

Sample Cyber Liability/Privacy Questions in Diligence

- A. Describe Company's (i) IT systems, (ii) IT staff, and (iii) disaster recovery and business continuity policies. Are such systems, staff, and policies sufficient for Company's size and nature? Has Company experienced any outages, interruptions in service, data corruption or security breaches in the past three years?

- B. How does Company collect and store customer data and PII? Are such practices consistent with applicable law, customer/vendor contracts, and Company's data privacy policies?

- C. Does Company process/store credit cards or bank account numbers? Discuss compliance with PCI/DSS, including whether a third-party payment processor is utilized.

- D. Discuss whether Company regularly conducts penetration tests, vulnerability scans, or risk assessments.

- E. Discuss Company's compliance with applicable data privacy laws. Is Company subject to CCPA or GDPR?

- F. Discuss any material costs incurred during the COVID-19 pandemic on Company's IT infrastructure (e.g. as a result of employees remotely working). Is the remote work infrastructure compliant with Company's data privacy procedures?

- G. Discuss Company's compliance with consumer protection laws such as CAN-SPAM, TCPA, and JFPA, including whether Company solicits business directly from individuals via emails, SMS texts, faxes or similar means.