

Morgan Lewis

Ezra D. Church

Partner
+1.215.963.5710
ezra.church@morganlewis.com

May 27, 2022

VIA EMAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place, 25th Floor
Baltimore, MD 21202
Email: idtheft@oag.state.md.us

Re: Notice of Data Breach

Dear Sir or Madame:

On behalf of **the New York Teamsters Conference Pension and Retirement Fund** (the "Fund"), pursuant to Md. Code. Com. Law § 14-3501 *et seq.*, we are writing to notify you of an information security incident occurring at its vendor **Express Scripts** ("Express Scripts") involving 3 Maryland residents.

Parties Involved

The Fund engages in financial services and serves as a pension for the New York Teamsters labor union. The Fund is located at 151 Northern Concourse Syracuse, NY 13212-4047.

Express Scripts is a private company that provides online pharmacy services and acts as a pharmacy benefit manager to individuals across various multiemployer benefit plans across various industries. Express Scripts provides prescriptions to various Fund members through home delivery. Express Scripts is located at One Express Way, St. Louis, Missouri 63121.

Nature of the Incident

On May 18, 2022, the Fund learned that Express Scripts was subject to a cybersecurity incident involving the potential compromise of Fund participant data. Based on information provided by Express Scripts, on April 30, 2022, Express Scripts identified and responded to suspicious network traffic on its mobile application. Express Scripts identified various logins using users' correct usernames and passwords and identified these as suspicious on May 1, 2022. Express Scripts immediately initiated efforts to respond to this incident and launched an investigation into the suspicious activity. Currently, neither Express Scripts nor the Fund are aware of any fraud or misuse of Fund participant data.

We understand that the investigation revealed that this bad actor may have been able to obtain a Fund participant's user ID and password in publicly available data from another entity's breach to use and login to the mobile application between April 30, 2022 and May 3, 2022. In order to prevent this from happening again, Express Scripts has locked the affected individual's accounts. Express Scripts provided notice of the event to the Fund on May 18, 2022, and subsequently provided a list of affected individuals. The Fund worked expeditiously to include address information identifying relevant states of residents, and Express Scripts agreed to provide notice to affected individuals occurring on or about May 27, 2022.

What Information was Involved?

After Express Script's investigation, it determined that the personal information accessed potentially included name and prescription information, including medication name(s), prescription number(s), medication dosage(s), prescribing physician name(s), and name(s) of pharmacy. Express Scripts has indicated that no financial information, such as social security numbers, was impacted.

Response to the Incident

Based on information provided by Express Scripts, after learning of the incident, Express Scripts and its Privacy Office have thoroughly investigated the circumstances surrounding this situation and have taken steps to help mitigate any harm that might result from the disclosure, including temporarily halting activity on its mobile application and implementing measures to further safeguard data. Since the incident, Express Scripts has secured the impacted application and confirmed that no other Express Scripts systems or applications have been impacted.

Upon notification, the Fund has worked closely with Express Scripts, through legal counsel, to determine the appropriate notification steps for affected individuals.

The US Department of Health and Human Services ("HHS") and affected Maryland residents were notified on or about May 27, 2022. A sample individual notification letter is attached.

Identity Theft Protection

Express Scripts is providing a complimentary identity monitoring services through Equifax®. This identity monitoring services include credit monitoring, up to \$1 million of identity theft insurance, fraud consultation, and identity theft restoration. None of the notified individuals have been asked or required to waive any right of private action as a condition of accepting the credit monitoring services.

Contact Information

If you have any questions concerning this matter, please contact me on behalf of the Fund at (215) 963-5710, or ezra.church@morganlewis.com.

Best regards,



Ezra D. Church

Enclosure

Sample Individual Notification Letter

Express Scripts
One Express Way, HQ2E03
St. Louis, MO 63121



Date

Member Name
Member Address
Member Address

Re: Reference Number: GPI3133350

Dear Mr./Ms. Member Last Name,

Express Scripts, providing services on behalf of (Covered Entity Name), is committed to protecting the confidentiality of member information. The purpose of this letter is to notify you of a potential disclosure of your information.

WHAT HAPPENED: During system monitoring, we identified potential unauthorized access to your account on the Express Scripts mobile application. A login using the correct username and password occurred on or around April 30, 2022 and was identified as suspicious on May 1, 2022. We believe this may have been a bad actor who was able to obtain your user ID and password in publicly available data from another entity's breach to use to login to the mobile application between April 30, 2022 and May 3, 2022.

WHAT INFORMATION WAS INVOLVED: During the login, the bad actor may have accessed your prescription history for the last 24 months. The information visible would have included your:

- Name
- Medication name(s)
- Prescription number(s)
- Medication dosage
- Prescribing physician name(s)
- Name(s) of pharmacy

WHAT WE ARE DOING: Express Scripts and its Privacy Office have thoroughly investigated the circumstances surrounding this situation and have taken steps to help mitigate any harm that might result from the disclosure. To prevent this from happening again, Express Scripts has locked your web account. In order for you to access your account again, you will have to reset your password, making sure to use a different password. To protect your other information, we also suggest you change your password on any other accounts where you may have used those same login credentials.

WHAT YOU CAN DO: It's important to note that we are confident that no financial information, such as credit card information or Social Security number (SSN), were compromised in this incident. However, as a courtesy and because we care about the security of your information, we partnered with Equifax® to provide its Complete Premier identify theft protection product at no cost to you. A description of this product is provided in the attached material, which also contains instructions on how to enroll (including your personal activation

code). Please review the information provided in the attached material and consider enrolling in this product at our expense. You should always remain vigilant for incidents of fraud or identity theft.

While we do not believe this incident likely places you at significant risk, if you have reason to believe that your personal information is being misused, you can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just any of the nationwide credit reporting agencies listed below. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file.

You may also periodically obtain credit reports from each nationwide credit reporting agency. If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit reporting agency delete that information from your credit report file. In addition, under federal law, you are entitled to one free copy every 12 months of your credit report from each of the three major credit reporting companies. You may obtain a free copy of your credit report by going on the Internet to www.AnnualCreditReport.com or by calling (877) 322-8228. You may contact the nationwide credit reporting agencies as indicated below.

In addition, you can contact the nationwide credit reporting agencies regarding how you may place a security freeze to restrict access to your credit report. You also have a right to place a security freeze on your credit report. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, mortgages, employment, housing or other services. There is no charge to place, lift or remove a security freeze. To place a security freeze on your credit report, you must send a written request to each of the three credit reporting agencies listed above. In order to request a security freeze, you will need to provide the following information:

- Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
- Social Security number;
- Date of birth;
- Your prior addresses if you have moved in the past several years;
- Proof of current address (e.g., a current utility bill or telephone bill); and
- A legible photocopy of a government issued identification card (e.g., state driver's license or ID card or military identification).

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report if a request is made by mail, and one (1) day after making a request by phone or online. The credit reporting agencies must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity access to your credit report, you must send a request to the credit reporting agencies by mail, telephone, or online and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of the entity you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for the identified entity or for the specified period of time if requested by mail, and one (1) hour to lift the freeze after a request by phone or online.

To remove the security freeze, you must send a request to each of the three credit reporting agencies by mail, telephone, or online and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit reporting agencies have three (3) business days after receiving your request to remove the security freeze if requested by mail, and one (1) hour to remove the freeze after a request by phone or online.

You may also have other rights under the FCRA. For information about your rights under the FCRA, please visit: http://files.consumerfinance.gov/f/201410_cfpb_summary_your-rights-under-fcra.pdf

Equifax	TransUnion	Experian
P.O. Box 740241 Atlanta, GA 30374	P.O. Box 6790 Fullerton, CA 92834	P.O. Box 9530 Allen, TX 75013
1-800-525-6285	1-800-680-7289	1-888-397-3742
www.equifax.com	www.transunion.com	www.experian.com

Additionally, you may contact the Federal Trade Commission (“FTC”) or state or local law enforcement, including your state Attorney General, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more about the FTC’s services, you can:

- Visit FTC’s website at www.ftc.gov/idtheft,
- Call the FTC at (877) IDTHEFT (438-4338) or
- Write to
Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW, Washington, DC 20580.

We take our role of safeguarding your information very seriously. We want to assure you that if a potential disclosure of your information is identified, it is investigated and analyzed thoroughly. We regret this situation has occurred and we extend our apologies to you.

FOR MORE INFORMATION: Please direct any inquiries regarding this matter to (place holder 1-877-463-0152). You may also contact the Privacy Office at Express Scripts, Mail Stop HQ2E03, One Express Way, St. Louis, MO 63121, or email us at Privacy@Express-Scripts.com. Please reference the following number when contacting the Privacy Office: GPI 13133350.

IF YOU ARE A DISTRICT OF COLUMBIA RESIDENT: You may obtain information about avoiding identity theft from the FTC (see contact information above) or the District of Columbia Attorney General’s Office, which can be reached at:

Office of the Attorney General
441 4th Street, NW
Suite 1100 South
Washington, DC 20001
(202) 727-3400
<https://oag.dc.gov/>

IF YOU ARE A MARYLAND RESIDENT: You may obtain information about avoiding identity theft from the FTC (see contact information above) or the Maryland Attorney General’s Office, which can be reached at:

Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023
www.oag.state.md.us

IF YOU ARE A NEW YORK RESIDENT: You may obtain information about security breach response and identity theft prevention and protection from the FTC (see contact information above) or from the following New York state agencies:

New York Attorney General
Consumer Frauds &
Protection Bureau
120 Broadway, 3rd Floor
New York, NY 10271
(800) 771-7755
www.ag.ny.gov

New York Department of State
Division of Consumer Protection
99 Washington Avenue
Suite 650
Albany, New York 12231
(800) 697-1220
www.dos.ny.gov

IF YOU ARE A NORTH CAROLINA RESIDENT: You may obtain information about preventing identity theft from the FTC (see contact information above) or the North Carolina Attorney General's Office. These offices can be reached at:

North Carolina Department of Justice
Attorney General Josh Stein
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
<http://www.ncdoj.com>

IF YOU ARE A RHODE ISLAND RESIDENT: You may contact state or local law enforcement to determine whether you can file or obtain a police report relating to this incident. In addition, you can contact the Rhode Island Attorney General at:

Office of the Attorney General
150 South Main Street
Providence, RI 02903
(401) 274-4400
<http://www.riag.ri.gov/>

IF YOU ARE A MASSACHUSETTS RESIDENT: Under Massachusetts law, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Sincerely,



Kimberly J. Piant
U.S. Privacy Officer
Express Scripts



<First Name> <Last Name>

Enter your Activation Code: <Activation Code>

Enrollment Deadline: <Expiration Date>

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"

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.com

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,