

Workstream Technologies, Inc.
521 7th Street
San Francisco, CA 94103

[Date], 2024

[Name]
[Address 1]
[Address 2]

NOTICE OF DATA BREACH

Dear [First Name],

Workstream Technologies Inc. (“we,” “us,” or “our”) is writing to inform you of potential unauthorized access to or acquisition of your personal information caused by our vendor, Dropbox. We provide products to your employer or a business where you submitted an employment application, and our vendor Dropbox is part of that product offering. You provided certain information to us via Dropbox as part of your employee onboarding process or the application process. Below are details of what happened, the steps we are taking to resolve the situation, and what we are doing to support potentially affected individuals.

WHAT HAPPENED?

On August 16, we discovered that a software update released by our vendor, Dropbox, contained a bug and rendered certain documents signed using the Dropbox tool in our product to be potentially accessible by human resources departments at certain other Workstream Technologies customers between August 8 and August 16. As a result, we immediately began an investigation and took steps with Dropbox to address their error. Our investigation was unable to confirm whether your personal information was accessed or acquired; however we are informing you of this incident out of an abundance of caution.

WHAT INFORMATION WAS INVOLVED?

The information that may have been accessed or acquired included your [Data element(s)].

WHAT ARE WE DOING?

Once we identified the issue, we limited access to materials in the service while Dropbox corrected their error. On August 23, Dropbox informed us that they identified and contained the root cause for this issue and mitigated the bug on all affected versions of their service. We also continue to assess further options to safeguard your information as we continue to work with Dropbox on their investigation.

While we have been unable to confirm whether your personal information has been subject to unauthorized access or acquisition, we are offering you complimentary access to 24 months of credit monitoring and identity theft restoration services through Equifax. You will need to enroll yourself in these services if you wish to do so, as we are not able to activate them on your behalf. Please review the instructions in the attached *Information on Credit Monitoring & Identity Theft*.

WHAT CAN YOU DO?

While we have no reason to believe your personal information has been misused, in addition to

enrolling in credit monitoring, we always recommend that you remain vigilant for incidents of fraud and identity theft as described below. We also encourage you to carefully review your account statements to ensure that all account activity is valid. Promptly report any fraudulent activity or any suspected incidents of identity theft to your bank or other financial institution holding your accounts, as well as any appropriate authorities, such as your state attorney general and the Federal Trade Commission (“FTC”). Individuals also have the right to obtain a police report in the event one has been created for this incident.

FOR MORE INFORMATION

For more information and assistance, please contact incidents@workstream.is or 415-669-8741 9 am through 5 pm PST Monday through Friday.

Please know that we take this matter very seriously, and we apologize for any stress or concern this may cause. We appreciate your patience as we have worked to address this issue.

Sincerely,

A handwritten signature in black ink, appearing to read 'DL', with a large, stylized flourish extending from the end of the signature.

Desmond Lim
Chief Executive Officer, Workstream Technologies Inc.

INFORMATION ON CREDIT MONITORING & IDENTITY THEFT



<First Name> <Last Name>

Enter your Activation Code: <Activation Code>

Enrollment Deadline: **December 31, 2024**

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications¹ when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts², which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock³
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to \$1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft⁴

Enrollment Instructions

Go to www.equifax.com/activate

Enter your unique Activation Code of <Activation Code> then click “Submit”

1. **Register:**

Complete the form with your contact information and click “Continue”.

If you already have a myEquifax account, click the ‘Sign in here’ link under the “Let’s get started” header.

Once you have successfully signed in, you will skip to the Checkout Page in Step 4

2. **Create Account:**

Enter your email address, create a password, and accept the terms of use.

3. **Verify Identity:**

To enroll in your product, we will ask you to complete our identity verification process.

4. **Checkout:**

Upon successful verification of your identity, you will see the Checkout Page.

Click ‘Sign Me Up’ to finish enrolling.

You’re done!

The confirmation page shows your completed enrollment.

Click “View My Product” to access the product features.

¹WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded. ²The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer

Services LLC. ³Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-

approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com ⁴The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Individuals are advised to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports and to promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general as well as the Federal Trade Commission.

The following are some resources:

Federal Trade Commission (“FTC”)

www.ftc.gov/idtheft

1-877-ID-THEFT (1-877-438-4338)

Federal Trade Commission 600 Pennsylvania Avenue, NW Washington, DC 20580

Take Charge: Fighting Back Against Identity Theft

This is a comprehensive guide from FTC to help guard against and deal with identity theft

<https://www.identitytheft.gov/>.

Credit Bureaus

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com, calling 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at www.annualcreditreport.com/manualRequestForm.action

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

<p>Equifax 1-800-685-1111 www.equifax.com/personal/credit-report-services/ P.O. Box 740241 Atlanta, GA 30374</p>	<p>Experian 1-888-397-3742 www.experian.com P.O. Box 4500 Allen, TX 75013</p>	<p>TransUnion 1-800-888-4213 www.transunion.com/fraud P.O. Box 1000 Chester, PA 19016</p>
---	--	--

You can obtain additional information from the FTC and the nationwide credit reporting agencies about placing a security freeze on your credit files and fraud alerts. A security freeze is a free tool that lets you restrict access to your credit report, which in turn makes it more difficult for identity thieves to open new accounts in your name. To place a security freeze on your credit files, contact each of the nationwide credit bureaus using the contact information listed above. You will need to supply your name, address, date of birth, social security number, and other personal information. You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies using the contact information listed above.

FOR NEW MEXICO RESIDENTS

You have rights pursuant to the Fair Credit Reporting Act. We encourage you to review these rights by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or by writing to Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

FOR NEW YORK RESIDENTS

You can obtain information about preventing identity theft from:

New York Department of State Division of Consumer Protection: www.dos.ny.gov/consumer-protection

NYS Attorney General at: www.ag.ny.gov

FOR NORTH CAROLINA RESIDENTS

You can obtain information about preventing identify theft from the FTC or:

North Carolina Attorney General:

Visit the North Carolina Office of the Attorney General at:

www.ncdoj.gov or call 1-877-566-7226

or write to this address:

Attorney General's Office

9001 Mail Service Center

Raleigh, NC 27699-9001