Mark R. Allen
Executive Vice President
General Counsel and Secretary
Member of the Executive Committee

942 South Shady Grove Road
Memphis, TN 38120

FedEx Corporation

VIA E-MAIL (*rule-comments@sec.gov*)

May 9, 2022

U.S. Securities and Exchange Commission
Ms. Vanessa A. Countryman
Secretary
100 F Street, NE
Washington, DC 20549-1090

Re: **Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (File No. S7-09-22)**

Dear Ms. Countryman:

On March 9, 2022, the Securities and Exchange Commission (the "Commission") issued a request for public comment soliciting input on the proposed rule regarding cybersecurity risk management, strategy, governance, and incident disclosure (the "Proposing Release"). FedEx Corporation ("FedEx") appreciates the opportunity to provide comments in response to the Commission's request.

FedEx is a global company that provides customers and businesses worldwide with a broad portfolio of transportation, e-commerce, and business services. Our annual revenues total approximately $92 billion, we have nearly 600,000 team members, and we serve customers in more than 220 countries and territories. Our common stock, of which nearly 260 million shares are outstanding, is listed on the New York Stock Exchange. We present our views from the perspective of a preparer of disclosures required to be filed with the Commission and as a large accelerated filer registered with the Commission.

We commend the Commission for its recent efforts to review existing rules and regulations and consider updates when appropriate in light of the evolution of U.S. public markets. We recognize the importance of protecting the privacy of our customers, vendors, and team members, and we deliver on this commitment by proactively ensuring a safe and secure online environment. Further, FedEx recognizes and appreciates the significance of critical cybersecurity practices and reporting material information about cybersecurity risks and incidents to investors in a timely manner. However, we are concerned that certain requirements in the Proposing Release raise significant concerns that must be addressed in any final rules adopted by the Commission.

We appreciate that the Proposing Release would require disclosure only of "material" cyber events, and that the decision as to whether a triggering event has occurred is based on the well-

understood definition of materiality expressed by the Supreme Court.[1] However, we are concerned that a hard and fast rule requiring disclosure of any material cyber event within four business days of an issuer's materiality determination, with no exceptions, is unworkable. In the event of a cyber incident, issuers work closely with federal and state regulatory agencies to identify the perpetrators and prevent future cyber incidents. For example, the Cybersecurity and Infrastructure Security Agency ("CISA") requires that companies make confidential filings, which enable CISA to assist in mitigating an ongoing cybersecurity incident. The Proposing Release would require disclosure even if the issuer has been informed by governmental authorities that delay of disclosure at that time would be in the interest of national security and/or that disclosure at that time would hinder law enforcement efforts to identify or capture the threat actor.

FedEx appreciates the importance of timely and comparable public disclosure of cybersecurity incidents. However, we do not believe the Proposing Release fully accounts for the appropriate balancing of these significant interests, which would place issuers in an untenable situation of potentially impeding matters of national security and/or law enforcement efforts while complying with public disclosure requirements. Additionally, the inflexibility of the disclosure requirements under the Proposing Release may result in harm to investor interests in such situations. Accordingly, it is important that the final rule include an exception for instances where public disclosure of cybersecurity incidents would conflict with national security and/or would hinder law enforcement efforts in connection with a cybersecurity incident. Such an exception will provide issuers with the necessary flexibility to delay public disclosure in such situations and ensure public disclosure requirements account for existing confidential reporting frameworks and law enforcement investigations, thus helping to protect companies, investors, and the United States from increased cybersecurity risks.

As stated above, FedEx appreciates that the Proposing Release would require disclosure only of material cybersecurity incidents. However, we view the requirement to disclose when a "series of previously undisclosed individually immaterial cybersecurity incidents become material in the aggregate" as burdensome and unnecessary. The requirement would result in disjointed and potentially imprecise assessments regarding whether cybersecurity incidents are related, especially in light of the scope and volume of highly immaterial cybersecurity incidents experienced by companies each day. As such, the requirement would impose increased costs on companies to make disclosures without a corresponding increase in the likelihood of producing decision-useful information for investors.

We appreciate your consideration of our comments. If you would like more information, please feel free to contact me at your convenience.

[1] *See, e.g., TSC Industries, Inc. v. Northway, Inc.*, 426 U.S. 438 (1976); *see also Basic, Inc. vs. Levinson*, 485 U.S. 224 (1988).

Sincerely yours,

FedEx Corporation

Mark R. Allen

cc: Robert B. Carter
Jinyu Sun
Clement E. Klank III
Arthur M. Foster
Alana L. Griffin

[1607192]