Schulte Roth&Zabel

Alert

Videoconferencing: Tips for Fund Managers to Navigate Security, Privacy and Compliance Risks

April 10, 2020

The COVID-19 pandemic has resulted in a dramatic increase in the use of web-based video and audio conferencing ("WC") services by private fund managers, as most, if not all, employees are working from home. While the availability of this technology is not new, and in fact has been widespread in some industries for many years, many fund managers are adopting WC for the first time or relying on it in new ways. With its expanded adoption and use, the security and privacy issues associated with the use of WC technology have come into the spotlight. For example, Zoom has become the subject of attorney general inquiries in New York, Connecticut and Florida as well as several lawsuits citing security and privacy concerns. In addition, several government entities, private businesses and schools have told their personnel to stop using Zoom.[1]

On March 30, 2020, the FBI's Boston field office issued a warning after numerous accounts of WC hijacking, colloquially referred to as "Zoombombing" or "Zoom raiding."[2] Instances of hijacking reported in the media have focused on the use of WC by schools, religious groups and public service organizations such as AA, where intruders have posted hateful, pornographic or otherwise offensive and disruptive content, often by exploiting a publicly-posted meeting link.[3] These alarming developments highlight the serious concerns presented by the use of WC services for meetings, where unauthorized access (either during the course of the meeting or, if recordings are made, thereafter) could compromise confidential and other sensitive business information. Unauthorized access also has implications for the privacy rights of meeting attendees or other persons, such as a manager's employees, clients and investors, whose personal information may be discussed or displayed during a meeting.

Chat features offered by some WC providers also present compliance issues for managers, specifically challenges in meeting their books and records obligations under Rule 204-2 of the Investment Advisers Act ("Books and Records Rule") or under their internal document preservation and other compliance policies.

As discussed in this *Alert*, there are a variety of measures private fund managers can take to mitigate the security, privacy and compliance risks associated with business conducted through the use of WC services.

---

[1] *See*, e.g., https://www.cnbc.com/2020/04/03/zoom-probed-by-three-states-for-potential-privacy-violations.html; https://www.cnet.com/news/zoom-every-security-issue-uncovered-in-the-video-chat-app/.

[2] *See* https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic.

[3] *See*, e.g., https://www.nytimes.com/2020/04/03/technology/zoom-harassment-abuse-racism-fbi-warning.html.

WC Services Technology

Generally speaking, WC services use software and hardware to permit remote users to connect and exchange live video, audio and written content, through laptops, desktops, smart phones and similar computerized devices. WC service providers, such as Zoom, LoopUp, Cisco WebEx, GoToMeeting, Slack and Skype, provide users with the software and hardware that enables such communications. WC software offers users various features, which vary across service providers, but typically include access controls (used by a host to manage participant access to a meeting), meeting recording, screen sharing and live chat among the users.

Books and Records Retention Considerations

Some WC services offer chat features that allow some or all participants to send chat messages. Managers should ensure that they are considering the implications of this technology in light of their obligations under the Books and Records Rule and their compliance policies. For example, some managers are advising personnel to host video conferencing only via Slack, which is already set up to capture and retain communications. All managers should consider providing guidance for using chat features on externally hosted WC services. Managers, for example, could advise personnel not to use the chat feature on any WC service that the manager does not have the ability to capture, or require any participant who uses a chat feature to download a copy of the chat and send via firm email.[4]

Best Practices for WC Platforms

Irrespective of the platform utilized, private fund managers should evaluate their use of WC services and adopt reasonable measures to protect the security and privacy of WC communications. Below is a list of best practices, compiled based on guidance from the FBI and IT experts, that can serve as points of reference:

1. *Run the Latest Version of WC Software.* WC service providers periodically release new versions of, and updates to, WC software that are intended to address security vulnerabilities, fix known bugs or provide new features or functions (some of which may be useful in improving the security of the WC services). Updating to the latest version of software is critical to keeping in step with bad actors as they find new ways to hack or disrupt WC services.
2. *Configure the WC Software with Robust Security Controls.* Although specific features vary by service provider, WC software generally contains controls that give a meeting host substantial control over an invited participant's access to and use of the WC services. When setting up an account, consider establishing defaults that enhance the security of meetings and don't allow the default settings to be changed, such as:
    a. *Use Unique Meeting IDs*. A meeting ID is one piece of information that is used to gain access to a particular meeting. In some WC configurations, meeting IDs are associated with specific users rather than with specific meetings (so all meetings initiated by a user have the same meeting ID). To prevent unauthorized access by persons who received the meeting ID for a prior meeting held by the same host, configure the WC software to generate a unique meeting ID every time a new meeting is created.

[4] *See,* generally, "OCIE Focusing on Safeguarding of Customer Information and Books and Records Retention," SRZ Private Funds Regulatory Update (August 2019) available here, regarding Risk Alerts OCIE has previously issued regarding electronic messaging.

b. *Require Passwords.* Some WC services may permit participant access to a meeting without a password. Require strong passwords for meeting access and do not allow passwords to be disabled by individual users.

c. *Use Multifactor Authentication*. If available, use multifactor authentication for the meeting host.

d. *Use Meeting Access Controls.* WC services allow the host to control participants' access to a WC meeting. Wherever feasible, hosts should leverage these controls to enhance meeting security as follows:

    i. *Waiting Rooms.* Waiting rooms allow a host to virtually assemble participants before starting a meeting. Using this feature allows the host the opportunity to validate that only invited participants have joined the meeting before any information is shared.

    ii. *Meeting Locks.* Meeting locks allow the host to restrict a participant's access to a meeting until the host has started the meeting and to prevent any new participants from joining a meeting after a meeting has started.

    iii. *Other Tools.* Some WC services allow a host to mute specific participants or remove them altogether from a meeting. Hosts should be prepared to use those tools as necessary to protect the integrity of a meeting.

e. *Turn off Screen Sharing.* WC services allow participants to share their screens during a meeting. Consider disabling the screen sharing function for all participants except for the host unless it is required.

f. *Turn off Recording.* If a WC service allows a meeting to be recorded for playback, disable this feature. If a meeting needs to be recorded, to retain for purposes such as training, consider disabling the recording feature for all participants except for the host.[5]

g. *Turn off Chat.* Many WC services permit participants to chat by live text. Disable this feature unless it is necessary for the meeting. If chat is enabled, it should be configured so that only messaging among the host and all participants (versus private messaging between participants) is permitted and the host can save and download the chat at the end for recordkeeping purposes.

3. *Use an Enterprise Solution with Sufficient Security Features.* WC vendors provide both personal (or "consumer") and enterprise versions of their software. Fund managers should purchase an enterprise solution that supports a sufficient number of participants and provides the necessary functionality, including features designed to enhance security and privacy. Free or lower-cost consumer versions often lack a full set of security controls and embed advertising that increases the risk of a security breach and unauthorized collection of personal information.

4. *Claim and Manage Your Domain.* If a WC service allows, claim your organization's email address domain (such as @srz.com) when adding users to your WC services account. Users with the specified domain (e.g., your employees) will be prompted to join your WC services account and therefore held to the security and privacy configurations set at an enterprise level.

[5] Managers should consider providing guidance to personnel about whether/when to record videoconferences, as well as how copies of videoconferences are stored, for how long and who can access them based on the nature of the meeting.

5. *Educate Personnel.* Send a communication to personnel about potential risks associated with WC services and best practices, including with respect to the controls discussed above. Send updates and reminders to personnel, particularly if the risk may be elevated (e.g., reports of a pervasive hacking scheme).

WC Vendor Diligencing and Monitoring

Diligencing Vendors. Fund managers should, of course, conduct and document the findings of cyber diligence on all new WC vendors, as for any other information technology vendors.[6] In February, the SEC's Office of Compliance Inspections and Examinations ("OCIE") issued guidance for vendor management that can serve as an outline of topics.[7] However, diligence should not be considered to be a "one time" event; cyber diligence on vendors should be refreshed on a periodic basis, and cyber measures should not be allowed to become overly stale.

Monitoring WC Vendor Security and Privacy Issues. WC-related security and privacy issues tend to arise with relative frequency and, similarly, are addressed by vendors on an ongoing basis. Since the COVID-19 pandemic hit, many WC vendors have changed or clarified their privacy practices and issued tips for enhanced security. Fund managers should stay up-to-date on threat communications and responses from WC vendors and ensure that they are implementing the latest security and privacy measures.

Documenting Oversight

All private fund managers are subject to regulatory oversight and to client and investor diligence inquiries, which makes it important to document, as completely and as contemporaneously as possible, the efforts undertaken to respond to changes in the overall environment and to vendor-specific WC issues and challenges. While this is difficult in a time of stress, all managers should be dedicating some resources to preparing for the discussions that will follow the end of the pandemic.

[6] For example, managers should review the service provider's terms of use and privacy policies to confirm they contain limited use rights that state the service provider has access to the content only to the extent needed to provide the WC service to the organization. Most WC service providers, including Zoom, Cisco WebX and GoToMeeting, have user policies that make clear that, as between the vendor and the customer, the customer owns and controls (and is responsible for) the content of the meetings. Additionally, managers that plan to store recordings with the service provider should review the service provider's terms of use to understand how long the service provider will maintain a copy of the recordings (typically 30 days) and the user's rights, if any, to obtain copies of those recordings.

[7] *See* https://www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf. OCIE suggested measures such as (a) ensuring vendors meet security requirements and that appropriate safeguards are implemented by leveraging questionnaires based on reviews of industry standards (e.g., SOC 2, SSAE 18) as well as independent audits; (b) understanding all contract terms, including rights, responsibilities, expectations and other specific terms, to ensure that all parties have the same understanding of how risk and security is addressed; (c) understanding and managing the risks related to vendor outsourcing, including vendor use of cloud-based services; and (d) monitoring the vendor relationship to ensure that the vendor continues to meet security requirements and to be aware of changes to the vendor's services or personnel.

Authored by Marc E. Elovitz, Brian T. Daly, Edward H. Sadtler, Kelly Koscuiszka, John C. Garces and Scott M. Kareff.

If you have any questions concerning this *Alert*, please contact your attorney at Schulte Roth & Zabel or one of the authors.

Schulte Roth & Zabel
New York | Washington DC | London
www.srz.com