framework

Dear Valued Framework Customer,

We are writing to inform you of a data breach at our business intelligence database provider Metabase that resulted in an attacker accessing customer names, email addresses, phone numbers, and addresses. Your information was in the database that was accessed in this breach. This breach did not include order or payment information.

We have full details on the incident below. We are deeply sorry for this breach of information, and are reviewing and improving our methodology for data storage in external database vendors.

We are also in the process of notifying the regulatory authorities in each region where relevant regulations exist. Note that while regulations in most regions do not require notification for breaches of names, email addresses, phone numbers, and addresses, we are sending this email to you regardless to ensure you have visibility and can take any actions needed.

What happened?

On August 6th, 2026 at 9am Pacific Time, Metabase notified us of a breach of their systems with the following email message:

On Monday, August 3, we discovered that Metabase Cloud was attacked by someone utilizing an unknown (“0-day”) security vulnerability in versions 1.58 and above. We immediately blocked the endpoints used for the attack, then quickly identified and patched the vulnerability. We notified law enforcement, and we have engaged with a third party forensics firm to conduct an independent investigation.

Your instance of Metabase was vulnerable to this 0-day. Therefore, to protect your company, we recommend you:

Rotate the credentials for every database connected to your instance; and

Review the admin accounts on your instance and remove anything you don't recognize.

We also discovered that the attacker was able to gain access to your instance. We created a report on the actions we believe the attacker took on your instance, which includes log files, and which you can get from the Metabase Store at [removed url].

(If you do not have access to the Metabase Store, are having issues accessing the report, or do not want to click on a link in an unexpected email, you can log into your instance directly and reach us at Help > Get help in the grid menu in the upper right hand corner. We'll confirm this message is from us and email you the report.)

This report is based on our own application logs. We did not query or read the data in your connected databases.

Depending on the jurisdictions in which you operate and kinds of data your instance connects to, you may have notification obligations under applicable laws. If you have concerns in this regard, we recommend you assess potential notification obligations with your company's legal or compliance experts.

We regret any inconvenience this incident may cause you, and we are here to support you. If you have questions, please reply to this email or email us at [removed email address], and we'll get back to you as quickly as we can.

Sameer Al-Sakran

Founder and CEO

Metabase

We immediately investigated the logs Metabase provided to us and confirmed that our database instance was accessed by the attacker. We confirmed that the following information was accessed:

- Full name
- Email address
- Login IPs
- Billing and shipping address information
    - Country
    - Address
    - City
    - State
    - Zip code

- Phone number
- Company

For Framework for Business customers, we are investigating whether the following information may additionally have been accessed:

- Company
- Phone
- VAT
- EIN
- Billing Email

No other personally identifiable information, order information, or payment information was accessed.

Note that Metabase has additionally flagged:

Important: This is a preliminary update based on our current knowledge.

We are working with a third-party forensic investigation firm to understand the full nature and scope of the event.

We are providing you this interim update in advance of completing our investigation to allow you to better understand any potential impact and secure your data.

Our investigation is ongoing and the information shared now is preliminary.

Please look at the application logs as well as the queries executed that are provided as separate files in the zip file for detailed activity and a potential timeline.

We're providing you notice of the breach in the meantime to ensure you have the earliest possible visibility. In the event Metabase notifies us of additional information that impacts you, we will send a follow-up email.

What was done to resolve the issue?

After we were notified of the breach by Metabase, we rotated credentials on all databases associated with our Metabase instance and confirmed that there were no changes in admin access or access to systems outside of Metabase.

What steps have you taken to ensure this doesn’t happen in the future?

We are evaluating the breadth and depth of data shared with business intelligence platforms, and scoping down their access to only the columns required for analysis.

Nirav Patel and the Framework Team

© 2026 Framework Computer Inc

447 Sutter St, PMB 135, San Francisco, CA, 94108-4618