

October 19, 2022

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

Dear Notification Office:

Broadridge Corporate Issuer Solutions, Inc. is the Transfer Agent for Morgan Stanley, and we keep records of stock ownership of Maryland residents on behalf of this client. We are writing to let you know about an incident involving unauthorized use of a Maryland resident's personal information. We reported this incident to the Federal Bureau of Investigation ("FBI"), and we will cooperate with law enforcement in seeking to identify the perpetrators. Please note that we have no information to indicate that our system was breached. Please note the following:

Approximate Date of Incident and How Discovered: On September 30, 2022, a client notified us that two (2) of their shareholders had new online Shareholder Portal profiles created on one of our websites: <https://investor.broadridge.com>. The two (2) shareholders did not create or authorize the creation of these profiles. Upon further investigation, we determined one additional Shareholder Portal profile relating to a Maryland resident was created from the same IP addresses as the initial two reporting shareholders. This additional Shareholder Portal profile was not created or authorized by the shareholder. In each instance, the unauthorized activity used personal information to create such accounts, including Name, Address, Account Number, and Social Security Number. The setup process also involves the presentation of, and correct responses to, personal identification information in the form of challenge questions. We do not know how this information was obtained. To Broadridge's knowledge, this information was not obtained from Broadridge.

Method: A third party, other than the registered shareholder, used personal information of one Maryland resident obtained from an unknown source to create an online Shareholder Portal Profile.

Number of Maryland Residents affected by Incident: One (1).

Steps Taken to Address Incident:

- We disabled the impacted online Shareholder Portal profile.
- We changed the account numbers of the affected shareholder.
- We temporarily shut down the online Shareholder profile account creation function to limit this activity.
- We escalated this matter internally and initiated an investigation.
- We engaged outside counsel and a forensic data security consultant to assist in investigating the cause of this exposure.
- We reported the incident to the FBI.

We believe we have taken adequate steps to limit the potential unauthorized new Shareholder Portal profile openings. However, in an abundance of caution, we have notified our affected clients and are providing notification and credit monitoring to the affected individuals on their behalf. Please find attached a copy of the template for the notification letter that we are mailing to the affected Maryland resident.

Please do not hesitate to contact me directly if you have any additional questions about this matter. We would be happy to answer any questions that you may have.

Very truly yours,

Robert Franz
Vice President – Operations



Broadridge Corporate Issuer Solutions
PO BOX 1342
Brentwood, NY 11717

October __, 2022

Re: Your Shareholder Account with (ISSUER NAME)

Dear [SHAREHOLDER NAME]

Broadridge is the Transfer Agent for (ISSUER NAME), and we keep records of your stock ownership on behalf of (ISSUER NAME). We are writing to alert you to an issue with your account that may require your immediate attention. While your account is secure, our records indicate that someone may have tried to access your account without your authority. This letter provides you with information regarding the actions Broadridge has taken to safeguard your data and steps you can take to remain vigilant in monitoring your personal data going forward. Please take the time to read this important notice and contact us with questions you may have.

What Happened?

An online profile within our Shareholder Portal (<https://investor.broadridge.com/>) was opened in connection with your [ISSUER NAME] account. Based on a review of the circumstances surrounding the establishment of the online profile, we suspect that this was not an action that you initiated.

What activity was involved?

Data about you was used to attempt to set up an online profile in our Transfer Agent system. This was accomplished using your Name, Address, Account Number, and Social Security Number. The setup process also involves the presentation of, and correct responses to, personal identification information in the form of challenge questions.

What are we Doing?

We have taken measures designed to protect your information from further incident. As a precaution, we deleted your online profile that was created and have opened a new account for you. All historical information has been migrated into this new account. We also reported this matter to the Federal Bureau of Investigation and we will cooperate with law enforcement in seeking to identify the perpetrators. We have also notified the Attorney General of your State. A statement will be mailed to you under separate cover.

What Can You Do?

We have arranged for you to enroll, at no cost to you, in an online three-bureau credit monitoring service for 12 months provided by Experian. We advise you to remain vigilant by reviewing account statements and monitoring free credit reports. Privacy laws do not allow us to register you for credit monitoring directly. To enroll in this service please follow the steps set forth in the attachment.

We take the security of your information in our care very seriously. If you have any questions regarding the foregoing or your shareholder account, please contact us at [____].

Sincerely,

Tara Altman

Vice President, Head of Client Experience

EXPERIAN CREDIT MONITORING

To enroll in Experian Credit Monitoring, please follow these steps:

- Ensure that you **enroll by**: January 31, 2023 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll:
<https://www.experianidworks.com/3bplus>
- Provide your **activation code**:

If you have questions about this product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **877-890-9332** by January 31, 2023. Be prepared to provide engagement number **B079109** as proof of eligibility for the identity restoration services by Experian.

Here are some additional details regarding your 12-month Experian IdentityWorks Membership:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only. Offline members will be eligible to call for additional reports quarterly after enrolling.
- **Credit Monitoring:** Actively monitors Experian, Equifax and TransUnion files for indicators of fraud.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance:**¹ Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at **877-890-9332**. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition). Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site. We recommend you remain vigilant for incidents of fraud and identity theft by reviewing your credit card account statements and monitoring your credit report for unauthorized activities. Finally, please review the enclosed attachment called *Preventing Identity Theft and Fraud* for more information on ways to protect against the potential misuse of your information.

¹ The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.



Broadridge Corporate Issuer Solutions
PO BOX 1342
Brentwood, NY 11717

PREVENTING IDENTITY THEFT AND FRAUD

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Immediately report any suspicious activity to your bank or credit union. If you do find suspicious activity on your credit reports or other statements, call your local police or sheriff's office or state Attorney General and file a report of identity theft. You have a right to a copy of the police report, and you may need to give copies of the police report to creditors to clear up your records and to access some services that are free to identity theft victims.

Under the U.S. Fair Credit Reporting Act and other laws, you have certain rights that can help protect yourself from identity theft. Many of these are explained in this document and at www.identitytheft.gov/Know-Your-Rights. For example, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call toll-free 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

At no charge, you can have these credit bureaus place a short-term or an extended "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

General contact information for each agency:

Equifax

P.O. Box 105069
Atlanta, GA 30348-5069
(800) 525-6285
www.equifax.com

Experian

P.O. Box 9554
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion

P.O. Box 2000
Chester, PA 19016-2000
800-680-7289
www.transunion.com

To add a fraud alert:

Equifax (888) 202-4025, Option 6 or <https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>

Experian (714) 830-7000, Option 2 or <https://www.experian.com/fraud/center.html>

TransUnion (800) 916-8800, Option 0 or <https://www.transunion.com/fraud-alerts>

You may also place a security freeze on your credit reports, free of charge. A security freeze, also known as a "credit freeze," prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised 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, credit mortgages, employment, housing, or other services. But unlike a fraud alert, you must separately place a security freeze on your credit file at **each** bureau. You can use the following addresses and contact information to place a security freeze with each major credit bureau:

Equifax Security Freeze. 1-800-685-1111. P.O. Box 1057881, Atlanta, GA 30348-0241.
www.equifax.com/personal/credit-report-services/credit-freeze/;

Experian Security Freeze. 1-888-EXPERIAN or 1-888-397-3742. P.O. Box 9554, Allen, TX 75013.
www.experian.com/freeze/center.html; or



Broadridge Corporate Issuer Solutions
PO BOX 1342
Brentwood, NY 11717

TransUnion. 1-800-680-7289. Fraud Victim Assistance Division, P.O. Box 2000, Chester, PA 19022-2000. www.transunion.com/credit-freeze

The Federal Trade Commission also provides additional information about credit freezes here:
<https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs>.

In order to request a security freeze, you may need to supply your full name (including middle initial, as well as Jr., Sr., II, III, etc.), date of birth, Social Security number, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or other statement to show proof of your current address. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning your identity theft.

The credit reporting agencies must place a security freeze on your credit report within one (1) business day after receiving a request by phone or secure electronic means, and within (3) business days after receiving your request by mail. The credit bureaus must then send written confirmation to you within five (5) business days of placing the security freeze, along with information about how to remove or lift the security freeze in the future.

You can further educate yourself regarding identity theft, fraud alerts, freezes, and the steps you can take to protect yourself by contacting the Federal Trade Commission or your state Attorney General. The Federal Trade Commission encourages those who discover their information has been misused to file a complaint with them. Instances of known or suspected identity theft should be reported to law enforcement or your state Attorney General as well.

The Federal Trade Commission can be reached at:

Federal Trade Commission
Consumer Resource Center
600 Pennsylvania Avenue NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.identitytheft.gov or www.ftc.gov

OTHER IMPORTANT INFORMATION

You may also file a report with your local police or the police in the community where identity theft, if any, took place. Further, you are entitled to request a copy of the police report filed in this matter.