A recent security incident involving Dropbox Sign

by Dropbox Sign team

May 1, 2024 • 6 minute read

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 email addresses, 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.

May 3, 2024 update: edited list of customer information to clarify that email addresses were involved, not emails

Up next:

Product news 2 minute read

Product news 4 minute read

eBook