



MAILING ADDRESS: P.O. BOX 34630, SAN ANTONIO, TEXAS 78265-4630
PHYSICAL ADDRESS: 555 IH-35 SOUTH, STE. 500, NEW BRAUNFELS, TX 78130
PHONE: (830) 626-5200

October 24, 2024

SENT VIA EMAIL: Idtheft@oag.state.md.us

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

CONFIDENTIAL

Notification of Data Breach

Greetings:

Pursuant to the laws of Maryland, Rush Enterprises, Inc. ("Rush") provides notice of a breach of its information systems. One (1) resident of Maryland and their personal information were potentially impacted by this breach.

On September 18, 2024, Rush identified access to its Microsoft Office 365 (M365) environment by an unauthorized third party ("Threat Actor"). Promptly after learning of the issue, we took steps to understand the nature and scope of the security issue and to secure our systems. We engaged leading security firms to assist our investigation and confirm the Threat Actor(s) were no longer present.

More specifically, between August 21, 2024, and September 18, 2024, a Threat Actor through a sophisticated spear-phishing exploit and compromise of employee account credentials accessed 1,080 email messages and one (1) SharePoint file associated with an employee's M365 account. During this time frame, we are aware of two further unsuccessful phishing attempts using the compromised account.

In addition, between September 16, 2024, and September 17, 2024, a Threat Actor spear-phished another employee's M365 account and accessed 423 email messages. On September 17, 2024, the Threat Actor sent an email to a Rush employee in an unsuccessful attempt to deceive the user into facilitating a fraudulent wire transfer payment to a bank account controlled by the Threat Actor.

Rush confirmed that the last evidence of Threat Actor activity in Rush's environment occurred on September 18, 2024.

Rush immediately changed the password accounts of the two employees and forced re-registration of multifactor authentication. In addition, with the assistance of leading security firms, Rush ensured there were no persistent threats. Rush is also evaluating additional security tooling to prevent or detect credential loss and is revising its InfoSec employee training and communications to further raise security awareness of spear-phishing threats.

Other than the three attempts by the Threat Actor(s) to use the compromised email accounts to impersonate the employees, there is no indication that personal or other confidential information has been misused, misappropriated, disseminated or sold. However, out of an abundance of caution, we have identified approximately 93 persons whose personal or confidential information was contained in accessed emails.

A copy of the form notification and complimentary monitoring services to be sent to potentially impacted individuals is attached.

Please do not hesitate to contact the undersigned with any questions you may have.

Sincerely,



Michael Goldstone
General Counsel
Rush Enterprises, Inc.



Postal Endorsement Line

<<Full Name>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

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

<<Country>>

***Postal IMB Barcode

<<Date>>

<<Variable Header>>

Dear <<Full Name>>:

Rush Enterprises, Inc. understands the importance of protecting the information we maintain. We are writing to notify you of a security issue that involved certain of your personal information. On or around August 21 and September 18, 2024, an unauthorized third party acquired access to two employee email accounts. These email accounts contained documents and records which included information such as name, contact information, date of birth, Social Security and driver's license numbers and certain employment or medical-related information. Promptly after learning of the issue, we took steps to understand its nature and scope and to further secure our systems. We engaged leading security firms to assist with our investigation.

Although to date we have no indication that any of your information was misused, Rush is providing this notification to you so that you may take steps to safeguard your information. As an added precaution, we are also offering 24 months of complimentary access to credit monitoring services through Equifax. If you wish to avail yourself of these services, you will need to enroll using the instructions enclosed with this letter.

Should you have questions about the incident that are not addressed in this letter, please call 855-277-9629 between 9:00 AM and 9:00 PM ET, Monday through Friday, excluding major U.S. holidays.

We hope this information is useful to you and regret any inconvenience this may cause you.

Sincerely,

Rush Enterprises, Inc.



Enter your Activation Code: <<Activation Code>>

Enrollment Deadline: <<Expiration Date>>

Enrollment Duration: **24 months**

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" 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.

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.

– OTHER IMPORTANT INFORMATION –

1. **Placing a Fraud Alert on Your Credit File.**

Whether or not you choose to use the complimentary 24-month credit monitoring services, we recommend that you place an initial one-year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax

P.O. Box 105788

Atlanta, GA 30348

<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>

(800) 525-6285

Experian

P.O. Box 9554

Allen, TX 75013

<https://www.experian.com/fraud/center.html>

(888) 397-3742

TransUnion LLC

P.O. Box 6790

Fullerton, PA 92834-6790

<https://www.transunion.com/fraud-alerts>

(800) 680-7289

2. **Consider Placing a Security Freeze on Your Credit File.**

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze

P.O. Box 105788

Atlanta, GA 30348

<https://www.equifax.com/personal/credit-report-services/credit-freeze/>

1-800-349-9960

Experian Security Freeze

P.O. Box 9554

Allen, TX 75013

<http://experian.com/freeze>

1-888-397-3742

TransUnion Security Freeze

P.O. Box 2000

Chester, PA 19016

<http://www.transunion.com/creditfreeze>

1-888-909-8872

In order to place the security freeze, 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 reporting company will send you a confirmation letter containing 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.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may re-freeze your credit file.

3. **Obtaining a Free Credit Report.**

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call 1-877-322-8228 or request your free credit reports online at www.annualcreditreport.com. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you

did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

4. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If this notice letter states that your financial account information and/or credit or debit card information was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: 515-281-5164.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 888-743-0023.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; <https://ag.ny.gov/consumer-frauds-bureau/identity-theft>; Telephone: 800-771-7755.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392