



Robert K. Jamieson
Direct Dial: 813.347.5110
rjamieson@guerraking.com

July 13, 2022

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

Dear Office of the Attorney General,

I represent Trade-PMR, Inc. (“TradePMR”) a FINRA registered broker-dealer (CRD No. 46350) located at 2511 NW 41st Street Gainesville, FL 32606. The firm has been licensed in the state of Maryland since June 1999. This letter is provided pursuant to Md. Code Ann. Comm. Law § 14-3504 to notify you of a potential breach of the security of certain computerized data owned by the firm.

Nature of the Data Event

On March 16, 2022, TradePMR identified suspicious email activity (suspected phishing emails) that appeared to originate from a TradePMR employee email account. Suspecting that an unauthorized user may have gained access to the account, the firm immediately terminated access to the email account as a precaution. A third-party specialist was then engaged to investigate and analyze the suspicious activity, and to determine the nature and scope of any potential data security breach.

That investigation showed that an unauthorized user – whose identity is unknown – gained access to the subject email account for approximately one to two hours before TradePMR shut it down. The investigation also determined that the unauthorized user sent a small number of phishing emails from the account to external recipients during the period of access, though there has been no evidence that any of the phishing attempts were successful. There was insufficient evidence available in the analysis to determine whether the unauthorized user was able to view or acquire any electronic data during the window of access such that the security, confidentiality, or integrity of any personally identifiable information contained therein would be compromised. Further, the firm is not currently aware of any indications that the unauthorized user has physical

possession of, has downloaded or copied, has used, or has made public any such electronic data or personally identifiable information.

Nevertheless, out of an abundance of caution, TradePMR undertook measures necessary to determine the scope of the potential data security breach in the event that the unauthorized user was able to view or acquire any computerized data that might compromise the security, confidentiality, or integrity of any personal information. From the firm's review and analysis of all data associated with the email account, together with its own internal records – which was completed on June 10, 2022 – the firm discovered that there are twelve Maryland residents whose personal information (social security numbers and driver's license number) could have potentially been viewed or acquired from the electronic data associated with the email account.

Since the data event TradePMR has instituted additional technical and administrative measures to strengthen the existing security of its email accounts, and it is in the process of evaluating and implementing additional technical and administrative measures to further increase email security.

Notice to Residents

Written notice of this potential data security breach is being mailed to the affected Maryland residents on this day, July 13, 2022. A sample of the notice mailed to those residents is enclosed with this letter.

Contact Information

Should you have any questions regarding this notification or other aspects of the above data event, please contact me at (813) 347-5110.

Very truly yours,

/s/ Robert K. Jamieson

Robert K. Jamieson

RKJ/nac
Enclosure



Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

July 13, 2022

i0885-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345



SAMPLE A SAMPLE - L01 GENERAL
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789



Notice of Data Breach

Dear Sample A. Sample,

We appreciate the opportunity to service your brokerage account and recognize the importance of maintaining the privacy of your personal information. Therefore, as a precautionary measure, we are writing to let you know about a data security incident that may involve some of your personal information. We also wanted to tell you about the steps we are taking to protect your information going forward and notify you about steps you can take to protect your personal information.

What Happened and What Information was Involved?

On March 16, 2022, we identified suspicious activity that appeared to originate from an internal email account. Suspecting that an unauthorized user may have gained access, we immediately terminated the account and rendered it inoperable. We then engaged specialists to investigate and analyze the account activity, and to determine whether any personal information may have been viewed or acquired by any unauthorized individuals.

From that investigation it was determined that an unknown user had circumvented our existing security measures and accessed the account in question for a period of a few hours. There was insufficient evidence available to determine whether the unknown user was able to actually view or acquire any personal information contained within the email account during the brief window of access.

Nevertheless, out of an abundance of caution, we undertook an extensive review of all data associated with the email account in the event that the unknown user was able to view or acquire any personal information. That review was completed on June 10, 2022. Although we have found no specific evidence that any of your information has been viewed, acquired, or misused as a result of the email intrusion, our review of the data revealed that your name and [Extra1] may have been exposed.

What We Are Doing.

As soon as we suspected a possible intrusion, we took steps to terminate access to the affected email account. This limited the window of access to a very brief period. We have already instituted additional technical and administrative measures to strengthen the existing security of our email accounts and protect your brokerage account(s), and we are in the process of evaluating and implementing additional measures to further strengthen our security. These measures will help to prevent a similar event from occurring in the future.

0000001



i0885-L01

In addition, while we are not currently aware of any misuse of your information, to help protect your identity we are offering a complimentary 24-month membership of Experian's® IdentityWorksSM which provides superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: September 30th, 2022 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/credit
- Provide your **activation code**: **ABCDEFGHI**

If you have questions about the product or 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 September 30th, 2022 on Monday through Friday 8 am – 10 pm CST, Saturday and Sunday 10 am – 7 pm CST (excluding major U.S. holidays). Be prepared to provide engagement number **B055215** as proof of eligibility for the identity restoration services by Experian.

What You Can Do.

The safety of your personal information is one of our highest priorities and, while there is no evidence at this time that your information has been viewed, taken, or misused in any way, there are steps that you can take to protect yourself going forward. In addition to taking advantage of the complimentary credit monitoring services being offered through Experian, we recommend that you remain vigilant for incidents of fraud and identity theft. This includes regularly reviewing your account activity and monitoring free credit reports. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or suspected incident of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission. For additional information about ways in which you can help protect yourself, please review the enclosed *Additional Information*.

For More Information:

We understand that you may have questions regarding this data event that are not addressed in this letter. If you have questions or would like additional information, please call TradePMR toll-free at (833) 618-7233 or email us at dataprotection@tradepmr.com

Sincerely,

James J. Halvosa

James J. Halvosa, CCO

Trade-PMR, Inc.

Mail: PO Box 358230, Gainesville FL 32635-8230
Packages: 2511 NW 41st Street, Gainesville FL 32606
(352) 332-8723 ♦ (888) 723-3767 ♦ Fax (352) 331-5830
www.TradePMR.com
Member FINRA/SIPC

Additional Information

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 4500, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-680-7289

Free Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies by visiting www.annualcreditreport.com, or calling toll-free at 1-877-322-8228. You can also mail a completed Annual Credit Report Request Form to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. (forms available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>)

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze prohibits a credit reporting agency from releasing information from a consumer's credit report without written authorization. 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, credit mortgages, employment, housing, or other services. To place a security freeze, you need to make a request to each of the three major consumer reporting agencies. You may make that request by certified mail, overnight mail, regular mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze: (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable report or complaint with a law enforcement agency. The request must also include a copy of a government-issued ID card and proof of current address, such as a recent utility bill, rental agreement, or deed. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. Under federal law, you cannot be charged to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 1-800-349-9960
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>

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

TransUnion Security Freeze P.O. Box 160 Woodlyn, PA 19094 1-800-909-8872
www.transunion.com/creditfreeze

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with:

- Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf);
- TransUnion (<https://www.transunion.com/fraud-alerts>); or
- Experian (<https://www.experian.com/fraud/center.html>).



A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. An initial fraud alert is free and lasts for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are listed above.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

File Police Report: Instances of known or suspected identity theft should be reported to law enforcement or the Attorney General. You have the right to file or obtain a police report if you experience identity fraud. Please note that to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General at consumer@ag.iowa.gov, by calling (515) 281-5926, or writing to 1305 E. Walnut Street Des Moines, Iowa 50319-0106.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General at <https://doj.state.or.us>, by calling (877) 877-9392, or writing to Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint using the contact information listed above.

For Connecticut residents: You may contact the Office of the Attorney General at 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

For District of Columbia residents: You may contact the Office of the Attorney General at 400 6th Street NW, Washington, D.C. 20001, (202) 727-3400, and oag@dc.gov

For Maryland residents: You may contact the Office of the Attorney General at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, and www.oag.state.md.us

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. Information about your rights pursuant to the Fair Credit Reporting Act is available at https://files.consumerfinance.gov/f/201410_cfpb_summary_your-rights-under-fcra.pdf

For North Carolina residents: You may contact the Office of the Attorney General at 9001 Mail Service Center, Raleigh, NC 27699- 9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov

For New York residents: You may contact the Office of the Attorney General at Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, and <https://ag.ny.gov/>

For Rhode Island residents: You may contact the Office of the Attorney General at 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.

