

From: Abby Mallek <amallek@tankstar.com>
Sent: Tuesday, October 8, 2024 4:35 PM
To: IDTheft
Subject: PRIVILEGED AND CONFIDENTIAL: Data Security Incident potentially involving MD residents
Attachments: TSI Notice of Data Security Incident to Employees (10.8.24).pdf
Follow Up Flag: Follow up
Flag Status: Flagged
Categories: Data breach

To Whom It May Concern,

On September 20th, 2024, unusual activity was detected on our company servers. It was eventually determined that our company was targeted by ransomware. While our IT team, assisted by an outside cybersecurity team, acted quickly to neutralize the threat, there is a chance the attackers acquired some of our data, and that data may have included personal information of employees. Therefore, we will send out the following Notice to everyone potentially affected, which includes (to our knowledge) the 23 Maryland residents under our employment. Further details, including the compromised information and steps the business is taking, are outlined in the Notice.

Please let me know if I need to take any additional steps to comply with Maryland's Personal Information Protection Act (PIPA).

Thank you.

Abby Mallek
In-House Counsel
Tankstar USA, Inc.
611 South 28th Street
Milwaukee, WI 53215
414-671-8075 Direct Dial



October 8, 2024

Notice of Data Security Incident

Dear Employee,

On behalf of its subsidiaries, Tankstar USA, Inc. ("Tankstar") is writing to inform you of a recent data security incident that resulted in unauthorized access to company data. While we have no evidence of fraudulent misuse of your personal information at this time, we want to be fully transparent and act out of an abundance of caution. Thus, we are providing you with details about the incident, the steps we are taking in response, and resources available to help you protect against any potential misuse of your personal information. Please be assured that Tankstar is committed to the protection of your data and takes this matter very seriously.

What Happened:

On September 20, 2024, Tankstar detected suspicious activity on certain company systems. In response, Tankstar immediately shut down its data network and engaged forensic specialists in cybersecurity and data privacy to investigate further. Through this investigation, Tankstar discovered that an unauthorized third party potentially accessed and acquired certain files during this incident.

What Information Was Involved:

At this time, Tankstar is unable to confirm the exact nature of the data that may have been accessed during the incident. However, based on the information available, we believe that some or all of the following data may have been subject to unauthorized access and acquisition: your name, address, Social Security number, date of birth, and driver's license number.

What We Are Doing:

Tankstar takes this incident and our responsibility to protect your personal information very seriously. Upon discovery of the incident, we immediately engaged an outside cybersecurity team and moved quickly to investigate, respond, and confirm the security of our systems. Additionally, Tankstar has taken proactive steps to prevent future incidents by resetting user credentials, enhancing our security protocols, and deploying advanced monitoring techniques.

As part of Tankstar's ongoing commitment to protecting your personal information, we are offering complimentary credit monitoring services through Aura for one year. If you wish to enroll, please contact us within 120 days to receive your unique activation code.



To enroll:

1. Call us at 414-671-8077 to obtain your unique code.
2. Once you have your code, visit <https://aura.com/activate>.
3. Follow the on-screen instructions to create your account.
4. Set up protection from your Aura dashboard.

For questions about the credit monitoring service or assistance with setup, you may also contact Aura directly at 1-833-552-2123.

We encourage you to take advantage of this offer to help protect your personal information.

What You Can Do:

Tankstar encourages you to remain vigilant in safeguarding your personal information against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such an incident and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file. Please review the enclosed *Steps You Can Take to Protect Your Information* to learn more about how to protect against the possibility of information misuse.

For More Information:

You may still feel the need to speak with Tankstar regarding this incident. If so, please call our legal department at 414-671-8077, email us at legal@tankstar.com, or write to us at 611 S. 28th Street, Milwaukee, WI 53215.

At Tankstar, we take our responsibility to protect your personal information very seriously. We trust that our transparency and the complimentary monitoring service we are offering demonstrate our continued commitment to your security. We apologize for any inconvenience this data security incident may have caused.

Yours Truly,

A handwritten signature in black ink, appearing to read "Jack P. Schwerman".

Jack Schwerman
President

Enclosure (1)

Steps You Can Take to Protect Your Information

1. Credit Reports. You may obtain a free copy of your credit report from each of the three major credit reporting agencies (Equifax, Experian, and TransUnion) once every 12 months by visiting <https://www.annualcreditreport.com>, by calling toll-free 877- 322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348.

2. Fraud Alerts. Place a fraud alert on your credit files by contacting each of the three reporting agencies. A fraud alert tells creditors to contact you personally before they open any new accounts. You may place a fraud alert by contacting any one or more of the following three agencies:

Equifax	Experian	TransUnion
(800) 525-6285 www.equifax.com/personal/credit-report-services/credit-fraud-alerts/ P.O. Box 105069 Atlanta, GA 105069	(888) 397-3742 www.experian.com/fraud/center.html P.O. Box 9554 Allen, TX 75013	(800) 680-7289 www.transunion.com/fraud-alerts P.O. Box 2000 Chester, PA 19016

3. Security Freezes. Place a security freeze on your credit files by contacting each of the three credit reporting agencies. Freezing credit files will prevent someone from using your personal information to open new accounts or borrow money in your name. Please understand that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card unless you lift the freeze temporarily or permanently. You may place a security freeze by contacting any one or more of the following three agencies:

Equifax	Experian	TransUnion
(888) 298-0045 www.equifax.com/personal/credit-report-services/credit-freeze/ P.O. Box 105788 Atlanta, GA 30348	(888) 397-3742 www.experian.com/freeze/center.html P.O. Box 9554 Allen, TX 75013	(888) 909-8872 www.transunion.com/credit-freeze P.O. Box 160 Woodlyn, PA 19094

4. Monitoring. Remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and by monitoring your credit report for suspicious or unusual activity.

5. File Police Report. If your personal information has been used to file a false tax return, to open an account or 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.

6. FTC and Attorney 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.

Take advantage of additional free resources on identity theft. We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at <https://consumer.ftc.gov/identity-theft-and-online-security>

Report incidents of suspected identity theft to the Federal Trade Commission, and your state attorney general. Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies. Information on how to contact your state attorney general may be found at www.naag.org/naag/attorneys-general/whos-my-ag.php.

For Illinois residents, you may obtain information about preventing identity theft from the Illinois Office of the Attorney General, 100 W Randolph Street, Chicago IL 60601, by calling 1-866-999-5630 or visiting their website at www.illinoisattorneygeneral.gov.

For Maryland residents, you may obtain information about preventing identity theft from the Maryland Office of the Attorney General, 200 St. Paul Place, Baltimore MD 21202, by calling 1-888-743-0023 or visiting their website at www.marylandattorneygeneral.gov.

For North Carolina residents, you may obtain information about preventing identity theft from the North Carolina Office of the Attorney General- Consumer Protecting Division, 9001 Mail Service Center, Raleigh NC 27699, by calling 1-877-566-4400 or visiting their website at www.ncdoj.gov.

For New York residents, you may obtain information about preventing identity theft from the New York Office of the Attorney General- Consumer Frauds & Protection, The Capitol, Albany NY 12224, by calling 1-800-771-7755 or visiting their website at www.ag.ny.gov.