April 2, 2024

The Honorable Gary Gensler
Chairman
U.S. Securities and Exchange Commission
100 F Street NE
Washington, District of Columbia 20549

Dear Chairman Gensler:

The undersigned write to you to express our concern with the Securities and Exchange Commission's enforcement case against SolarWinds and its chief information security officer (CISO) based on the Russian-backed SUNBURST cyberattack and SolarWinds' subsequent disclosures of details to investors. As we discuss below, the SEC's theory of liability with respect to SolarWinds and its CISO raise significant concerns for small businesses across the country by undermining CISOs' ability to engage in good faith efforts to prevent and mitigate cyberattacks.

We are small business entrepreneurs, innovators, and independent developers located across the country that compete in verticals across every industry. We are committed to advancing security by design and a secure software development lifecycle (SDLC), and to enhancing the ability to understand, manage, reduce, and communicate cybersecurity risk across emerging technology areas. Despite the significant resource constraints we face in comparison to the companies the SEC regulates, the market still demands that we—assisted by our CISOs—proactively address cybersecurity risks and build in security by design as a prerequisite to features and speed to market, and that we make timely and appropriate cybersecurity-related disclosures. In fact, for many of us, the CISO role is often occupied by someone serving other important executive functions; in other cases, we are fractional CISOs for numerous companies.

The SEC's enforcement case against SolarWinds and its CISO represents the first time that an enforcement action has been brought that would place personal liability on a CISO. Cybersecurity resiliency requires frank discussions and assessments to be made internally at organizations in light of the capabilities and resources they have. Should the SEC's theory of liability proposed in its enforcement case before the U.S. District Court for the Southern District of New York succeed, it would create a precedent for CISO personal liability based on public filings they are not directly responsible for. Undermining CISOs stands to increase the risks all U.S. businesses face, particularly small businesses like us that may have fractional CISOs or CISOs wearing multiple hats, damaging the U.S. cybersecurity risk posture. Further, the SEC's liability theory stands in contrast to the federal government's approach to cybersecurity risk management provided in its widely-supported National Institute of Standards and Technology *Cybersecurity Framework*,[1] which focuses on scaling risk mitigation to harms presented using international standardized approaches.

[1] https://www.nist.gov/cyberframework.

We recognize that it may be seen as unprecedented that a community of businesses that is not regulated by the SEC would send a letter raising its concerns with policies impacting publicly-traded companies the SEC regulates, and note our broad alignment with SEC goals of increasing investors' knowledge of companies' cybersecurity postures. However, we are compelled to do so because of the broad influence the SEC's theory of liability would have in policymaking across the states and at the federal level more broadly, and the ultimate direct impact on our—and our CISOs'—ability to appropriately address cybersecurity risks and harms.

We are committed to creating a digital economy that is resilient to evolving cybersecurity attacks and for creating appropriate accountability standards. However, imposing personal liability on CISOs, as proposed in the SEC's enforcement case, is not the correct approach to enhance our national cybersecurity posture or promote good faith efforts in cybersecurity risk management. Ultimately, we believe the most appropriate next step is for SEC to withdraw its proposed SolarWinds enforcement case's unprecedented theory of personal liability with respect to SolarWinds' CISO. SEC is strongly encouraged to engage with other cybersecurity leaders in government (e.g., NIST, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, etc.); industry, including the small business community; as well as CISO professionals to ensure that its approach to protecting investors improves the U.S. national cybersecurity posture.

Sincerely,

365.Training

Alchemy Security

Colorado Technology Consultants

ComputerWays, Inc.

Counterpart

Epic Reach

ForAllAbilities

Fresco Capital

Homnick Systems

Paye EyeX

Rotational Labs

SPENDiD

Youdle

cc: Commissioner Hester M. Peirce
Commissioner Caroline A. Crenshaw
Commissioner Mark T. Uyeda
Commissioner Jaime Lizárraga
Gurbir Grewal, Director, Division of Enforcement