Hacked Electronic Collaborative Tools Trigger Cybersecurity Reporting Obligations

In light of the COVID-19 pandemic and related "stay home" orders, web conferencing technology has become a critical tool in allowing people and businesses to remain connected and continue operating. Recent reports, however, suggest that these tools, experiencing massive surges in usage, are not without risk and may not be ready for prime time from a digital security, confidentiality, and privacy perspective, particularly when transmitting confidential or other private data. Hackers have become more sophisticated and have attacked these web conferencing platforms during online meetings.[1]

The most high-profile example of this practice is "Zoom-bombing" – occurring most frequently on the web conferencing platform Zoom – with business meetings, school lectures, social happy hours, and even professional sports organizations having been subject to such disruptions. On April 4, 2020, Zoom CEO Eric Yuan, acknowledging that the platform had been subject to such attacks, vowed to "win users trust back" and implement further security on Zoom's platforms.[2]

In response to these attacks, the New York Attorney General Letitia James sent Zoom a letter asking what, if any, new security measures the company has put in place to handle increased traffic on its network and to detect hackers.[3]

Regardless of the platform used by its employees, companies have an obligation under the law to protect the confidential and private data of their clients and must remain proactive in protecting themselves by vetting and approving these online platforms before permitting their use.

Companies must remain in compliance with their due diligence requirements and, if subject to such an attack, their notification requirements under New York's Stop Hacks and Improve Electronic Data Security Act (the "SHIELD Act"). These data protection statutes are crucial initial steps in proactively protecting propriety and confidential information from unauthorized access and use.

The SHIELD Act mandates that a company must "implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of…private information including, but not limited to, [the] disposal of data,"[4] and must implement a data security program having reasonable

[1] Taylor Lorenz, 'Zoombombing': When Video Conferences Go Wrong, *New York Times*, April 7, 2020.
[2] Alex Konrad, All Eyes on Zoom: How The At-Home Era's Breakout Tool Is Coping With Surging Demand- And Scrutiny, *Forbes*. April 3, 2020.
[3] Danny Hakim and Natasha Singer, New York Attorney General Looks Into Zoom's Privacy Practices, *New York Times*, March 30, 2020.
[4] N.Y. Gen. Bus. Law § 899-bb(2)(a).

administrative, technical, and physical safeguards.[5] A small business [6] will be deemed compliant if its security program contains reasonable administrative, technical, and physical safeguards that are appropriate for the size and complexity of the business, the nature and scope of its activities, and the sensitivity of the personal information the small business collects from or about consumers.[7]

If a company experiences such an attack, it must give notice to anyone whose data may have been compromised. It must disclose a description of the categories of information, and the specific information, that were reasonably believed to have been acquired, and must inform the effected individuals of the breach via: (1) phone notification; (2) written notice; (3) electronic notice; or (4) some other notification type (email, a public posting, or statewide media announcement).

The standards and requirements of the SHIELD Act apply broadly to anyone or any business that owns or licenses the private information of a New York resident. Remember to maintain best practices and of your obligations under the SHIELD Act to report suspected privacy and security breaches.

Telecommuting techniques being employed today were previously unthinkable, perhaps even deemed impossible. Walden Macht & Haran LLP (WMH) recognizes the increased impact of COVID-19 on our communities, and our lawyers can assist in crafting targeted and cost-effective solutions to the SHIELD Act requirements and risks. There is no higher priority than the health and well-being of our colleagues, clients, their loved ones and the public. Our hearts go out to all who have been personally affected.

About Walden Macht & Haran LLP

WMH is a New York-based boutique law firm with deep experience in resolving complex compliance challenges. Our partners have held numerous senior positions in the public and the private sphere and have the breadth and depth of experience to advise in connection with the most pressing matters and to handle the most sensitive engagements. The partnership includes seven former federal prosecutors, many of whom held senior supervisory positions in the Department of Justice, a former counsel for national security at the Federal Bureau of Investigation, a former general counsel of a NYSE listed multinational, a former chief compliance officer of a publicly traded company, and multiple former state prosecutors. We are known for our experience, integrity, and outstanding track record in both state and federal court and in connection with banking monitorships.

[5] Id.at 2(b).
[6] Fewer than 50 employees, less than $3 million in gross annual revenue in each of the last 3 fiscal years, or less than $5 million in year-end total assets.
[7] N.Y. Gen. Bus. Law § 899-bb(2)(b).