen sharing, meeting recording, and instant messaging.
    - A Microsoft Teams meeting can be locked by enabling the lobby setting and not allowing entrance into the meeting.
    - Appropriate for arbitrations or mediations based on available features.
- Conference Call (no video – please see below)
    - Appropriate for arbitrations or mediations.
- GoToMeeting™ –This platform includes features such as screen sharing, meeting recording, and instant messaging.
    - Provides each participant a password in order to enter the session.
    - The neutral has total control and can lock the room once the session begins to restrict others from accessing the videoconference.
    - Only appropriate for arbitration hearings based on available features.
- WebEx: This platform offers features such as screen sharing, meeting recording, and instant messaging.
    - Provides each participant a password in order to enter the session.
    - The neutral has total control and can lock the room once the session begins to restrict others from accessing the videoconference.
    - Only appropriate for arbitration hearings based on available features.

Audio Only

If the parties prefer not to use videoconference, JAMS can arrange for a mediation session telephonically through the use of LoopUp. This platform offers unique features by allowing participants to join the session with a click of a button, users can see who is speaking, and provides the host the capability to mute background noise.

JAMS has found that LoopUp is highly reliable and has had success with it thus far.

Can I resolve my case through virtual ADR proceedings if there are HIPAA compliance issues?

Yes. If a particular case or proceeding needs a HIPAA (Healthcare Insurance Portability and Accountability Act) compliant platform, please contact the local business manager and we can provide you with additional options and information.

What is JAMS reaction to the lawsuit(s) filed against Zoom related to security?

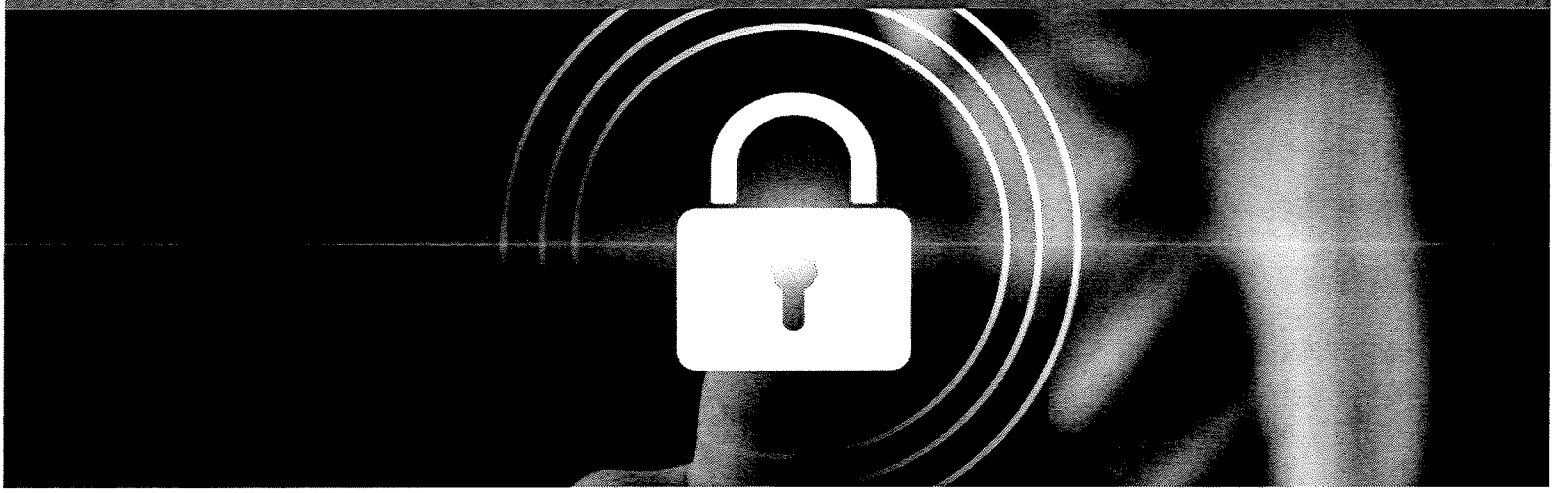
JAMS is continually reviewing updates and news related to various online platforms and making necessary adjustments to our procedures as needed. Through the JAMS Institute, JAMS offers industry leading, ongoing training to its neutrals and associates on the use of available security measures from each platform. JAMS is instructing its neutrals and associates to take full advantage of security features in order for proceedings to be protected.

With any virtual platform or electronic medium, security is an important factor. JAMS does not have an opinion on legal action by other parties, which is consistent with our position of neutrality. As with anything, there are no guarantees. If a client or party prefers any particular platform, JAMS will do its best to accommodate the request. Attorneys are encouraged to reach out to us directly to discuss their options.

zoom

Security Guide

Zoom Video Communications, Inc.



Zoom helps businesses and organizations bring their teams together in a frictionless environment to get more done. Our easy, reliable cloud platform for video, voice, content sharing, and chat runs across mobile devices, desktops, telephones, and room systems.

Zoom places security as the highest priority in the operations of its suite of products and services. Zoom strives to continually provide a robust set of security features and practices to meet the requirements of businesses for safe and secure collaboration.

The purpose of this document is to provide information on the security features and functions that are available with Zoom. The reader of this document is assumed to be familiar with Zoom functionalities related to meetings, webinars, chat, file sharing, and voice calling.

Unless otherwise noted, the security features in this document apply across the product suite of Zoom Meetings, Zoom Video Webinars, Zoom Rooms, and Zoom Voice, across supported mobile, tablet, desktop, laptop, and SIP/H.323 room system endpoints.

Infrastructure

The Zoom cloud is a proprietary global network that has been built from the ground up to provide quality communication experiences. Zoom operates in a scalable hybrid mode; web services providing such functions as meeting setup, user management, conference recordings, chat transcripts, and voice mail recordings are hosted in the cloud, while real time conference media is processed in globally distributed tier-1 colocation data centers with SSAE 16 SOC 2 Type 2 certifications.

Realtime Media Processing

A distributed network of low-latency multimedia software routers connects Zoom's communications infrastructure. With these multimedia routers, all session data originating from the host's device and arriving at the participants' devices is dynamically routed between endpoints. Zoom real-time sessions operate analogously to the popular mobile conversation over the public mobile network.

Firewall Compatibility

During session setup, the Zoom client connects via HTTPS (port 443/TLS) to Zoom servers to obtain information required for connecting to the applicable meeting or webinar, and to assess the current network environment such as the appropriate multimedia router to use, which ports are open and whether an SSL proxy is used. With this metadata, the Zoom client will determine the best method for real time communication, attempting to connect automatically using preferred udp and tcp ports 8801, 8802, and 8804. For increased compatibility and support of enterprise SSL proxies, connection can also be made via HTTPS (port 443/TLS). An HTTPS connection is also established for users connecting to a meeting via the Zoom web browser client.

Client Application

Role-based user security

The following pre-meeting security capabilities are available to the meeting host:

- Secure log-in using standard username and password or SAML single sign-on
- Start a secured meeting with password
- Schedule a secured meeting with password

Selective meeting invitation: The host can selectively invite participants via email, IM, or SMS. This provides greater control over the distribution of the meeting access information. The host can also create the meeting to only allow members from a certain domain email to join.

Meeting Details Security: Zoom retains event details pertaining to a session for billing and reporting purposes. The event details are stored at the Zoom secured database and are available to the customer account administrator for review on the customer portal page once they have securely logged-on.

Application security: Zoom can encrypt all presentation content at the application layer using the Advanced Encryption Standard (AES) 256-bit algorithm.

Zoom client group policy controls: Specifically applicable to the Zoom Meetings client for Windows and Zoom Rooms for Windows, administrators can define a broad set of client configuration settings that are enforced through Active Directory group policy controls.

Chat Encryption: Zoom chat encryption allows for a secured communication where only the intended recipient can read the secured message.

Meeting Security

Role-based user security

The following in-meeting security capabilities are available to the meeting host:

- Meetings are encrypted by default
- Waiting Room
- Enable wait for host to join
- Expel a participant or all participants
- End a meeting
- Lock a meeting
- Chat with a participant or all participants
- Mute/unmute a participant or all participants
- Screen share watermarks
- Audio signatures
- Enable/disable a participant or all participants to record
- Temporary pause screen-sharing when a new window is opened

The following in-meeting security capabilities are available to the meeting participants:

- Mute/unmute audio
- Turn on/off video
- Blur snapshot on iOS task switcher

Host and Client authenticated meeting: A host is required to authenticate (via https) to the Zoom site with their user credentials (ID and password) to start a meeting. The client authentication process uses a unique per-client, per-session token to confirm the identity of each participant attempting to join a meeting. Each session has a unique set of session parameters that are generated by Zoom. Each authenticated participant must have access to these session parameters in conjunction with the unique session token in order to successfully join the meeting.

Open or password protected meeting: The host can require the participants to enter a password before joining the meeting. This provides greater access control and prevents uninvited guests from joining a meeting.

Edit or delete meeting: The host can edit or delete an upcoming or previous meeting. This provides greater control over the availability of meetings.

Host controlled joining meeting: For greater control of meeting, the host can require participants to only join the meeting after the host has started it. For greater flexibility, the host can allow participants to join before the host. When joining before the host, participants are restricted to a 30-minute meeting.

In-meeting security: During the meeting, Zoom delivers real-time, rich-media content securely to each participant within a Zoom meeting. All content shared with the participants in a meeting is only a representation of the original data. This content is encoded and optimized for sharing using a secured implementation as follows:

- Is the only means possible to join a Zoom meeting
- Is entirely dependent upon connections established on a session-by-session basis
- Performs a proprietary process that encodes all shared data
- Can encrypt all screen sharing content using the AES 256 encryption standard
- Can encrypt the network connection to Zoom using 256-bit TLS encryption standard
- Provides a visual identification of every participant in the meeting

Host controlled joining meeting

Authentication methods include single sign-on (SSO) with SAML or OAuth.

With SSO, a user logs-in once and gains access to multiple applications without being prompted to log-in again at each of them. Zoom supports SAML 2.0 which enables web-based authentication and authorization including SSO. SAML 2.0 is an XML-based protocol that uses security tokens containing assertions to pass information about a user between a SAML authority (an identity provider) and a web service (such as Zoom). Zoom works with Exchange ADFS 2.0 as well as enterprise identity management such as Centrify, Fugen, Gluu, Okta, OneLogin, PingOne, Shibboleth, Symplified, and many others. Zoom can map attributes to provision a user to different group with feature controls.

OAuth-based provisioning works with Google or Facebook OAuth for instant provisioning. Zoom also offers an API call to pre-provision users from any database backend.

Additionally, your organization or university can add users to your account automatically with managed domains. Once your managed domain application is approved, all existing and new users with your email address domain will be added to your account.

Administrative Controls

The following security capabilities are available to the account administrator:

- Secure login options using standard username and password or SAML SSO
- Add user and admin to account
- Upgrade or downgrade user subscription level
- Delete user from account

- Review billing and reports
- Manage account dashboard and cloud recordings

Special Security Features/Options API

APIs are available for integrating Zoom with custom customer applications and third party applications. Each customer account may include API integration key credentials managed by the customer account admin. API calls are transmitted securely over secure web services and API authentication is required.

Meeting Connector

Zoom Meeting Connector is a hybrid cloud deployment method, which allows a customer to deploy a Zoom multimedia router (software) within the customer's internal network.

User and meeting metadata are managed in Zoom communications infrastructure, but the meeting itself is hosted in customer's internal network. All real-time meeting traffic including audio, video, and data sharing go through the company's internal network. This leverages your existing network security setup to protect your meeting traffic.

When customers choose a hybrid deployment, they have the option to segment by type of user where Pro and Free (Basic) user types will use the cloud, and Business and Enterprise user types will use the on-premise.

If on-premise is offline, the meeting will automatically revert to the cloud. Both our cloud and on-premise solutions are designed with failover and load balancing mechanisms when deployed.

Zoom Rooms

Zoom Rooms is Zoom's software-based conference room system. It features video and audio conferencing, wireless content sharing, and integrated calendaring running on off-the-shelf hardware. Communications are established using 256-bit TLS encryption and all shared content is encrypted using AES-256 encryption. The Zoom Rooms app is secured with App Lock Code. The App Lock Code for Zoom Rooms is a required 1-16 digit numeric lock code that is use to secure your Zoom Rooms application. This prevents unauthorized changes to your Zoom Rooms application and settings on your accompanying hardware.

Zoom Chat

Persistent, cross-platform chat is a feature of Zoom Meetings that enables users to chat and share files 1-1 or in groups. Users can click "Meet" from any chat to start an instant Zoom video meeting with the group participants. Chat can be encrypted for HIPAA-compliant settings.

Zoom Phone

Zoom Phone is a cloud phone system available as an add-on to Zoom's platform. Support for inbound and outbound calling through the public switched telephone network (PSTN) and seamlessly integrated telephony features enable customers to replace their existing PBX solution and consolidate all of their business communication and collaboration requirements into their favorite video platform.

Utilizing standards-based Voice-over-Internet-Protocol (VoIP) to deliver best in class voice services, Zoom Phone delivers a secure and reliable alternative to traditional on-premise PBX solutions. Call setup and in-call features are delivered via Session Initiation Protocol (SIP). While leveraging OPUS as the preferred codec to ensure the highest quality possible, Zoom Phone also supports additional industry standard codecs G.722, G.711, and G.729 for media transcoding.

Authentication

- Zoom Phone SIP registration authenticates using AES-128 bit TLS 1.2 encryption

Media Encryption

- VoIP media is transported and protected by Secure Real-time Transport Protocol (SRTP) with AES-128 encryption

Private Network Peering

- Zoom has established direct private network peering links between Zoom Phone data centers and Zoom Phone PSTN service provider networks to ensure maximum protection.

Emergency Calling

- Zoom Phone supports E911 (USA/CAN) enhanced emergency services to provide caller location to the local Public Safety Answering Point (PSAP) as required by law. Originating call location addresses can be defined and assigned at the account and individual user level.
- Emergency calls made from the Zoom mobile app on iOS and Android smartphones will automatically default to the mobile device's native outbound cellular calling feature and bypass the Zoom Phone service to directly route the emergency call to the mobile network operator's PSAP.
- Zoom Phone administrators may optionally choose to automatically intercept and reroute emergency calls to internal response teams.

Toll Fraud

- Zoom Phone prevents toll fraud through access control and automated detection capabilities. Our security department actively monitors customers' accounts to detect irregular calling patterns and will notify customers of potential fraudulent activities.

Calling Black Lists

- Customizable global and personal black lists allow users and administrators to easily add and manage blocked phone numbers

Invoking Elevate-to-Meeting feature

- When elevating a Zoom Phone call to a Zoom Meeting, all available Zoom Meeting security features will then apply to the interaction.

Zoom Video Webinars

In Zoom Video Webinars, up to 100 video panelists can present with video, audio, and screen sharing with up to 10,000 view-only attendees. These webinars feature registration options, reporting, Q/A, polling, raise hand, attention indicators, and MP4/M4A recording). Zoom Video Webinars can stream to YouTube and Facebook Live to reach an unlimited live audience. Panelists are full participants in the meeting. They can view and send video, screen share, annotate, and so forth. Panelist invitations are sent separately from the Webinar attendees. Webinar contents and screen sharing are secured using AES 256 and communicate over secured network using 256-bit encryption standard.

Registration Webinar

- Manually Approve Registration - The host of the Webinar will manually approve or decline whether a registrant receives the information to join the webinar.
- Automatically Approve Registrants - All registrants to the webinar will automatically receive information on how to join the webinar.

Registration-less Webinar

- One-Time - Attendees will join the webinar only once. After the webinar ends, attendees will not be able to use the same information to join the Webinar.
- Recurring - Attendees will be able to repeatedly join the same Webinar with the information provided.

Recording Storage

Zoom offers customers the ability to record and share their meetings, webinars, and Zoom Phone calls. Meetings and Webinar recordings can be stored on the host's local device with the local recording option or Meetings, Webinars, and Zoom Phone calls can be stored in Zoom's cloud with the Cloud Recording option (available to paying customers). Recordings stored locally on the host's device can be encrypted if desired using various free or commercially available tools.

Cloud Recordings are processed and stored in Zoom's cloud after the meeting has ended; these recordings can be password protected or available only to viewers logged in under a certain domain email. The recordings are stored in both video/audio format and audio only format. In-meeting chat messages, shared files and meeting transcripts can be optionally saved to Zoom's cloud, where they are stored encrypted as well. The meeting host can manage their recordings through the secured web interface. Recordings can be downloaded, shared, or deleted. Zoom Phone voicemail recordings are processed and stored in Zoom's cloud and can be managed through the secured Zoom client.

Zoom Rooms People Counting

Zoom Rooms people counting is a feature that is off by default, but can be turned on by room administrators. This feature allows administrators to view data around number of in-room meeting participants joined from Zoom Rooms.

This feature works by capturing images throughout the duration of the meeting. Images are temporarily stored on the Zoom Rooms local hard-drive and never sent to the cloud. Once the meeting ends, the locally-stored images are used to count the max number of visible in-room meeting participants. Throughout this process, face detection (without ties to personal information) is used to count individuals based on the images captured. Once the images are done being processed to capture the number of people, the images are permanently deleted.

By enabling the participant count feature for Zoom Rooms, you acknowledge your obligation to comply with all laws and that it is your responsibility to ensure that you provide adequate notice to users that this feature is enabled and have gathered appropriate consent from data subjects in compliance with applicable recording and/or privacy regulations for both the collection and storage of this data.

Privacy

Zoom only stores basic information under user account profile information:

- Email address
- User password - salted, hashed
- First name
- Last name
- Company name (optional to provide)
- Company phone number (optional to provide)
- Profile picture (optional to provide)

For more information about our privacy policy, visit https://zoom.us/privacy.

Billing Details

Zoom leverage a third-party, PCI-compliant partner to process payment and handle all aspects of billing. We do not store any user credit card information or billing information in our database.

Security and Privacy Certifications

SOC2:

The SOC 2 report provides third-party assurance that the design of Zoom, and our internal processes and controls, meet the strict audit requirements set forth by the American Institute of Certified Public Accountants (AICPA) standards for security, availability, confidentiality, and privacy. The SOC 2 report is the de facto assurance standard for cloud service providers.

TRUSTe:

TRUSTe has certified the privacy practices and statement for Zoom and also will act as dispute resolution provider for privacy complaints. Zoom is committed to respecting your privacy. If you have an unresolved privacy or data use concern that we have not addressed satisfactorily, please contact our U.S.-based third-party dispute resolution provider (free of charge) at https://feedback-form.truste.com/watchdog/request.

EU-US Privacy Shield:

Zoom participates in and has certified its compliance with the EU-U.S. Privacy Shield Framework. Zoom has committed to subjecting all personal data received from European Union (EU) member countries, in reliance on the Privacy Shield Framework, to the Framework's applicable principles. To learn more about the Privacy Shield Framework, visit the U.S. Department of Commerce's Privacy Shield List https://www.privacyshield.gov/list.

FedRAMP:

Zoom is authorized to operate under The Federal Risk and Authorization Management Program (FedRAMP), a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services used by federal agencies.

Enterprise businesses, healthcare organizations, and educational institutions around the world use the Zoom platform everyday to connect their teams, grow their organizations, and change the world. Zoom places privacy and security as the highest priority in the lifecycle operations of our communications infrastructure and meeting connector networks. In addition, we strive to continually provide a robust set of security features to achieve our goal of providing the most efficient and secure video first unified communications.

U.S. DISTRICT COURT FOR THE SOUTHERN DISTRICT OF NEW YORK MEDIATION OFFICE:

FINALIZING AGREEMENTS IN REMOTE MEDIATION

JULY 2020

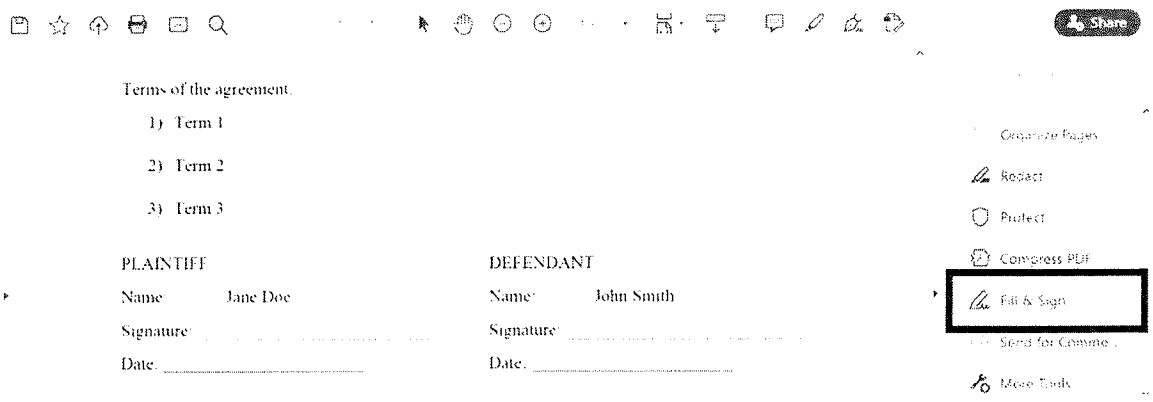
(Compiled by Sean McLaughlin, and credit for the Zoom screenshots goes to the Mitchell Hamline School of Law Mediation Clinic)

DECIDING THE METHOD: General Information

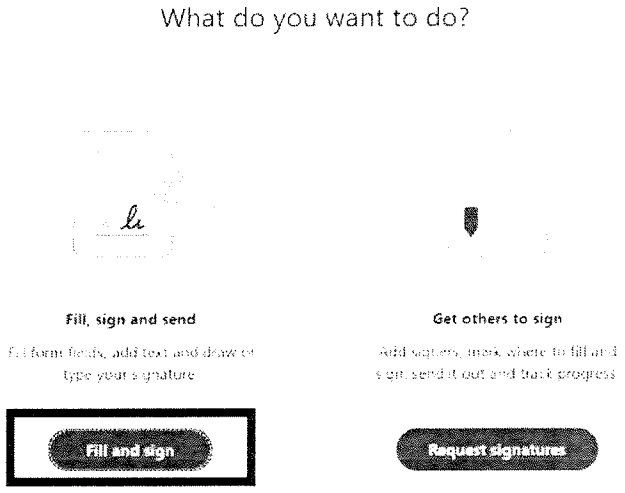
- There are several options for finalizing the terms of settlement at the end of a virtual (phone or video) mediation. The most common ways are through: (1) PDF, (2) screen sharing if you are using a videoconferencing platform with that feature, (3) Google Docs, or (4) an electronic document signing app, such as DocuSign or PandaDoc,
- The primary differences between the above options are security, accessibility, ease of use.
- Using a PDF is easy and accessible, but the method will not be encrypted as strongly as other methods discussed below. If you are comfortable with PDFs and email, this is the most efficient method, and is similar to what you may already practice when collecting signed confidentiality forms from your mediation participants.
- Using "Share Screen" in video conferencing application is as secure as those applications (e.g. Zoom or BlueJeans). For example, each Zoom meeting is password protected, and several security features such as Waiting Rooms, Locking Rooms, and Removing Participants all increase the security of Zoom. If you have basic experience with these applications, this method will be familiar.
- Google Docs is as secure as using Gmail. This means it is fairly secure by industry standards, but it still can be hacked and the encryption protections are not as strong as they are for applications such as DocuSign or PandaDoc. Also, sharing access to a Google Doc does open the document up to being shared to a wider array of people. The more people a Google Doc is shared with, the less secure it will be. However, the Google Docs interface makes it easy to use and fairly accessible. If you are comfortable with Google Docs, learning how to finalize agreements will not be challenging.
- Using an electronic signing app, such as DocuSign or PandaDoc, is the most secure method due to the high level of encryptions protecting each signed document. Such applications must be purchased and learned like any new computer application. (The SDNY does not currently provide training in these applications.)

FORMALIZING IN PDF WITHOUT A PAID ACCOUNT

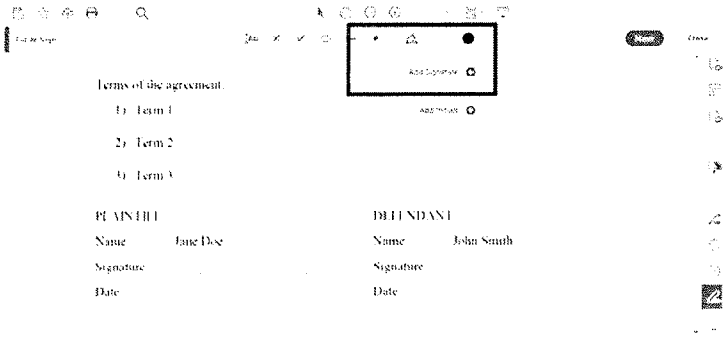
- To formalize in PDF you will not need a paid Adobe PDF subscription, however, the paid subscription will have more features, be more customizable, and have additional encryptions and protections.
- To formalize an agreement in PDF, the first step is to memorialize the terms and save them as a PDF. This can be done by converting a word document, or by adding text directly to a PDF agreement template.
- To sign a PDF document, start by clicking on "**Fill & Sign**" on the right-hand side of your PDF file.



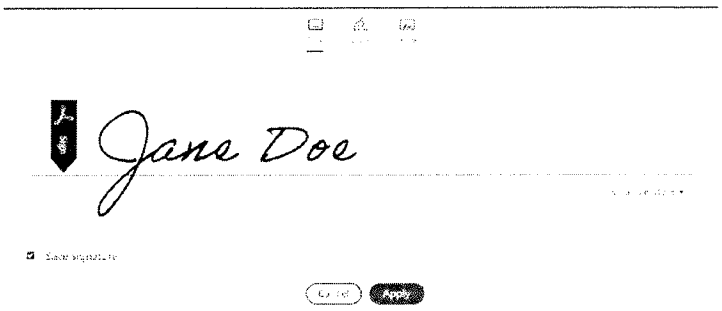
- Next, click "**Fill and sign**" on the left of the two options you are presented.



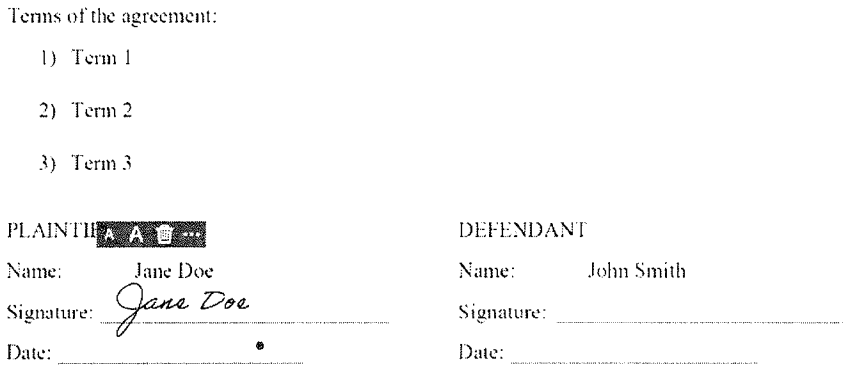
- Now, click the "**Sign**" option in the top center of your document, and scroll down and click the first option to "**Add Signature.**"



- The party signing will then type their name in the box provided and click "**Apply**."

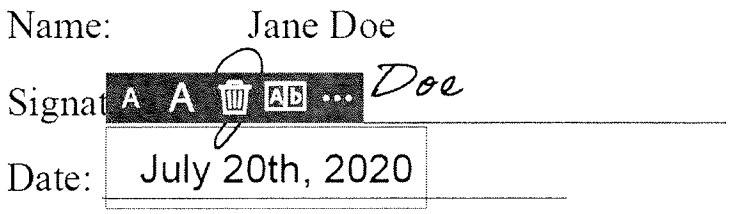


- A box with the signature will appear. You will need to drag the box with your signature over to where you need it to be. To drag the box, hover your cursor over the border line of the box and left click. Four pointing arrows will appear. Drag the box, then release your mouse, to place the signature where you want it.



- To add a date, click the "**IAB**" at the top left of your document.

- Now, left click on the location where you need to drop the textbox and type the date in. Finally, save the signed and dated document.



- The terms sheet may be **executed by counterpart**. This is similar to how the Confidentiality Form is typically signed in the Mediation Program, since the advent of remote mediation. Each party can sign their term sheet via PDF as shown above and

provide it to the mediator, or counsel, to combine and circulate.

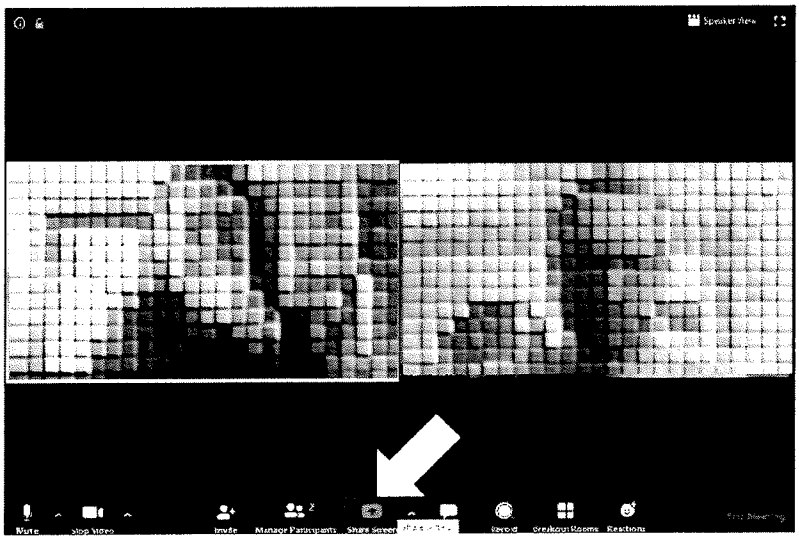
- A **round-robin** style sharing of the same term sheet for all parties to sign is an alternative method.

- The mediator should coordinate with the parties to determine which method all parties are most comfortable with.

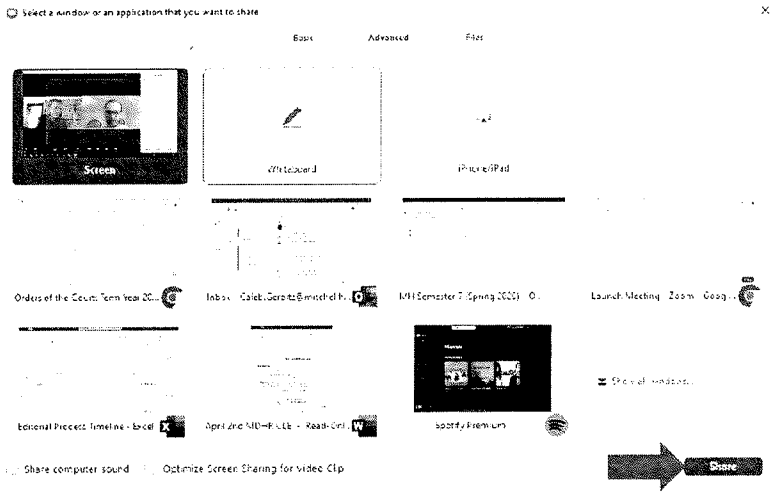
FORMALIZING THROUGH VIDEOCONFERENCE APPLICATION

- If all parties have agreed to terms, and those terms have been memorialized on a document (Word or PDF), you can use the screen share function to finalize the agreement. To finalize an agreement in this manner, you have to use a videoconferencing application that has screen sharing (two common ones are Zoom and BlueJeans). See details for Zoom below:

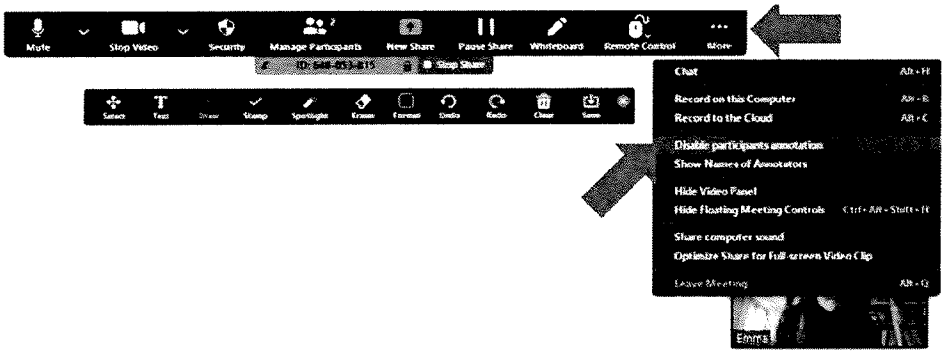
- First, open the term sheet document. To share your screen, click the "**Share Screen**" feature in the bottom center of your Zoom video conference interface. The box will be green.



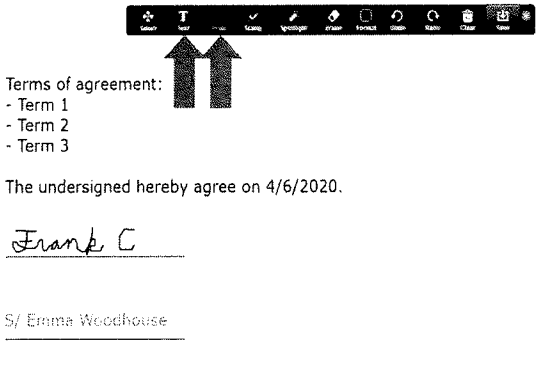
- When you click "**Share Screen**" you will see several boxes you can select to share which represent the different files you currently have open and available on your desktop. Select the correct file and click "**Share.**"

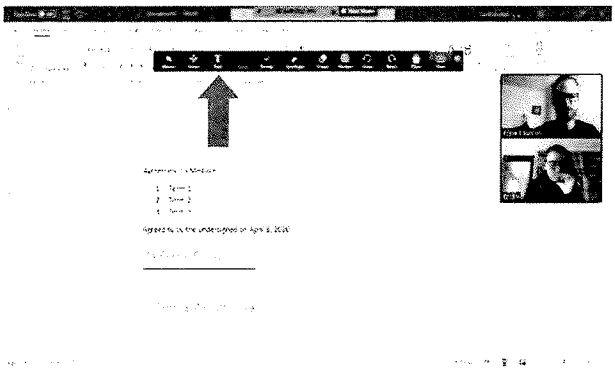


- Next, click "**More**" from the toolbar at the top and make sure the option to "**Disable participants annotation**" **is <u>not</u> checked (**if it is, you can uncheck it). You need participant annotation abilities *enabled* for all parties to sign. If the dropdown list says **disable** then it means the function is presently enabled.

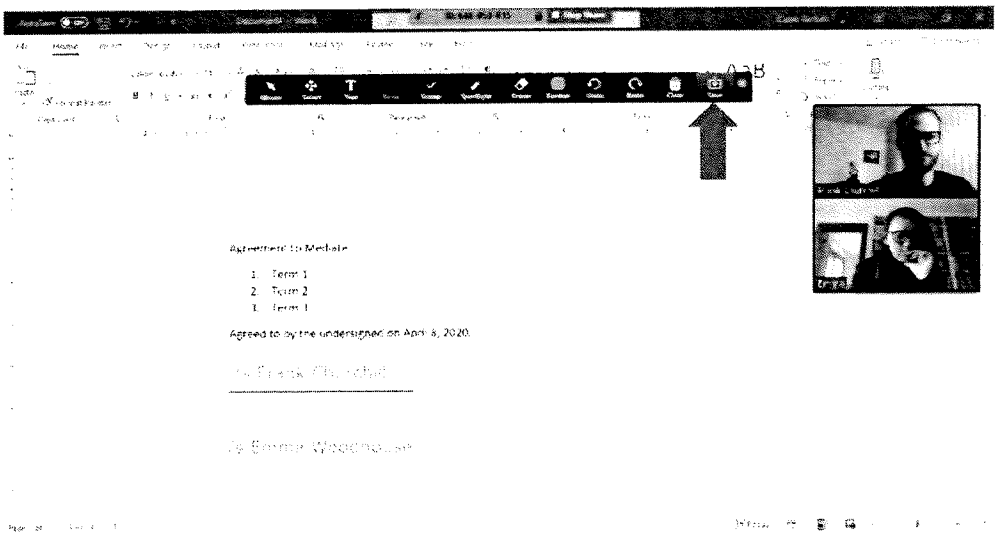


- Direct the participants to use either the text box or draw functions from the toolbar at the top to sign the document.





- Lastly, click the "**Save**" button at the top right of your share screen toolbar. Zoom will automatically create a "Zoom" folder in your "Documents" folder. The signed document will be saved there. You can email the signed, saved, document to all parties.

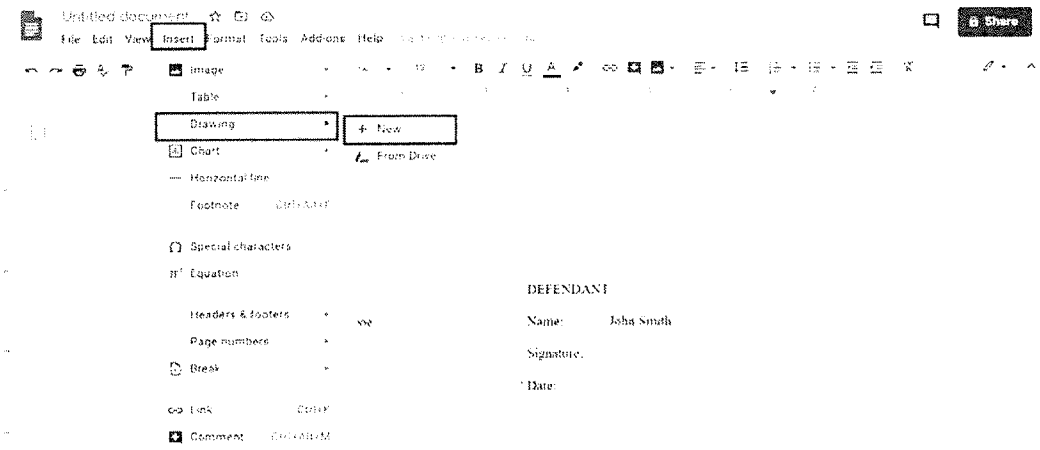


FORMALIZING IN GOOGLE DOCS

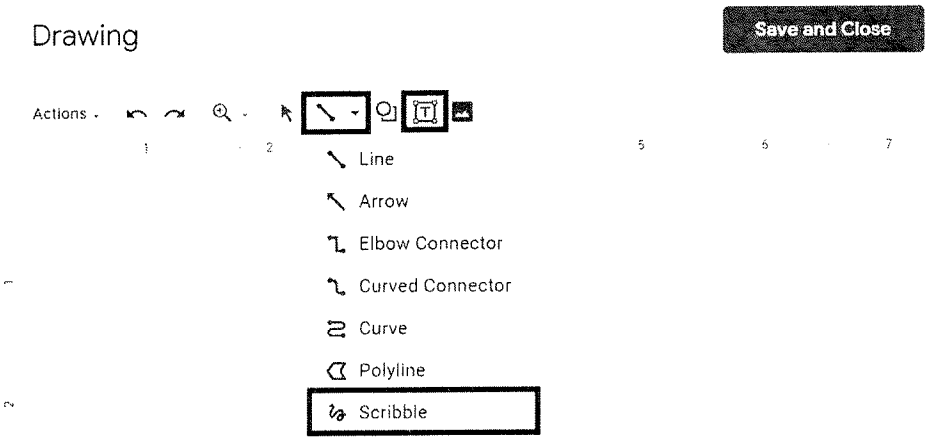
- A benefit of using Google Docs is that this application enables the mediator to have all parties sign the same document either simultaneously, or at different times. Since the Google Doc automatically updates live, a signature will populate immediately for all parties who have access to the Google Doc. The term sheet may also be executed in counterparts by having the mediator, or counsel, download the separately signed Google Docs, and combine and circulate.

- To access Google Docs, all you need is a Google Account, which you can set up for free with access to *any* email account. If you have Gmail, then you can access Google Docs from your Gmail. If you don't have Gmail, you can set up a Google Account at: https://accounts.google.com/signup/v2/webcreateaccount?hl=en&flowName=GlifWebSignIn&flowEntry=SignUp

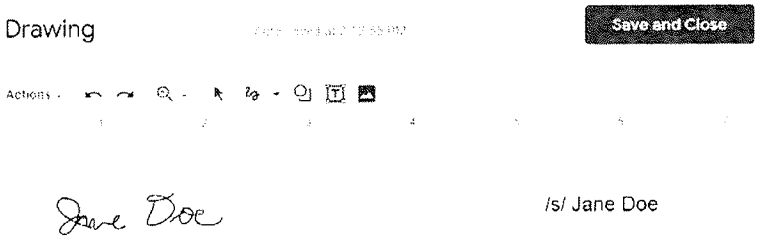
- To formalize an agreement in Google Docs, start by insuring the Google Doc is open in your browser. Next, go to the toolbar at the top and select **Insert → Drawing → New**. Click on **New**.



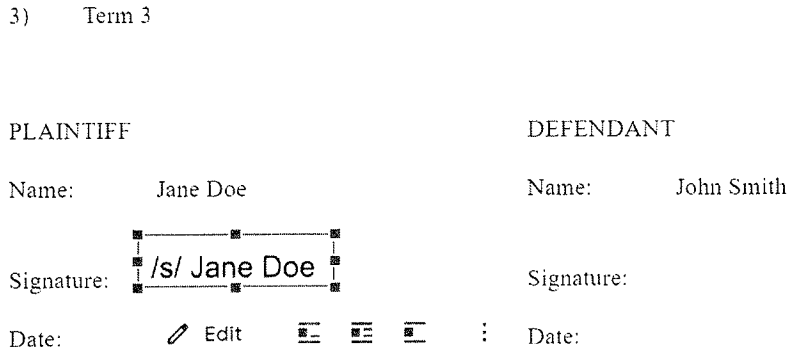
- Next, select *either* the **Line** icon and then **Scribble**, *or* select the **Text box** icon.



- The signature on the left represents using the **Scribble** function to sign, and the signature on the right represents using the **Text box** function to sign. Whichever is selected, once chosen, click "**Save and Close**" in the top right.



- The signature chosen will appear in a box, which you can click and drag to the proper location on the document. Use the **Text box** function to place the date. Google Doc automatically saves, so once complete you are free to share or download the signed document.

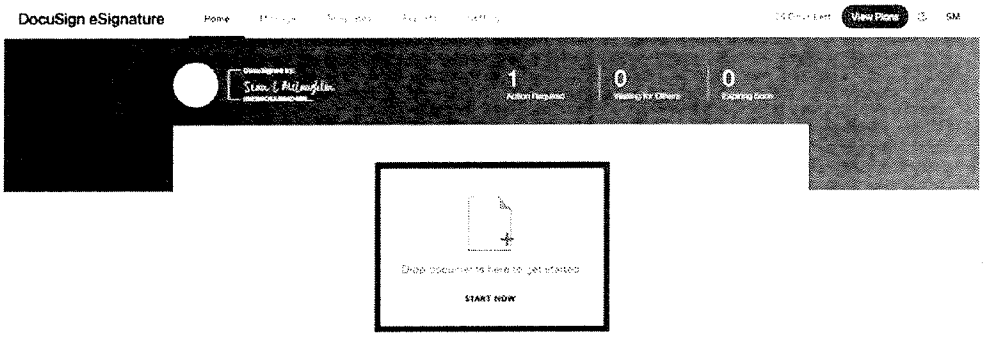


FORMALIZING IN DOCUSIGN

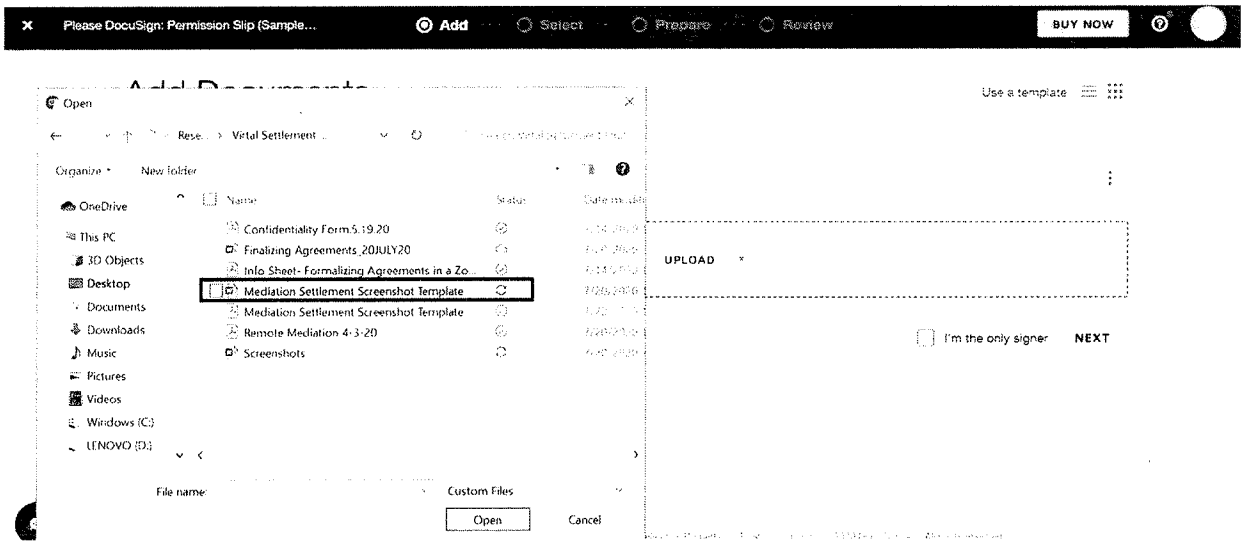
- A paid, encrypted electronic signing application such as DocuSign or PandaDoc is the most secure method of signing and transferring documents. Additionally, such applications typically have methods to streamline ease of signing and transferring documents between parties. The cost of such applications vary.

- DocuSign is the most secure platform. It works best when the terms of the settlement are already agreed to and written in a file that can be dropped into the DocuSign system for signing and emailing out to participants.

- To start, login to your DocuSign account. On the home page you will see an option in the center of your page to "**Start Now.**" Click it to upload the term sheet.



- Next, you will be brought to a screen where you can drag the file containing the terms of the settlement or click "**Upload**" and browse your desktop for the relevant document.

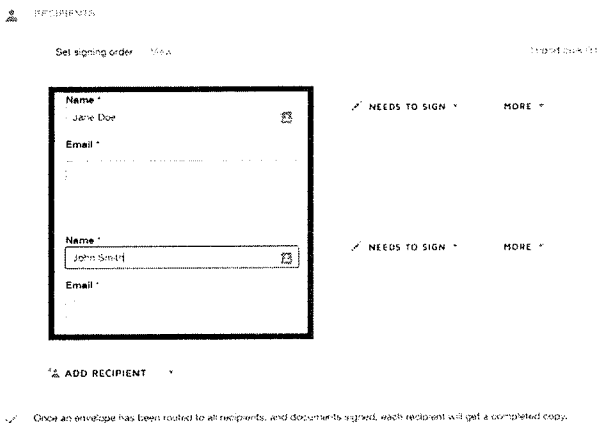


- When the file has uploaded, click "**Next**" in the bottom right of the screen.

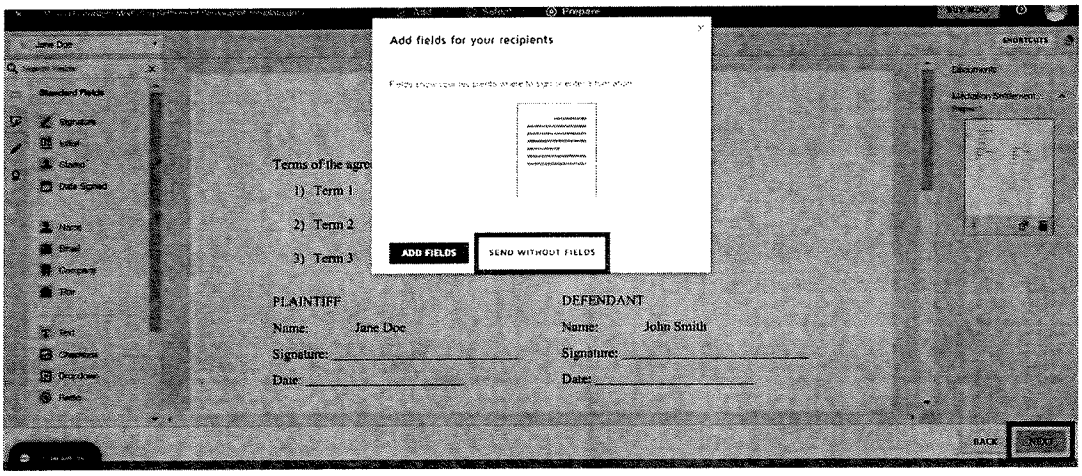
- There are some important considerations when adding recipients. Who you add as a recipient could include the parties, everyone including the mediator, or could be *only* the mediator depending on if you are executing by counterpart or by round-robin.

- The convenience of DocuSign is largely through using the round-robin method of signing a term sheet. If all parties are comfortable with this, DocuSign has a secure and fairly convenient way to transfer signed documents between all parties as indicated above.

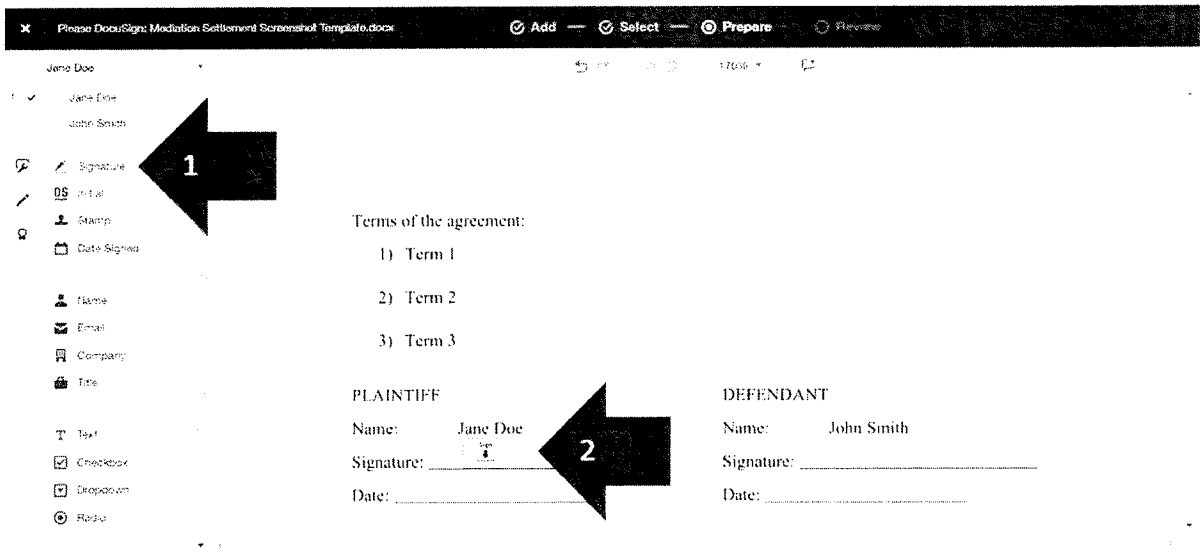
- Now, insert the name and email of each recipient as seen in the screenshot below. Once inserted, click "**Next**" at the bottom right of your screen.



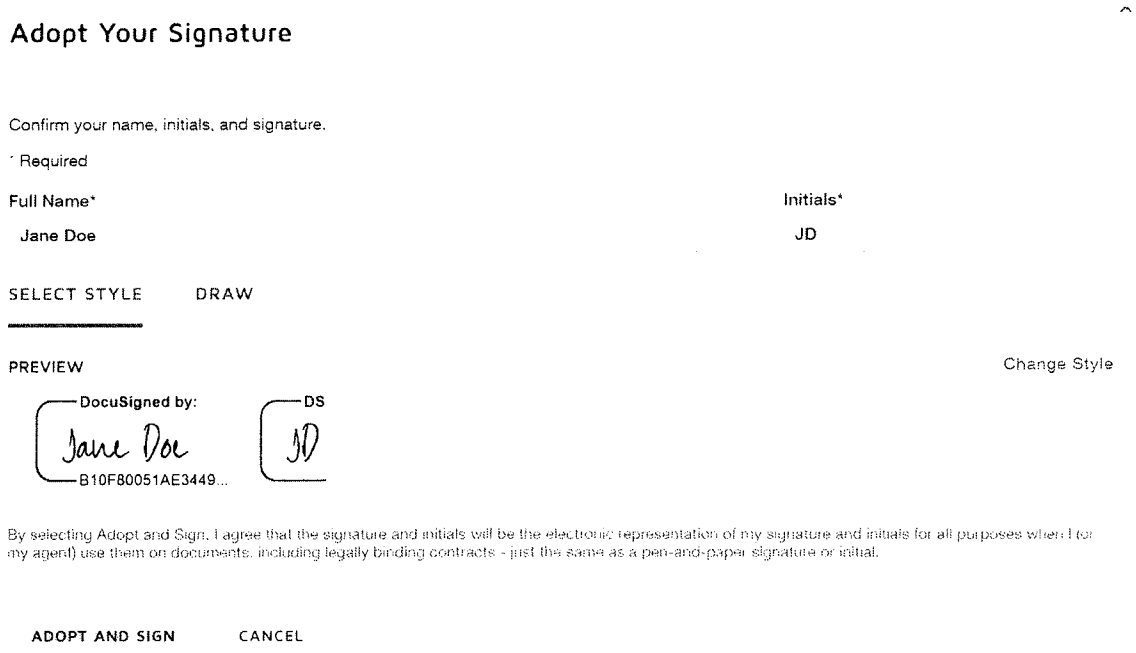
- The next screen will show the document you uploaded and will have lots of options. Click **Next → Send without fields**. This will email the attached document to the email addresses you provided in the previous section. All participants required to sign will then receive an email from DocuSign with the terms of the settlement attached along with a request to sign.



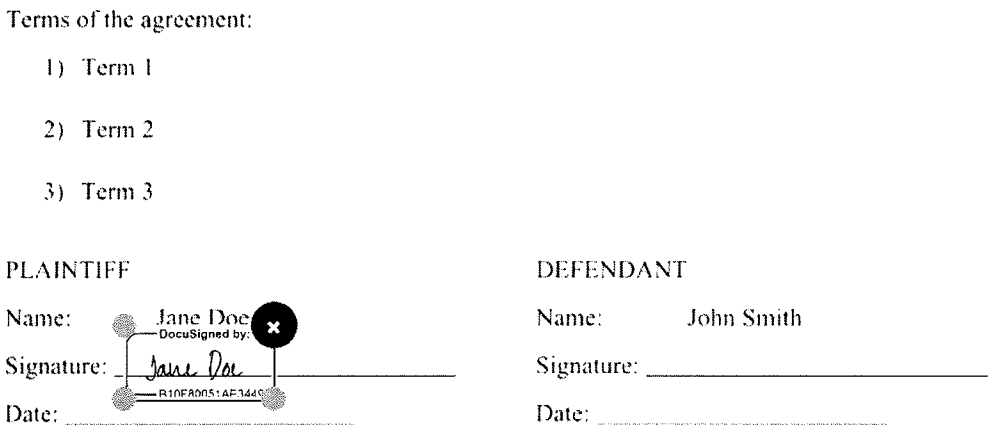
- When a participant clicks the link in the email, she will be prompted to "**Review the Document**." Clicking the link will take her to the document in DocuSign. To sign, she will first click "**Signature**" on the top left-hand side of her screen. Next, she will drag the **signature box** over to the proper place in the document to sign.



- Once she drops her signature box in the appropriate area, she will be prompted by the screen below to confirm her signature and initials before adopting and signing the document.



- Once she clicks "**Adopt and Sign**," the document will be formally signed by her. Next, she will hit the "**Finish**" box at the top right of her screen. This will prompt a version of her signed document to be sent out to the remaining participants, who will then need to sign the document in the same manner as she did. You will get prompts from the DocuSign Chatbot in your Zoom application every time someone signs.



USING DOCUSIGN THROUGH ZOOM

- If you use Zoom, another pathway to DocuSign is to use it as an application attached to your Zoom account.

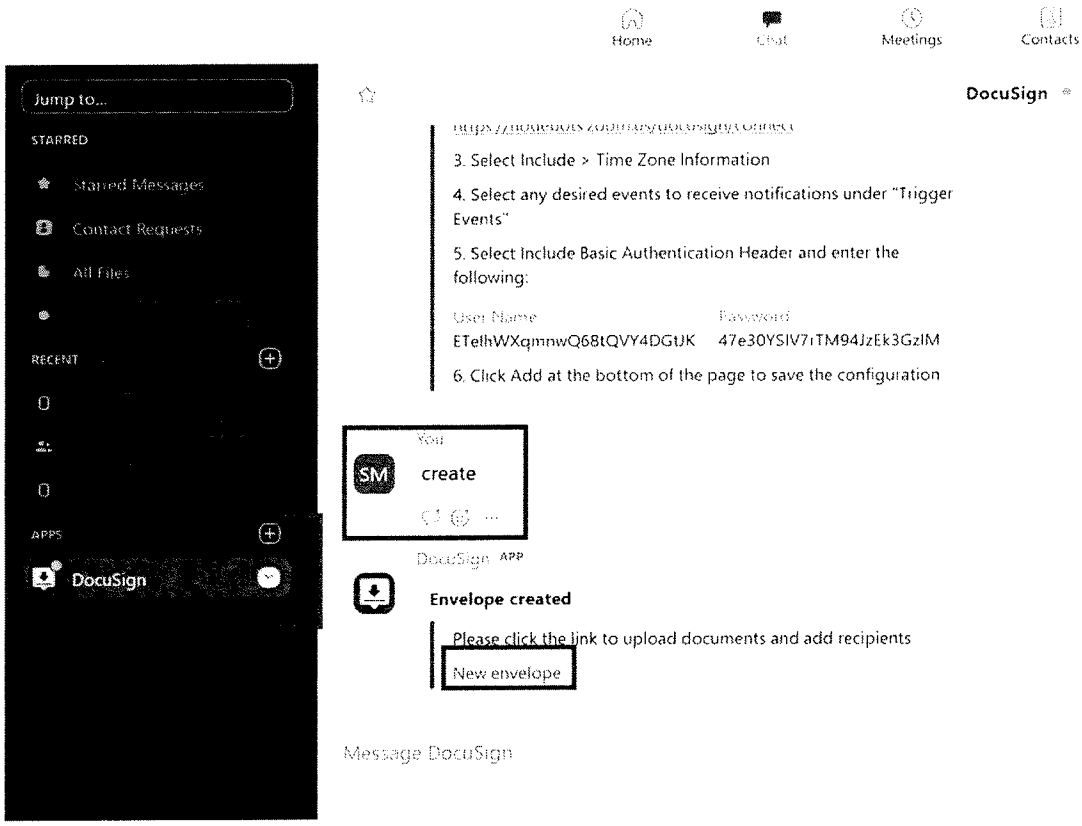
- To use DocuSign for secure electronic signatures as an application connected to your Zoom account, start by following the instructions in the link below to connect both

accounts: https://marketplace.zoom.us/apps/tg7aLkNsS1-7SJTbwjpu-Q

- *Integrating your DocuSign account with your Zoom account is not complicated, but there are many steps. Follow the video link above step-by-step to ensure you properly connect your two accounts.*

- Specifically, the tutorial above will show step-by-step how to access DocuSign from the Zoom Marketplace, download DocuSign, integrate and connect via the DocuSign Chatbot with your Zoom application, and then configure your personal settings in DocuSign to enable the creation, signing, and sending of encrypted documents.

- Once you have connected your DocuSign account with your Zoom account, go to **DocuSign** → type "**create**" in the Message Box → click the "**New envelope**" hyperlink that DocuSign created. This will take you into your DocuSign account where you can upload the document that contains the terms of the settlement.



AMERICAN BANKRUPTCY INSTITUTE
JOURNAL
The Essential Resource for Today's Busy Insolvency Professional

Mediation Matters

BY LESLIE A. BERKOFF AND HON. LOUIS H. KORNREICH

Taking Mediation Online: The Practicalities and the Pitfalls

Coordinating Editor Leslie A. Berkoff
Moritt Hock & Hamroff LLP; New York

Hon. Louis H. Kornreich
Bernstein, Shur, Sawyer & Nelson PA Portland, Maine

Leslie Berkoff is a partner with Moritt Hock & Hamroff LLP in New York and is co-chair of ABI's Mediation Committee. Hon. Louis Kornreich, a former bankruptcy judge, is Of Counsel at Bernstein, Shur, Sawyer & Nelson PA in Portland, Maine, and is co-chair of the Special Projects Subcommittee of ABI's Mediation Committee.

Editor's Note: *ABI recently launched its Coronavirus Resources for Bankruptcy Professionals website (abi.org/covid19), which aggregates information for bankruptcy professionals to assist clients and provide guidance due to the fallout from the COVID-19 pandemic.*

Bankruptcy lawyers and mediators agree that mediation should take place in person with all decision-makers physically present. When faced with exceptional circumstances, however, many of us have participated in telephonic or video mediations. The universal social distancing precautions adopted in response to the COVID-19 pandemic present us with a new and extraordinary circumstance justifying remote mediations.[1]

Learning to adapt and utilize remote mediation is necessary if bankruptcy lawyers and mediators are to serve those who have engaged them to resolve disputes. Doing so will enable lawyers and mediators to meet the explosion in bankruptcy cases that is likely to occur in the aftermath of the current health crisis when bankruptcy courts are likely to be overwhelmed. Traditional face-to-face mediations and in-court proceedings will resume at some point, but courts and lawyers will be looking for ways to move many new cases forward in an efficient, cost-effective manner.

Lawyers and mediators who have acquired remote mediation expertise will be well positioned to meet this new challenge. In addition, the normalization of remote mediation will expand the reach of skilled mediators to the entire country and beyond. It may also expand the mutual referral base of mediators when conflicts of interest arise and additional or new assistance is required.

Much has already been written on the general subject of remote mediation. The purpose of this article is to convince the bankruptcy community that remote mediation is a particularly good tool to use in bankruptcy practice. Let's begin with the obvious: Remote mediation is not as good as face-to-face mediation, which enables participants to have eye contact, read body language and assess the positions of adversaries based on their deportment. It is hard to refute these well-known attributes of in-person mediation. The purpose of this article is to convince readers that when in-person mediation is impossible or impractical, remote mediation is an appropriate and effective way to resolve bankruptcy disputes and should not be dismissed out of hand.

While there are some articles that discount the usefulness of remote mediation,[2] other articles explain how remote mediation can be effective.[3] Most of the criticism of remote mediation comes from outside of the bankruptcy context, where timing is not as critical. However, in bankruptcy, time is a luxury that many debtors and creditors do not have. Accordingly, remote mediation might be a more appealing option to resolve time-sensitive bankruptcy disputes.

Bankruptcy professionals are "can-do" types who know how to improvise. Bankruptcy lawyers rarely have an opportunity to sit back and wait until the time is right to participate in an in-person mediation. They know the pressures of the case, and the strictures of the Bankruptcy Code and Rules often prevent a delay of any kind. Their "must-do-now" mindset should be applied to mediation.

1 The authors do not intend to offer technical advice or provide a "go-to" program for running mediations online. There are many resources available for training in Zoom and other remote modalities. Readers should turn to the many other resources available on this topic.

2 *See, e.g.*, Jeff Kichaven, "The Era of Video Mediation Is Here — Or Is It?," *Law360*, April 6, 2020.

3 *See, e.g.*, Michael Willemin, "In Defense of Virtual Mediation," *Law360*, April 13, 2020.

A bankruptcy mediator can make remote mediation effective if lawyers and their clients are committed to the process and remove barriers to working in a new format. Bankruptcy courts have paved the way, as telephonic hearings have been in use for a number of years and video hearings are now occurring with regularity. Applying technology to mediation is a step in the same direction,[4] and training mediators and the bar will be another key to its success.

Things to Consider

There are many important considerations that will improve the effectiveness of remote mediation. First, it is important for a mediator who is conducting a remote mediation to be both capable and comfortable with the technology they use. Just as mediators are trained in the art of conducting in-person sessions, they must be similarly trained to conduct mediations online.

Further, in the present environment, the mediator must take the lead in preparing participants — both the lawyers and the parties — in the workings of a remote session. Everyone must be comfortable with the concept and technology for remote mediation. The mediator should provide participants with training provided by the system vendor, then set up a practice session to ensure that everyone is comfortable with the technology.

Just as a mediator would ensure that every participant is comfortable and knows where the amenities are located in real conference rooms for an in-person mediation, every participant should be made aware of how to use the mute button or request, set up and participate in a private caucus for a remote mediation. Preparing participants in this way is part of a mediator's trust-building role. It is also the best way to avoid frustrating and devastating mistakes.

Second, the mediator needs to ensure that all participants are comfortable with the confidentiality of the online process. It is easier to assess confidentiality when the participants are sitting in a private conference space where it is obvious that what is said is heard only by those who are in the room. This is more difficult to do online. Moreover, most remote platforms have recording features, which must be disabled. The mediator and lawyers must carefully review the confidentiality expectations of all the participants and stress the importance of maintaining the confidentiality of the process. Adding passwords that are exchanged solely with the participants will build confidence in the process. Further, in advance of the mediation, the mediator and lawyers must stress that each participant should be in a private space where they cannot be overheard. The parties should not be on public Wi-Fi and should be in an area with good connectivity to avoid disruptions.

Third, security precautions should be taken with a remote vendor, and every participant should be made aware of these precautions. By adding dual passwords, locking the session once all participants have joined and implementing some of the other recommended precautions, remote mediation will be as secure as the technology allows.

Fourth, the parties should agree upon a contingency plan in case the technology fails to work, such as having technicians on standby.

Fifth, the mediation agreement should be re-crafted to incorporate all the above concerns and any special concerns of the participants. It should be read and signed by the mediator and every participant.

Benefits and Concerns

There are several benefits to remote mediation. One of the primary benefits is cost savings. Without the need to travel, expenses will be reduced, and participants will have more flexibility in scheduling. Setting up remote mediations might also be less intrusive for participants and easier to calendar around work and family obligations. Of course, all of this comes with an inclination toward informality. Thus, it will be necessary to remind participants to treat remote mediation with the same seriousness as in-person mediation. Those participating must avoid falling prey to the distractions of other activities and multi-tasking. A remote mediation must occur as if it were being conducted in a live setting.

There are other benefits, such as utilizing technology to share documents electronically. Most online programs such as WebEx provide for document-sharing, which is easier than printing and making copies of documents. Indeed, utilizing technology, parties can literally be focused on the same place on a page of a document. There are some risks to sharing documents online, however, such as losing some level of control as to where the documents are sent and who may have access to them. However, most mediation agreements and orders contain provisions requiring the parties to agree to strict confidentiality. It should be made clear that anyone attempting to record the mediation, send an improper email or misuse a confidential document will be subject to sanctions, and that the loss of credibility from such abuses would not be worth whatever benefit might be gained.

Perhaps the greatest drawback to keep in mind is that not everyone is comfortable with or trusts technology. While today's world is becoming more technologically driven and recent events have perhaps accelerated that trend, not everyone has access to the same technology or even the ability to participate from an area with a stable broadband connection. Of course, this goes back to the initial step of ensuring that every participant is familiar and comfortable with the process ahead of time. Asking participants to certify that they are comfortable with the process as a condition of going forward should be part of a pre-mediation checklist, and advocates should ensure that their clients are comfortable even before the practice sessions with the mediator.

Mediation always depends on the parties having trust in the mediator and the process. Therefore, it is up to the mediator to properly set the stage by establishing trust in the mediator, the technology and the process of remote mediation.

Conclusion

While we all hope that things will return to normal soon so that professionals may resume face-to-face

4 The authors do not know whether Winston Churchill, a master of in-person disputation, would have accepted remote mediation as a means of dispute resolution. However, he astonishingly predicted the use of video conferencing in a 1931 article that appeared in *Macleans Magazine* entitled, "Fifty Years Hence." Andrew Roberts, *Churchill: Walking with Destiny* 357 (2018).

mediation, one byproduct of this pandemic will be the normalization of remote mediation for use in appropriate circumstances. Lawyers and mediators who become skilled in the art of remote mediation will better understand when it will work best, even after the world rights itself. abi

Reprinted with permission from the ABI Journal, Vol. XXXIX, No. 6, June 2020.

ABA AMERICAN BAR ASSOCIATION (/) blt
Business Law Section

Business Litigation & Dispute Resolution (Https://Businesslawtoday.Org/Practice-Area/Business-Litigation-Dispute-Resolution/)

Taking Your Mediation Practice Online in the Face of COVID-19

4 Min Read

By: Leslie Ann Berkoff (/author/leslie-berkoff/) | Yesterday

Having served as a mediator for twenty-plus years, I am generally a proponent of having the mediation take place in person, with all decision makers physically present. I have always believed it was important to be able to see people during the mediation in order to secure trust and develop rapport, and also to read and evaluate micro-expressions during the process. Humans by nature connect and evaluate one another in various ways, including through eye contact and body language, both of which are visual cues, as opposed to voice inflection, which can, of course, be detected over the phone. Yet, from time to time, I have conducted mediations by telephone, although I have tried to limit those to instances where the issues were discrete enough that telephonic shuttle diplomacy would still get the job done. However, in the face of COVID-19, at a time when so many courts are not even allowing in-person hearings or any hearings at all, finding a way to conduct online mediations becomes essential for many to continue their business.

Many practitioners are turning to existing tools, such as WebEx and Zoom. These programs still satisfy that "in-person" touch that so many mediators and participants desire because they allow the parties to hear and see each other via webcams, and they also allow for separate sessions to be created, thereby mimicking joint and private caucuses. While these are great options, there are a few considerations that users should keep in mind. First, no matter which platform you choose, you must be facile with the program and have the ability to not only use it yourself, but also be able to guide the participants who may not be as familiar with the platform so that they are equally comfortable. To that end, aside from taking the many training sessions that are popping up, be sure to practice the use of the technology yourself. There is nothing more frustrating to a mediation advocate or participant than technology that impedes rather than enhances the mediation process. Thereafter, I would recommend that you set up a time before the actual mediation to virtually "meet" with each side, including clients, to be sure they are equally comfortable with the technology. Just as you would ensure that participants are comfortable in your conference room and understand where the amenities are located, they need to be sure they know how to use the mute button, or discretely request, set up and/or participate in a private caucus session. Second, as the mediator you need to ensure that all parties are comfortable with the confidentiality of the online process. It is easy to gauge confidentiality when you are sitting in a private conference space and can determine that what is being said is only being heard by the actual participants who are present in that room. With online programs, there is a limited view of where the other participants are physically sitting. Moreover, all of the platforms have recording features, which you should ensure are turned off and you should request that all participants do the same. You should review and identify the confidentiality expectations with all the participants and stress the importance of maintaining confidentiality of the process; whatever presentation you normally give for confidentiality should be modified for this new format. Further, you should stress, in advance, that the parties themselves should be in a private space where they cannot be overheard. The parties should not be on public WiFi and should be in an area with good connectivity to

avoid disruptions to the process. Third, you need a contingency plan in case the technology does not work and/or the participants, despite prior testing, cannot get it to work.

Mediation is always dependent upon the parties having trust in the mediator and the process. It is important to keep in mind that not everyone is comfortable with or trusts technology. Therefore, in order for the process to work while utilizing these alternative methodologies, it is up to you as the mediator to do your part to properly set the stage, and establish the trust in you, the technology method, and the process. Any good mediator spends time setting the stage in advance by reading position statements and speaking to the parties in advance; now mediators should add a review of the technology to ensure that the parties are comfortable as one more step to achieving a successful process. How you build that extra time into your fee structure must be decided by each of you, but presently, my thought is not to charge for X hours of technological preparation.

ABOUT THE AUTHOR

(/author/leslie-berkoff/)

Garden City, NY

Leslie Ann Berkoff

(/author/leslie-berkoff/)

Chair of Moritt Hock & Hamroff's Dispute Resolution Practice Group. A skilled mediator having handled mediations in bankruptcy courts for all

phases of bankruptcy-related litigation, as well...

+ Follow

MORE FROM THIS AUTHOR

(https://businesslawtoda
adr-clauses-financial-ma-joint-venture-disputes/)

17 Min Read
Business Litigation & Dispute Resolution

July 11, 2019

Drafting ADR Clauses for Financial, M&A, and Joint Venture Disputes

(https://businesslawtoday.org/2019/07/drafting-adr-clauses-financial-ma-joint-venture-disputes/)

By: Leslie Ann Berkoff, Andrew Barton, Serena K. Lee, Peter R. Day, Susan Tomaine

Many enterprises and lawyers that handle financial, M&A, and joint venture transactions are now turning...

Read More

(https://businesslawtoda
otherwise-final-award-exception-functus-officio-doctrine/)

3 Min Read
Business Litigation & Dispute Resolution

June 7, 2019

Clarifying an Otherwise Final Award: An Exception to the Functus Officio Doctrine

(https://businesslawtoday.org/2019/06/clarifying-otherwise-final-award-exception-functus-officio-doctrine/)

By: Leslie Ann Berkoff

Functus Officio is a Latin term meaning that once the purpose of the task at hand is completed, there...

Read More

(https://businesslawtoda
court-decides-applicability-section-1-federal-arbitration-act/)

12 Min Read
Business Litigation & Dispute Resolution

February 12, 2019

Supreme Court Decides on Applicability of Section 1 of the Federal Arbitration Act

(https://businesslawtoday.org/2019/02/supreme-court-decides-applicability-section-1-federal-arbitration-act/)

By: Leslie Ann Berkoff

Summary Background In a term that seems to be touching upon the Federal Arbitration Act (the FAA) with...

Read More

(https://businesslawtoda
continues-hot-topic-supreme-court/)

6 Min Read
Business Litigation & Dispute Resolution

December 18, 2018

Arbitration Continues to Be a Hot Topic Before the Supreme Court

(https://businesslawtoday.
continues-hot-topic-supreme-court/)

By: Leslie Ann Berkoff

Interpretation of the Federal Arbitration Act (FAA) has been a frequent issue considered by the U.S....

Read More

By Leslie A. Berkoff

The Continuing Value of the Joint Session in Mediation

Coordinating Editor
Leslie A. Berkoff
Moritt Hock & Hamroff LLP; New York

Leslie Berkoff is a partner with Moritt Hock & Hamroff LLP in New York and serves as co-chair of the firm's Litigation and Bankruptcy Practice Group. She also serves as a mediator and is on the Mediation Panels for the Eastern, Southern and Northern Districts of the U.S. Bankruptcy Courts in Delaware and the Eastern District of Pennsylvania, as well as the Commercial Mediation Panel for Nassau County.

Traditionally, the joint session has been the foundation of the mediation process. In biblical times, sparring community members often resolved conflicts by gathering together in an open forum alongside other community members to discuss and resolve disputes in a collaborative fashion. In more modern times, the joint session has built upon this foundation to serve additional purposes, such as allowing the mediator to set the tone for and explain the mediation process to participants. In addition, the joint session provides an opportunity for the mediator to lay out the protocols for the mediation session, such as confidentiality regarding the information being exchanged and how the caucuses will work. Most importantly, the joint session allows the parties a chance to communicate directly with one another.

In that regard, it is important to remember that the origins of mediation are rooted in joint sessions rather than separate caucuses. Further, mediation was not dependent on party representation through counsel. Over time, perhaps starting in the 1990s, the mediation process morphed and the line between mediation and litigation blurred. Mediation participants began introducing litigation-based issues and demands into the mediation process at the expense of focusing on a more traditional exchange of thoughts, concerns, proposals and needs. That trend tracked with the increased number of parties retaining counsel to represent them in mediations — lawyers who were almost always litigators.

As a result, the dynamic of the joint session has been threatened. Some counsel view the opportunity as a quasi-litigation forum to posture and argue — even pounding the table to demonstrate the righteousness of client positions while the clients remain mute and entrenched in their positions. When a session is used in such a way, the mediator (who has no authority to make rulings on arguments) risks morphing into a referee in an effort to maintain some control over the process. When viewed as an opportunity for advocacy, mediation loses its essential client-driven nature with the potential for parties to speak and contribute to a creative and collaborative end result. In such settings, mediation is nothing more than a precursor to litigation or a stop along the path to the courthouse.

In recent years, some advocates have requested — and some mediators have decided — to dispense with the use of the joint session universally across the board. For some, the fear grew that allowing lawyers to use the joint session as a courtroom podium simply did not advance the mediation process and caused more harm than good.

Others who are more cynical believe that there is a more calculated purpose to seeking to dispense with the joint session: a belief that the desire comes from the individual parties thinking they can slant the facts and the mediator's focus more easily if they are in separate caucus rather than having the other side hear their view of the world and refute it directly.

Some experienced mediators believe that a more troubling basis might exist for the threat to the joint session. Specifically, in order for a joint session to be truly effective and impactful, the lawyers must prepare themselves and their clients. In order for that to be fruitful, time and effort must be expended. Lawyers and clients might not want to commit time and resources to preparing for the mediation, and this lack of preparation may result from a lack of faith in the ability of the process to work. Mediation can and does work for parties when the right mediator has the full participation and commitment of the parties. Cynics suggest one other possible reason for the threat to the joint session: the self-interest of lawyers who might be incentivized to keep the hourly clock running, although one would hate to think that this is true.

Now, in fairness, there can be some solid reasons and justifications for lawyers or even mediators to want to dispense with the joint session in a particular matter or be concerned about its use in a specific case. Emotions might be running too hot to bring the parties together due to prior history, and this might derail the entire process. A lawyer might have a client who is difficult to "manage," and the client might say or share things that could adversely impact the mediation process or undermine the client's case in open caucus. We have all had clients who have a tendency to just say too much against advice. (This is why, as an advocate, I wear high heels so I can stop on an insole.) All fun aside, in this mediator's view the joint session is an opportunity to showcase to the other side why settlement is in everyone's interest and how everyone gains in the process (this is very different than grandstanding and trying to prove you have the winning hand or that your position is better than the other party's position). Mediation should be a settlement-focused, persuasive and cordial process. Let's emphasize this again: Courtesy and civility to the other side (and

obviously the mediator) is paramount; harsh or condescending comments will get you nowhere.

Despite the threats to the joint session, the usage of the session, if the foundation and framework are properly laid out, can be an extremely effective tool in the mediator's toolkit. Of course, the joint session should be modified to meet the needs of each specific case and, if appropriate, as previously indicated, dispensed with only if the cases so warrant. The basic premise behind the joint session is that the clients have the chance to speak; in fact, this might be the only opportunity for a client to speak outside of a courtroom or deposition — both of which include much more limited and controlled statements. This is a time for the clients to have a proverbial seat at the table. When clients have the opportunity to have a voice and advocate their own positions, without the filter of an attorney, additional facts, opinions and important issues come to light and can impact the process in a positive way. Also, allowing your client to hear the other side directly can be very illuminating for them, which allows both sides to see the issues through the other's eyes.

Both clients and attorneys determine their strategies in response to the positions taken by the other side. In mediation, that decision can be impacted by the manner in which the message is conveyed. Thus, both the lawyers and clients can assess the sincerity of the other side's story or belief and commitment in their side of the case and position, as well as understand why they feel justified or aggrieved. You can also evaluate your own client's ability to project as a credible witness in an open forum and project toward a courtroom setting; this cuts both ways, for both the other side's client and your own. During this time, the legal arguments take on a life of their own and can lead to a more personalized and successful process.

It is important for the mediator to diligently control this process. Prior to the mediation, both in writing and in separate calls, I emphasize the importance of the nature of the presentations to be made at the joint session; they are to be settlement-focused, and the client should be allowed to actively participate and speak. This is a collaborative process, and the parties can (and should) identify the key areas of concern, voice their grievances and try to focus the discussion in a manner that enables the other side to "understand where they are coming from." This is where clients should focus on needs, not wants. It is common that through this face-to-face dialogue, each side learns something new about the other's position, which up until this point has not filtered through their counsel and legal papers. The joint session is also a chance to present each side's version of the case or issues to the other side. While the joint session is not a time for argument, it is a time for a party to express the basis for its position in a manner that provides the other side the opportunity to understand the basis for that position.

In order to set the tone for the joint session, I speak with counsel jointly and at times separately, and sometimes with their clients, prior to the mediation. I also emphasize to each of them that the written statements that will be shared among the parties should be settlement-focused, persuasive statements — not litigation-based treatises. I also discuss who will be present at the mediation, or perhaps who should be present. For example, at times, the existence of an intractable personal conflict between two specific individuals might preclude resolution of a conflict, while involvement of others with authority might accomplish resolution in a more peaceful manner. I encourage the parties to give careful thought to what information to bring, collect and have available, such as demonstratives in appropriate cases.

Moreover, at times other than when there is a bankruptcy trustee in place or a litigation committee, the parties might have existing longstanding relationships with one another. As such, they may have things that not only need to be said, but thoughts on constructing a resolution that might facilitate an ongoing relationship. At times, parties have been creative in resolving their differences by speaking to one another and compromising on current or future business terms or dealings in order to resolve the dispute at hand. This is accomplished much more easily without the lawyers trying to negotiate basic deal points or shuttle back and forth with a number exchange. This gets to the heart of the original purpose of mediation and the joint session, allowing the parties to speak and trade items, or dollars, in order to resolve the dispute.

Moreover, the joint session is also not just for the parties to assess each other. Rather, the session also allows the mediator

continued on page 67

Mediation Matters: The Continuing Value of the Joint Session in Mediation

from page 31

to assess the dynamics among the parties and get a read on how they interact with each other and where they (versus their lawyers) are entrenched in a position, or those things that matter most to them individually. This can be very helpful in determining how to manage the process during separate caucus, as well as picking a path to develop the negotiation process and further resolution. The joint session also allows the mediator to see how the lawyers are interacting with one another and perhaps determine that there might be other factors at play in the inability to resolve the matter, such as significant personality differences that need to be managed or implicit bias concerns wherein each side might be underestimating, undermining or undervaluing the options and statements of the other to the potential detriment of the client's concerns.

All of these factors are not readily apparent outside a joint session and interplay among the parties. Separate caucus only shows a window into one specific side of the negotiation process. While the mediator can utilize the joint session to even the playing field a bit and mitigate some of these concerns, huge issues in this area (which can be flagged in early calls) might lead to a real consideration to dispense with the joint session; therefore, keep this in mind when you hold an advance lawyers-only call and how the attorneys interact with one another. The mediator's job is not to serve as counsel to the parties, so incompetent lawyering cannot be fixed by the mediator, such as by suggesting defenses to one side or claims to the other (that would be a remarkable breach of ethics by a mediator). However, the mediator can manage evidence of implicit bias that might be adversely impacting the process and manage the parties so that hot personalities do not get in the way of the process.

Despite all of the foregoing, there are indeed times when a joint session should be skipped (*e.g.*, when the exchange of vitriol or threatening messages will lead to a breakdown in communications and the overall settlement process). However, it is still a valuable tool that should not be automatically pushed aside. So, from this mediator's perspective, the session should be utilized judiciously when it serves a purpose, and not by rote. Lawyers: When a joint session is utilized, please encourage and prepare your clients to speak! Mediation is a client-driven process that allows the chance for clients to create a solution that meets both of their needs more effectively than what might be achieved in court. Allowing this forum for open dialogue and an assessment of each side's position is invaluable to resolution. Always keep in mind something I emphasize and have now named the "four C's of effective mediation": civility, cooperation, creativity and collaboration. The joint session can be an excellent place to ensure that these four concepts are embedded in the mediation process. abi