

BakerHostetler

Baker & Hostetler LLP

312 Walnut Street
Suite 3200
Cincinnati, OH 45202-4074

T 513.929.3400
F 513.929.0303
www.bakerlaw.com

Joseph L. Bruemmer
direct dial: 513.929.3410
jbruemmer@bakerlaw.com

December 5, 2024

VIA E-MAIL (IDTHEFT@OAG.STATE.MD.US)

Anthony G. Brown
Attorney General
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Incident Notification

Dear Attorney General Brown:

We are writing on behalf of our client, Sprouts Farmers Market ("Sprouts"), to notify your office of a security incident involving one Maryland resident. Sprouts is headquartered at 5455 E. High Street, Suite 111, Phoenix, Arizona 85054.

Sprouts learned of unauthorized activity within a limited number of Sprouts' team members' Workday accounts. Sprouts immediately implemented its response protocols, took measures to contain the activity, and launched an investigation. A cybersecurity firm that has assisted other companies with similar situations was engaged. The evidence showed that an unauthorized actor accessed the team members' accounts on October 11, 2024, using their usernames and passwords. There was no evidence that the unauthorized actor obtained the usernames and passwords from Sprouts' systems. Sprouts reviewed the information that the unauthorized actor would have viewed in the team members' accounts and determined that it included the name and financial account number of one Maryland resident.

Sprouts previously discussed the incident with the Maryland resident, and on December 3, 2024, Sprouts mailed a notification letter to the resident via U.S. mail in accordance with Md. Code Ann., Com. Law § 14-3504. A copy of the notification letter is enclosed. Sprouts is offering the resident a complimentary one-year membership in a credit monitoring and identity protection service. Sprouts also has provided the resident with a phone number and email address that they can use to contact Sprouts for technical assistance or with questions about the incident.

Anthony G. Brown
December 5, 2024
Page 2

To help prevent this type of incident from happening again, Sprouts has taken steps to enhance its existing security measures.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

A handwritten signature in blue ink, appearing to read "Joseph L. Bruemmer", with a large, stylized initial "J" and "B" on the left.

Joseph L. Bruemmer
Partner

Enclosure

<<Name 1>>

<<Name 2>>

<<Address 1>

<<Address 2>>

<<Address 3>>

<<City>><<State>><<Zip>>

<<Date>>

Notice of Data Breach

Dear <<Name 1>>:

Sprouts Farmers Market recognizes the importance of protection information. We are writing to provide additional information concerning the recent unauthorized activity in your Workday account. This notice explains the incident, the measures we have taken in response, and some additional steps you may consider taking.

What Happened?

We previously discussed with you that an unauthorized actor changed the direct deposit information in your Workday account. Upon discovering this activity, we immediately implemented our response protocols, took measures to contain the activity, and launched an investigation. The evidence showed that an unauthorized actor accessed your account on October 11, 2024 using your username and password. There is no evidence that the unauthorized actor obtained your username and password from Sprout's systems.

What Information Was Involved?

We reviewed the activity in your account and, on November 5, 2024, determined that the unauthorized actor would have viewed your name and financial account number when they changed the direct deposit information in your account.

What We Are Doing.

We wanted to notify you of this incident and to assure you that we take it seriously. We have implemented additional security measures to help prevent a similar incident from happening again, which include enforcing enhanced authentication measures for logins to employee Workday accounts.

Additionally, we have arranged for you to receive one year of access to Equifax CompleteTM Premier credit monitoring. This product helps detect possible misuse of your information and provides you with identity protection solutions focused on immediate identification and resolution of identity theft. Activating this product will not hurt your credit score. For more information on identity theft prevention and Equifax CompleteTM Premier, including instructions on how to activate your one year of access, as well as some additional steps you can take in response, please review the pages that follow this letter.

What You Can Do.

Unauthorized actors commonly use usernames and passwords obtained from one online account to log into other online accounts that use the same username and password. If you have not already done so, you should reset the password associated with your Sprouts employee ID, available in Okta. Please contact the Sprouts IT Support Desk if you need assistance. If you used the same password for any other online accounts, you should also change the passwords for those accounts. In addition, you can enroll in the identity monitoring solution that Sprouts has arranged for you to receive, as described above.

For More Information.

We regret this occurred and apologize for any inconvenience. If you have any questions, please contact us at [telephone number] or [email address].

Sincerely,

Sprouts Farmers Market



<FIRST NAME> <LAST NAME>

Enter your Activation Code: <ACTIVATION CODE>

Enrollment Deadline: <DEADLINE MMMM DD, YYYY>

Equifax Complete™ Premier

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

Key Features

- Annual access to your 3-bureau credit report and VantageScore¹ credit scores
- Daily access to your Equifax credit report and 1-bureau VantageScore credit score
- 3-bureau credit monitoring² with email notifications of key changes to your credit reports
- WebScan notifications³ 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 alerts⁴, which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock⁵
- 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 theft⁶.
- Lost Wallet Assistance if your wallet is lost or stolen, and one-stop assistance in canceling and reissuing credit, debit and personal identification cards.

Enrollment Instructions

Go to www.equifax.com/activate

Enter your unique Activation Code of <ACTIVATION CODE> then click “Submit” and follow these 4 steps:

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.

¹The credit scores provided are based on the VantageScore® 3.0 model. For three-bureau VantageScore credit scores, data from Equifax®, Experian®, and TransUnion® are used respectively. Any one-bureau VantageScore uses Equifax data. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness.

²Credit monitoring from Experian and TransUnion will take several days to begin. ³WebScan 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. ⁴The Automatic

Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC. ⁵Locking 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.co

⁶The 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.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity over the next 12 to 24 months. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.identitytheft.gov

Fraud Alerts and Security Freezes

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Sprouts is headquartered at 5455 E. High Street, Suite 111, Phoenix, Arizona 85054 and can be reached at 1 (888) 577-7688.

Additional Information for Resident of the Following State(s):

Maryland: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.marylandattorneygeneral.gov/