SILICON VALLEY
LEADERSHIP GROUP

**TESTIMONY**
**California Privacy Protection Agency**
**Stakeholder Sessions | May 4, 2022**
***Businesses' Experiences with CCPA Responsibilities***

- Good afternoon, my name is Peter Leroe-Muñoz and I am the General Counsel and Senior Vice President of Technology & Innovation for the Silicon Valley Leadership Group.
- Our members represent the breadth of technology companies — ranging from software and consumer devices to nanotech, semiconductors and cleantech. The balance of our membership includes a variety of industries that support our technology core, including financial and professional services, healthcare, higher education, and more. Our membership includes businesses of all sizes, as well as most of the large brands in the Valley.
- On behalf of the Leadership Group, I'd like to thank the CPPA Board for the opportunity to share my comments today regarding the "Businesses' Experiences to Date with CCPA Responsibilities" and "Cybersecurity Audits and Risk Assessments Performed by Businesses".
- In the past few years, data privacy laws and regulations have emerged across the country, and while our members understand that it is a high priority to protect consumer data, the manner in which the policies have been passed have lacked harmonization, creating an extremely challenging legislative and regulatory environment for businesses that are looking to comply. In a January report by Information Technology & Innovation Foundation (ITIF), a nonprofit, nonpartisan research and educational institute it states that, "Since 2018, 34 states have passed or introduced 72 privacy bills regulating the commercial collection and use of personal data." Many California businesses operate outside of state lines which means they are subject to a myriad of privacy policies, not to mention an additional layer of privacy mandates specific to certain industries such as the financial sector and have been in place for years. There should be a consistent standard for assessing what constitutes a significant risk across state lines to allow for businesses to continue to build robust processes to protect consumers' information.
- Needless to say, businesses' experience with CCPA responsibilities has not been easy.
- Examples of compliance measures that create operational and cost concerns include actions such as hiring technical staff, purchasing systems to build/maintain information, training and managing staff, and ongoing maintenance to ensure compliance with out of state privacy policies.
- And as it relates to the cybersecurity audits and risk assessments performed by business, we highly encourage the Board to ensure these items are confidential to avoid the revealing trade secrets and avoid the potential for "fishing expeditions". The audits and assessments should only be conducted on a specific risk or issue. If not, this could open the floodgates for fraud and security breaches and dissuade businesses from taking further compliance action for fear that it would threaten the existence of their business.
- We are concerned that all these costly and burdensome privacy provisions and very little resources and information to support businesses' good faith efforts to comply will negatively impact businesses and will have a ripple effect of unintended consequences such as lower worker productivity, economic harm, and limitations on innovation in California. Thank you.