UNITED STATES
SECURITIES AND EXCHANGE COMMISSION

Washington, D.C. 20549

Form 8-K

CURRENT REPORT
Pursuant to Section 13 or 15(d)
of the Securities Exchange Act of 1934

April 29, 2024
Date of Report (date of earliest event reported)

DROPBOX, INC.

(Exact name of Registrant as specified in its charter)

Delaware	**001-38434**	**26-0138832**
(State or other jurisdiction of incorporation)	**(Commission File Number)**	**(I. R. S. Employer Identification No.)**

1800 Owens St.
San Francisco, California 94158
(Address of principal executive offices)
(415) 930-7766
(Registrant’s telephone number, including area code)
N/A
(Former name or former address, if changed since last report)

Check the appropriate box below if the Form 8-K filing is intended to simultaneously satisfy the filing obligation of the registrant under any of the following provisions (see General Instruction A.2. below):

☐ Written communications pursuant to Rule 425 under the Securities Act (17 CFR 230.425)

☐ Soliciting material pursuant to Rule 14a-12 under the Exchange Act (17 CFR 240.14a-12)

☐ Pre-commencement communications pursuant to Rule 14d-2(b) under the Exchange Act (17 CFR 240.14d-2(b))

☐ Pre-commencement communications pursuant to Rule 13e-4(c) under the Exchange Act (17 CFR 240.13e-4(c))

Securities registered pursuant to Section 12(b) of the Act:

Title of each class	Trading Symbol(s)	Name of exchange on which registered
Class A Common Stock, par value $0.00001 per share	DBX	The NASDAQ Stock Market LLC (Nasdaq Global Select Market)

Indicate by check mark whether the registrant is an emerging growth company as defined in Rule 405 of the Securities Act of 1933 (§230.405 of this chapter) or Rule 12b-2 of the Securities Exchange Act of 1934 (§240.12b-2 of this chapter).

Emerging growth company ☐

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act. ☐

Item 1.05 Material Cybersecurity Incidents

On April 24, 2024, Dropbox, Inc. ("*Dropbox*" or "*we*") became aware of unauthorized access to the Dropbox Sign (formerly HelloSign) production environment. We immediately activated our cybersecurity incident response process to investigate, contain, and remediate the incident. Upon further investigation, 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. Based on what we know as of the date of this filing, there is no evidence that the threat actor accessed the contents of users' accounts, such as their agreements or templates, or their payment information. Additionally, we believe this incident was limited to Dropbox Sign infrastructure and there is no evidence that the threat actor accessed the production environments of other Dropbox products. We are continuing our investigation.

When we became aware of the incident, we launched an investigation with industry-leading forensic investigators to understand what happened and mitigate risks to our users. We have notified and are working with law enforcement. As appropriate, we are also notifying regulatory authorities and users with respect to unauthorized access to personal information.

As of the date of this filing, the incident has not had, and we do not believe it is reasonably likely to have, a material impact on our overall business operations, given our current understanding that this incident is limited to the Dropbox Sign infrastructure. We have not determined that the incident is reasonably likely to materially impact our financial condition or results of operations. We remain subject to various risks due to the incident, including potential litigation, changes in customer behavior, and additional regulatory scrutiny. Our remediation efforts are ongoing.

Forward-Looking Statements

This Form 8-K contains forward-looking statements as defined in the Private Securities Litigation Reform Act of 1995. Such forward-looking statements include statements regarding our ongoing investigation of the cybersecurity incident, the nature and known extent of the incident, the isolation of the incident to our Dropbox Sign infrastructure, Dropbox's mitigation and remediation efforts, the potential disruption to our business or operations, and the potential impact on our operations, financial conditions, and results. These statements involve certain risks and uncertainties that may cause actual results to differ materially from expectations as of the date of this release. Among the factors that could cause actual results to differ materially from those indicated in the forward-looking statements are risks and uncertainties associated with the ongoing investigation of the incident, risks related security breaches or incidents, as well as other risks listed or described from time to time in Dropbox's filings with the Securities and Exchange Commission (the "*SEC*"), including Dropbox's Annual Report on Form 10-K filed with the SEC on February 16, 2024. All forward-looking statements are based on information and estimates available to Dropbox at the time of this Current Report on Form 8-K and are not guarantees of future performance. Except as required by law, Dropbox assumes no obligation to update any of the statements in this Current Report on Form 8-K.

Item 7.01 Regulation FD Disclosure

On May 1, 2024, Dropbox posted a blog regarding the incident. A copy of the blog is furnished as Exhibit 99.1 to this report.

The information in this Item 7.01 and Exhibit 99.1 shall not be deemed to be "filed" for purposes of Section 18 of the Securities Exchange Act of 1934, as amended (the "*Exchange Act*"), or otherwise subject to the liability of that section, and shall not be incorporated by reference into any registration statement or other document filed under the Securities Act of 1933, as amended, or the Exchange Act, except as shall be expressly set forth by specific reference in such filing.

Item 9.01 Financial Statements and Exhibits

(d) Exhibits:

Exhibit No.	Exhibit Description
99.1	Dropbox Blog Post dated May 1, 2024 titled "A Recent Security Incident Involving Dropbox Sign"
104.0	Cover Page Interactive Data File (embedded within the Inline XBRL document).

SIGNATURES

Pursuant to the requirements of the Securities Exchange Act of 1934, as amended, the Registrant has duly caused this report to be signed on its behalf by the undersigned hereunto duly authorized.

Dated: May 1, 2024

Dropbox, Inc.
/s/ Bart Volkmer
Bart Volkmer
Chief Legal Officer

Exhibit 99.1

A Recent Security Incident Involving Dropbox Sign

On April 24th, we became aware of unauthorized access to the Dropbox Sign (formerly HelloSign) production environment. Upon further investigation, we discovered that a threat actor had accessed Dropbox Sign customer information. We believe that this incident was isolated to Dropbox Sign infrastructure, and did not impact any other Dropbox products. We're in the process of reaching out to all users impacted by this incident who need to take action, with step-by-step instructions on how to further protect their data. Our security team also reset users' passwords, logged users out of any devices they had connected to Dropbox Sign, and is coordinating the rotation of all API keys and OAuth tokens. Please read on for additional details and an FAQ.

On April 24th, we became aware of unauthorized access to the Dropbox Sign (formerly HelloSign) production environment. Upon further investigation, we discovered that a threat actor had accessed data including Dropbox Sign customer information such as emails, usernames, phone numbers and hashed passwords, in addition to general account settings and certain authentication information such as API keys, OAuth tokens, and multi-factor authentication.

For those who received or signed a document through Dropbox Sign, but never created an account, email addresses and names were also exposed. Additionally, if you created a Dropbox Sign or HelloSign account, but did not set up a password with us (e.g. "Sign up with Google"), no password was stored or exposed. We've found no evidence of unauthorized access to the contents of customers' accounts (i.e. their documents or agreements), or their payment information.

From a technical perspective, Dropbox Sign's infrastructure is largely separate from other Dropbox services. That said, we thoroughly investigated this risk and believe that this incident was isolated to Dropbox Sign infrastructure, and did not impact any other Dropbox products.

What happened and our response

When we became aware of this issue, we launched an investigation with industry-leading forensic investigators to understand what happened and mitigate risks to our users.

Based on our investigation, a third party gained access to a Dropbox Sign automated system configuration tool. The actor compromised a service account that was part of Sign's back-end, which is a type of non-human account used to execute applications and run automated services. As such, this account had privileges to take a variety of actions within Sign's production environment. The threat actor then used this access to the production environment to access our customer database.

In response, our security team reset users' passwords, logged users out of any devices they had connected to Dropbox Sign, and is coordinating the rotation of all API keys and OAuth tokens. We reported this event to data protection regulators and law enforcement.

What we're doing next

At Dropbox, our number one value is to be worthy of trust. We hold ourselves to a high standard when protecting our customers and their content. We didn't live up to that standard here, and we're deeply sorry for the impact it caused our customers.

We've been working around the clock to mitigate risk to our customers, and we're in the process of reaching out to all users impacted by this incident who need to take action, with step-by-step instructions on how to further protect their data.

We're also conducting an extensive review of this incident to better understand how this happened, and to protect against this kind of threat in the future. We are grateful for our customers' partnership, and we're here to help all of those who were impacted by this incident.

To contact us about this incident, please reach out to us here.

Customer FAQ

I’m a Sign customer - what has Dropbox done to protect me and what do I need to do?

- We’ve found no evidence of unauthorized access to the contents of users’ accounts (i.e. their documents or agreements).
- We’ve expired your password and logged you out of any devices you had connected to Dropbox Sign to further protect your account. The next time you log in to your Sign account, you’ll be sent an email to reset your password. We recommend you do this as soon as possible.
- If you’re an API customer, to ensure the security of your account, you’ll need to rotate your API key by generating a new one, configuring it with your application, and deleting your current one. As an additional precaution, we’ll be restricting certain functionality of API keys while we coordinate rotation. Only signature requests and signing capabilities will continue to be operational for your business continuity. Once you rotate your API keys, restrictions will be removed and the product will continue to function as normal. Here is how you can easily create a new key.
- Customers who use an authenticator app for multi-factor authentication should reset it. Please delete your existing entry and then reset it. If you use SMS you do not need to take any action.
- If you reused your Dropbox Sign password on any other services, we strongly recommend that you change your password on those accounts and utilize multi-factor authentication when available.

If I have a Sign account linked to my Dropbox account, is my Dropbox account affected?

- No. Based on our investigation to date, we believe this incident was isolated to Dropbox Sign infrastructure, and did not impact any other Dropbox products.
- However, if you reused your Dropbox Sign password on any other services, we strongly recommend that you change your password on those accounts and utilize multi-factor authentication when available. Instructions on how to do this for your Dropbox Sign account can be found here.

I’m a Sign API customer. Was my customers’ data exposed as well?

- Names and email addresses for those who received or signed a document through Dropbox Sign, but never created an account, were exposed.

Where can I go for more information on this incident?

- We’re in the process of reaching out to all impacted users who need to take action, and we expect all notifications to be complete within a week.

Is your investigation complete?

- Our investigation is still ongoing, and we’ll provide additional updates as we have them.