May 6th, 2022

Ms. Vanessa Countryman
Secretary, Office of the Secretary
US Securities and Exchange Commission
100 F Street NE
Washington, DC 20549-1090

Re: Comments on SEC File No. S7-09-22, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

Ms. Countryman:

Paylocity is a leading provider of payroll and human capital management (HCM) software solutions. Paylocity's comprehensive product suite delivers a unified platform for professionals to make strategic decisions in the areas of benefits, core HR, payroll, talent, and workforce management, while cultivating a modern workplace and improving employee engagement. In response to the request for public input regarding File Number S7-09-22, Cybersecurity Risk Management, Strategy, Governance and Incidence Disclosure, we submit the following in response to the questions provided.

Question 5. *Should there be a different triggering event for the Item 1.05 disclosure, such as the registrant's discovery that it has experienced a cybersecurity incident, even if the registrant has not yet been able to determine the materiality of the incident? If so, which information should be disclosed in Form 8-K based on a revised triggering event? Should we instead require disclosure only if the expected costs arising from a cybersecurity incident exceed a certain quantifiable threshold, e.g., a percentage of the company's assets, equity, revenues or net income or alternatively a precise number? If so, what would be an appropriate threshold?*

Paylocity Response. The proposal asks if the SEC should instead require disclosure only if the expected costs arising from a cybersecurity incident exceed a certain threshold. Paylocity supports this approach. Doing so would provide a reasonable and quantitative approach to defining a material incident. a quantifiable, objective measure on what triggers a reporting event. When you leave it up to the organization to decide what an investor will care about, that's too subjective and either we will end up overreporting, or rationalizing in our minds why a normal investor wouldn't care about the incident to avoid reporting altogether.

Question 8. *We are proposing to include an instruction that "a registrant shall make a materiality determination regarding a cybersecurity incident as soon as reasonably practicable after discovery of the incident." Is this instruction sufficient to mitigate the risk of a registrant delaying a materiality determination? Should we consider further guidance regarding the timing of a materiality determination? Should we, for example, suggest examples of timeframes that would (or would not), in most circumstances, be considered prompt?*

Paylocity Response. The proposal would require a registrant to make a materiality determination regarding a cybersecurity incident as soon as reasonably practicable after discovery of the incident. This would create an undue burden on security teams. Security teams are often alerted to potential security incidents multiple times a day, most of which are false positives. Time must be provided to investigate the issue, and even after confirmation of the security event, it'll take considerable time and resources to contain and eradicate the event before we can think about reporting. In most privacy laws require reporting 72 hours after a confirmed breach; meaning, there has been time to fully investigate the situation, vet it that the threat is real, and then timer starts running before disclosure obligations begin.

Question 10. *As described further below, we are proposing to define cybersecurity incident to include an unauthorized occurrence on or through a registrant's "information systems," which is proposed to include "information resources owned or used by the registrant." Would registrants be reasonably able to obtain information to make a materiality determination about cybersecurity incidents affecting information resources that are used but not owned by them? Would a safe harbor for information about cybersecurity incidents affecting information resources that are used but not owned by a registrant be appropriate? If so, why, and what would be the appropriate scope of a safe harbor? What alternative disclosure requirements would provide investors with information about cybersecurity incidents and risks that affect registrants via information systems owned by third parties?*

Paylocity Response. Registrants would not be able to reasonably obtain information to make a materiality determination about cybersecurity incidents affecting information resources that are used by not own by the Registrant. The Registrant should only be required to disclose an incident if the vulnerable third party led to a compromise of the Registrant's information resources.

Question 36. *Should we adopt the proposed Item 407(j)(2) safe harbor to clarify that a director identified as having expertise in cybersecurity would not have any increased level of liability under the federal securities laws as a result of such identification? Are there alternatives we should consider?*

Paylocity Response. Paylocity supports the proposal to adopt the Item 407(j)(2) safe harbor. Board members are not close enough to the everyday workings of the program to be held liable.

Paylocity appreciates your consideration of our comments and would be happy to provide any additional information that may further assist you as your address this important topic.

Respectfully,

Corinne Tirone, JD

Director, Government Relations