

April 25, 2026

[Massachusetts Employee] [Employee Work Email]

## **Re: Notice of Data Security Incident Involving Your Personal Information**

Dear [Massachusetts Employee],

We are writing to notify you of a data security incident that affected your personal information. We take the privacy and security of your information seriously and want to provide you with a clear account of what occurred, what information was involved, and what steps we have taken in response.

**What Happened.** On April 1, 2026, Axosoft LLC (dba GitKraken) discovered that certain employee personal information had inadvertently been routed into our internal product telemetry data systems via a third-party integration. Specifically, when employees used the Claude Office 365 Excel integration to interact with a payroll and finance spreadsheet, the integration generated telemetry events that captured the contents of the spreadsheet, including the personal and compensation information described below. This data was stored in our internal Snowflake data warehouse and associated cloud storage. The incident was discovered on April 1, 2026 and the data first appeared in our systems on March 31, 2026. The maximum possible exposure window begins on approximately March 4, 2026, when the relevant integration was enabled.

**Information Involved.** The following categories of your personal information may have been present in the affected systems:

- Your full name
- Your work email address
- Your employee ID number
- Your salary and/or compensation information
- Your 401(k) contribution and/or account information

**What We Did.** Upon discovering the incident on April 1, 2026, we took immediate action to secure the affected data. We masked access to the affected data within hours of discovery, blocked the responsible integration from submitting further data on April 3, 2026, and deleted all affected records from our primary database and cloud storage on April 3, 2026. We have conducted a detailed access log investigation and confirmed that the affected data did not propagate to any downstream systems.

**Scope of Access.** We have no indication that your personal information left the control of the company or our authorized internal systems at any point. Based on our investigation, we do not believe your information was accessed by anyone outside of Axosoft LLC. Access to the

systems where the data was present was limited to a small number of authorized Finance and HR personnel in the ordinary course of their responsibilities, and to the internal technical staff who identified and contained the incident. We are not aware of any unauthorized viewing, copying, or use of your information.

**What You Can Do.** While we are not aware of any misuse of your information as a result of this incident, we encourage you to remain vigilant and take the following steps to protect yourself:

- **Place a free security freeze on your credit file.** Under federal law, you are entitled to place a security freeze with each of the three major credit bureaus at no cost. A freeze prevents new credit from being opened in your name without your explicit authorization. Contact each bureau directly:
  - Equifax: [equifax.com/personal/credit-report-services](https://equifax.com/personal/credit-report-services) or 1-800-685-1111
  - Experian: [experian.com/freeze](https://experian.com/freeze) or 1-888-397-3742
  - TransUnion: [transunion.com/credit-freeze](https://transunion.com/credit-freeze) or 1-888-909-8872
- **Place a free fraud alert.** You may place a free one-year fraud alert with any one of the three credit bureaus — that bureau will notify the other two. A fraud alert requires creditors to take extra steps to verify your identity before extending new credit.
- **Monitor your financial accounts.** Review your bank accounts, 401(k), and benefits accounts regularly for any unauthorized activity or changes.
- **Be alert for phishing.** Be cautious of unexpected emails, calls, or messages that may use your personal information. We will never ask for your password or financial credentials by email.

**Your Rights Under Massachusetts Law.** Under Massachusetts law (M.G.L. c. 93H), you have the right to obtain a police report in connection with this incident, which may assist you if you become a victim of identity theft. You also have the right to request a security freeze on your credit file with each of the three major credit reporting agencies. Security freezes are provided at no charge under federal law (Pub. L. 115-174). To place a freeze, contact each bureau at the addresses listed above. Massachusetts residents seeking additional information about identity theft protection may contact the Massachusetts Attorney General's Office at [mass.gov/ago](https://mass.gov/ago) or the Office of Consumer Affairs and Business Regulation at [mass.gov/ocabr](https://mass.gov/ocabr).

**Contact Us.** If you have questions about this notice or the incident, please contact us at [legal@gitkraken.com](mailto:legal@gitkraken.com) or by mail at Axosoft LLC, Attn: Privacy, 16435 N. Scottsdale Road, Scottsdale, Arizona 85254. We deeply regret any concern this incident may cause you and are committed to protecting your information going forward.