June 14, 2024

Via EDGAR
U.S. Securities and Exchange Commission
Division of Corporation Finance
Office of Manufacturing
100 F Street, N.E.
Washington, D.C. 20549-3720
Attn: Geoffrey Kruczek
Suzanne Hayes

Re: Dropbox, Inc.
Form 8-K filed May 1, 2024
File No. 001-38434

Ladies and Gentlemen:

Dropbox, Inc. ("we", "our" or the "Company") submits this letter in response to a comment from the staff (the "Staff") of the Securities and Exchange Commission (the "Commission") received by letter (the "Comment Letter") dated June 3, 2024, relating to the Company's Current Report on Form 8-K (File No. 001-38434) filed with the Commission on May 1, 2024 (the "Form 8-K").

In this letter, we have recited the comment from the Staff in italicized, bold type and have followed the comment with the Company's response.

Form 8-K filed May 1, 2024

General

1. ***We note the statement that you experienced a cybersecurity incident in your Form 8-K filed on May 1, 2024. Please advise us as to why you determined to file under Item 1.05 of Form 8-K given your statement that the incident has not had a material impact on your business operations, you do not believe it is likely to have a material impact on your overall business operations and you have not determined whether the incident is reasonably likely to material impact financial condition or results of operations.***

We respectfully advise the Staff that, as disclosed in the Form 8-K, we became aware of unauthorized access to our Dropbox Sign production environment on April 24, 2024. Over the course of the next several days, we engaged in an investigation, in which we discovered that the threat actor had accessed data related to all users of Dropbox Sign, such as emails and usernames, in addition to general account settings. For subsets of users, the threat actor also accessed phone numbers, hashed passwords, and certain authentication information such as API keys, OAuth tokens, and multi-factor authentication. We did not at that time, and do not now, have evidence that the threat actor had accessed the contents of users' accounts, such as their agreements or templates, or their payment information.

Dropbox Sign represents a low single-digit percentage of our total revenue, its infrastructure is largely separate from other Dropbox services, and the unauthorized access did not impact our operations or the operations of our users outside of Dropbox Sign. Given the relative size of Dropbox Sign's operations and financial contribution to our overall business, we did not believe that

the unauthorized access was reasonably likely to be material to our overall business operations and we had not determined that the incident was reasonably likely to materially impact the financial condition and results of operations of the Company as a whole. However, as noted by the Commission in the adopting release for the new cybersecurity rules[1] and more recently, in the statement issued by Erik Gerding, Director of the Commission's Division of Corporation Finance,[2] the analysis with respect to disclosure obligations and materiality should not be limited to financial and operational impacts. Accordingly, we took into account the Commission's statements that, in assessing the impact of incident (or reasonably likely impact), companies should assess all relevant factors, "that assessment should not be limited to the impact on 'financial condition and results of operation,'" and "companies should consider qualitative factors alongside quantitative factors." For example, companies should consider whether the incident will "harm . . . [its] reputation, customer or vendor relationships, or competitiveness."[3] Companies also should consider "the possibility of litigation or regulatory investigations or actions, including regulatory actions by state and Federal Governmental authorities and non-U.S. authorities."[4] In the days after we discovered the unauthorized access, we assessed the number of users impacted, the requirement to notify regulatory authorities, the possibility of litigation, the potential for reputational harm, and the potential impact on our customer relationships.

Taking into account these additional qualitative factors in the aggregate, many of which were uncertain and remain uncertain, we determined that it was reasonably possible that investors would believe that the incident was important. We also took into account that we did not expect to have certainty on these qualitative factors and the impact on our business for some time. We further considered that, at the time of our filing on May 1, 2024, many other companies that had experienced incidents and had come to similar conclusions determined to file a Form 8-K under Item 1.05. We evaluated the requirements of Item 1.05 and concluded that a filing prior to a definitive determination regarding materiality was permissible, and, given that a specific item number had been provided for disclosing cybersecurity incidents, we believed that it was advisable to file our disclosure under Item 1.05. We note, based on Director Gerding's Statement, which was published after the Form 8-K was filed, that the Commission believes that prior to a definitive determination of materiality, cybersecurity incidents should be disclosed under Item 7.01 or 8.01. In light of this statement, we may have made a different decision with regard to the item number under which we filed our disclosure.

We believe that the content of our disclosure enabled investors to evaluate the facts in the context of their own voting and investment decisions.

*****

[1] *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, Release Nos. 33-11216; 34-97989 (July 26, 2023) [88 FR 51896 (Aug. 4, 2023)] (the "Adopting Release").
[2] *Disclosure of Cybersecurity Incidents Determined To Be Material and Other Cybersecurity Incidents*, May 21, 2024, available at https://www.sec.gov/news/statement/gerding-cybersecurity-incidents-05212024 ("Director Gerding's Statement").
[3] Id. (citing the Adopting Release).
[4] Id.

If you have any questions or comments, please contact me.

Sincerely,

/s/ Bart Volkmer

Bart Volkmer
Chief Legal Officer

cc:

Lisa L. Stimmell, Wilson Sonsini Goodrich & Rosati, P.C.