Anjali C. Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

September 15, 2025

Via Online Portal:

Attorney General Nick Brown
Washington Attorney General's Office
1125 Washington St SE
PO Box 40100
Olympia, WA 98504

Re: Notice of Cybersecurity Incident

Dear Attorney General Brown:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents Trusteed Plans Service Corporation ("TPSC"), a custom health benefit solution provider for corporate employers located at 1101 Pacific Ave, Tacoma, Washington, with respect to a recent cybersecurity incident that was first discovered by TPSC on December 26, 2024 (hereinafter, the "Incident"). TPSC takes the security and privacy of the information in its control very seriously and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the Incident, what information may have been compromised, the number of Washington residents being notified, and the steps that TPSC has taken in response to the Incident. We have also enclosed hereto a sample of the notice letter mailed to the potentially impacted individuals, which includes an offer for complimentary credit monitoring services.

1. Nature of the Incident

On December 26, 2024, TPSC detected unusual activity within its computer environment. Upon discovery of this Incident, TPSC promptly engaged a specialized third-party cybersecurity firm to secure its computer systems and conduct a comprehensive investigation to determine the initial cause and scope of the Incident. The forensic investigation determined that an unauthorized user gained access and obtained information from within TPSC's environment.

Based on the findings of the forensic investigation, TPSC conducted a data mining exercise with the assistance of a third-party vendor to identify the individuals impacted and the specific types of information that may have been acquired by the unauthorized user. The data mining exercise was completed on August 7, 2025. Upon completion of the data mining project TPSC took the time necessary to obtain the contact information for the impacted individuals and engage a third-party notification vendor to provide affected individuals with complimentary credit monitoring services to help secure their personal information.

Although TPSC is unaware of any fraudulent misuse of information, it is possible that individuals' names, addresses, dates birth, Social Security numbers, health insurance information, medical treatment information, medical diagnosis information, medical procedure information, Medicare/Medicaid numbers, may have been exposed as a result of this unauthorized activity.

As of this writing, TPSC has not received any reports of related identity theft since the date of the incident (December 26, 2024, to present).

2. Number of Washington residents affected.

Based on its investigation, TPSC identified and notified 13,659 Washington residents whose information was impacted as a result of the Incident. Notification letters to these individuals were mailed on September 15, 2025, by U.S. First Class Mail. A sample copy of the notification letter is included with this letter under **Exhibit A**.

3. Steps taken in response to the Incident.

TPSC is committed to ensuring the security and privacy of all personal information in its control and is taking steps to prevent a similar incident from occurring in the future. Upon discovery of the Incident, TPSC moved quickly to investigate and respond to the Incident, assessed the security of its systems, and notified the potentially affected individuals. Further, TPSC implemented the following security measures to prevent a similar incident from occurring in the future: upgraded desktop operating systems, increased firewall security, further implementation of multi-factor authentication, deployed additional security agents to monitor server and desktop activity, engaged third-party vendor for internal assessments and external penetration testing, and encrypted data at rest.

Although TPSC is not aware of any actual or attempted misuse of the affected personal information, TPSC offered twelve (12) months of complimentary credit monitoring and identity theft restoration services through HaystackID to Washington residents to help protect their identity. Additionally, TPSC provided guidance on how to better protect against identity theft and fraud, including providing information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and the contact details for the Federal Trade Commission.

4. Contact information

TPSC remains dedicated to protecting the sensitive information within its control. Should you have any questions or need additional information, please do not hesitate to contact me at Anjali.Das@WilsonElser.com or 312-821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Anjali C. Das

EXHIBIT A

Trusteed Plans Service Corp.
c/o HaystackID
PO Box 5012
Branchburg NJ 08876

0000009**000002*****SCH 5-DIGIT 98206*****000002**000002

REDACTED

0000009

September 15, 2025

Notice of Data Security Incident

Dear Parent/Guardian of REDACTED,

Trusteed Plans Service Corporation ("TPSC") is writing to inform you of a recent data security incident that may have resulted in unauthorized access to your child's personal information. TPSC collected yours and your child's information for purposes of processing custom healthcare benefit solutions for your plan sponsor/health plan, which provides certain health and welfare benefits. While we are unaware of any fraudulent misuse of your child's personal information at this time, we are providing you with details about the incident, steps we are taking in response, and resources available to help you protect against the potential misuse of your child's information.

What Happened?

On December 26, 2024, TPSC detected unusual activity within its computer environment. Upon discovery of this Incident, TPSC promptly engaged a specialized third-party cybersecurity firm to secure its computer systems and conduct a comprehensive investigation to determine the initial cause and scope of the unauthorized activity. The forensic investigation determined that an unauthorized user gained access and obtained information from within TPSC's environment.

Based on the findings of the forensic investigation, TPSC conducted a data mining exercise with the assistance of a third-party vendor to identify the specific individuals impacted and the specific types of information that may have been acquired by the unauthorized user. The data mining exercise was completed on August 7, 2025. Following its review of the data mining results, TPSC contacted your plan sponsor/ health plan to report that your information may have been impacted as a result of the incident. We are now providing you with this related notice.

Please note that, to date, the investigation has found no evidence of actual or attempted misuse of information as a result of this incident.

What Information Was Involved?

Although TPSC has no evidence that any personal information has been misused by the unauthorized user or any other third parties as a result of this incident, we are notifying you for purposes of full transparency. Based on the forensic investigation, the following information related to you may have been subject to unauthorized access: REDACTED.

What We Are Doing

Data privacy and security are among TPSC's highest priorities, and we are committed to doing everything we can to protect the privacy and security of the personal information within our care. Since the discovery of the incident, TPSC moved quickly to investigate, respond, and confirm the security of our systems. Specifically, TPSC disconnected all access to our network, changed administrative credentials, restored operations in a safe and secure mode, enhanced the security measures, and took steps (and will continue to take steps) to mitigate the risk of future harm.

In response to the incident, we are providing you with access to **Cyber Monitoring** services for you and your minor child for 12 months at no charge. Cyber monitoring will look out for your and your child's personal data on the dark web and alert you if your personally identifiable information or your child's is found online. These services will be provided by HaystackID; a company specializing in fraud assistance and remediation services.

What You Can Do

To enroll in the free Cyber Monitoring services, please log on to REDACTED and follow the instructions provided. When prompted please provide the following unique code to receive services: REDACTED.

Once you have enrolled yourself, click on your name in the top right of your dashboard and select "Manage Family Protection" then "Add Family Member" to enroll your child. In order for you to receive the monitoring services described above, you must enroll within ninety (90) days from the date of this letter. The enrollment requires an internet connection and e-mail account. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

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 or unauthorized activity. Additionally, security experts suggest that you contact your financial institutions and all major credit bureaus to inform them of the incident and then take whatever steps are recommended to protect yours and your child's interests, including the possible placement of a fraud alert or freeze on your and your child's credit file. Please review the enclosed resource, *ADDITIONAL RESOURCES TO HELP PROTECT YOUR CHILD'S INFORMATION*, to learn more about how to protect against the possibility of personal information misuse.

We would like to reiterate that, at this time, there is no evidence that your child's personal information was misused. However, we encourage you to take full advantage of the services offered.

For More Information

If you have any questions or concerns not addressed in this letter, please call 888.844.0928 (toll free) during the hours of 9:00 am to 9:00 pm Eastern time, Monday through Friday and 9:00 am to 6:00 pm Saturday (excluding U.S. national holidays).

TPSC sincerely regrets any concern or inconvenience this matter may cause and remains dedicated to ensuring the privacy and security of all information in our control.

Sincerely,

Trusteed Plans Service Corporation

ADDITIONAL RESOURCES TO HELP PROTECT YOUR CHILD'S INFORMATION

Monitor Your Accounts We recommend that you remain vigilant for incidents of fraud or identity theft by regularly reviewing your credit reports and financial accounts for any suspicious activity. You should contact the reporting agency using the phone number on the credit report if you find any inaccuracies with your information or if you do not recognize any of the account activity.

You may obtain a free copy of your credit report by visiting www.annualcreditreport.com, calling toll-free at 1-877-322-8228, or by mailing a completed Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report for a fee by contacting one or more of the three national credit reporting agencies.

You have rights under the federal Fair Credit Reporting Act (FCRA). The FCRA governs the collection and use of information about you that is reported by consumer reporting agencies. You can obtain additional information about your rights under the FCRA by visiting https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act.

Credit Freeze You have the right to add, temporarily lift and remove a credit freeze, also known as a security freeze, on your credit report at no cost. A credit freeze prevents all third parties, such as credit lenders or other companies, whose use is not exempt under law, from accessing your credit file without your consent. If you have a freeze, you must remove or temporarily lift it to apply for credit. Spouses can request freezes for each other as long as they pass authentication. You can also request a freeze for someone if you have a valid Power of Attorney. If you are a parent/guardian/representative you can request a freeze for a minor 15 and younger. To add a security freeze on your credit report you must make a separate request to each of the three national consumer reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The following information must be included when requesting a security freeze: (i) full name, with middle initial and any suffixes; (ii) Social Security number; (iii) date of birth (month, day, and year); (iv) current address and any previous addresses for the past five (5) years; (v) proof of current address (such as a copy of a government-issued identification card, a recent utility or telephone bill, or bank or insurance statement); and (vi) other personal information as required by the applicable credit reporting agency.

Fraud Alert You have the right to add, extend, or remove a fraud alert on your credit file at no cost. A fraud alert is a statement that is added to your credit file that will notify potential credit grantors that you may be or have been a victim of identity theft. Before they extend credit, they should use reasonable procedures to verify your identity. Please note that, unlike a credit freeze, a fraud alert only notifies lenders to verify your identity before extending new credit, but it does not block access to your credit report. Fraud alerts are free to add and are valid for one year. Victims of identity theft can obtain an extended fraud alert for seven years. You can add a fraud alert by sending your request to any one of the three national reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The agency you contact will then contact the other credit agencies.

Federal Trade Commission For more information about credit freezes and fraud alerts and other steps you can take to protect yourself against identity theft, you can contact the Federal Trade Commission (FTC) 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 by way of the contact information listed above.

You should also report instances of known or suspected identity theft to local law enforcement and the Attorney General's office in your home state and you have the right to file a police report and obtain a copy of your police report.

You may also review helpful sites to learn more about medical identity theft. Helpful information may be found in the Federal Trade Commission's What to Know About Medical Identity Theft Article for consumers, which can be found at https://consumer.ftc.gov/articles/what-know-about-medical-identity-theft.

Contact Information Below is the contact information for the three national credit reporting agencies (Experian, Equifax, and TransUnion) if you would like to add a fraud alert or credit freeze to your credit report.

Credit Reporting Agency	Access Your Credit Report	Add a Fraud Alert	Add a Security Freeze
Experian	P.O. Box 2002 Allen, TX 75013-9701 1-866-200-6020 www.experian.com	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 https://www.experian.com/fraud/center.html	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 www.experian.com/freeze/center.html
Equifax	P.O. Box 740241 Atlanta, GA 30374-0241 1-866-349-5191 www.equifax.com	P.O. Box 105069 Atlanta, GA 30348-5069 1-800-525-6285 www.equifax.com/personal/credit-report-services/credit-fraud-alerts	P.O. Box 105788 Atlanta, GA 30348-5788 1-888-298-0045 www.equifax.com/personal/credit--report-services

TransUnion	P.O. Box 1000 Chester, PA 19016-1000 1-800-888-4213 www.transunion.com	P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-alerts	P.O. Box 160 Woodlyn, PA 19094 1-800-916-8800 www.transunion.com/credit-freeze

Iowa and Oregon residents are advised to report suspected incidents of identity theft to local law enforcement, to their respective Attorney General, and the FTC.

Massachusetts residents are advised of their right to obtain a police report in connection with this incident.

District of Columbia residents are advised of their right to obtain a security freeze free of charge and can obtain information about steps to take to avoid identity theft by contacting the FTC (contact information provided above) and the Office of the Attorney General for the District of Columbia, Office of Consumer Protection, at 400 6th St. NW, Washington, D.C. 20001, by calling the Consumer Protection Hotline at (202) 442-9828, by visiting https://oag.dc.gov, or emailing at consumer.protection@dc.gov.

Maryland residents can obtain information about steps they can take to avoid identity theft by contacting the FTC (contact information provided above) or the Maryland Office of the Attorney General, Consumer Protection Division Office at 44 North Potomac Street, Suite 104, Hagerstown, MD 21740, by phone at 1-888-743-0023 or 410-528-8662, or by visiting http://www.marylandattorneygeneral.gov/Pages/contactus.aspx.

New Mexico residents, state law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach.

New York residents are advised that in response to this incident they can place a fraud alert or security freeze on their credit reports and may report any incidents of suspected identity theft to law enforcement, the FTC, the New York Attorney General, or local law enforcement. Additional information is available at the website of the New York Department of State Division of Consumer Protection at https://dos.nysits.acsitefactory.com/consumerprotection; by visiting the New York Attorney General at https://ag/ny.gov or by phone at 1-800-771-7755; or by contacting the FTC at www.ftc.gov/bcp/edu/microsites/idtheft/ or https://www.identitytheft.gov/#/.

North Carolina residents are advised to remain vigilant by reviewing account statements and monitoring free credit reports and may obtain information about preventing identity theft by contacting the FTC (contact information provided above) or the North Carolina Office of the Attorney General, Consumer Protection Division at 9001 Mail Service Center, Raleigh, NC 27699-9001, or visiting www.ncdoj.gov, or by phone at 1-877-5-NO-SCAM (1-877-566-7226) or (919) 7166000.

Rhode Island residents are advised that they may file or obtain a police report in connection with this incident and place a security freeze on their credit file and that fees may be required to be paid to the consumer reporting agencies.

Trusteed Plans Service Corp.
c/o HaystackID
PO Box 5012
Branchburg NJ 08876

0000001**000001*****ALL FOR AADC 070*****000001**000001

0000001

REDACTED

September 15, 2025

Notice of Data Security Incident

Dear REDACTED

Trusteed Plans Service Corporation ("TPSC") is writing to inform you of a recent data security incident that may have resulted in unauthorized access to your personal information. TPSC collected your information for purposes of processing custom healthcare benefit solutions for your plan sponsor/health plan, which provides certain health and welfare benefits. While we are unaware of any fraudulent misuse of your personal information at this time, we are providing you with details about the incident, steps we are taking in response, and resources available to help you protect against the potential misuse of your information.

What Happened?

On December 26, 2024, TPSC detected unusual activity within its computer environment. Upon discovery of this Incident, TPSC promptly engaged a specialized third-party cybersecurity firm to secure its computer systems and conduct a comprehensive investigation to determine the initial cause and scope of the unauthorized activity. The forensic investigation determined that an unauthorized user gained access and obtained information from within TPSC's environment.

Based on the findings of the forensic investigation, TPSC conducted a data mining exercise with the assistance of a third-party vendor to identify the specific individuals impacted and the specific types of information that may have been acquired by the unauthorized user. The data mining exercise was completed on August 7, 2025. Following its review of the data mining results, TPSC contacted your plan sponsor/ health plan to report that your information may have been impacted as a result of the incident. We are now providing you with this related notice.

Please note that, to date, the investigation has found no evidence of actual or attempted misuse of information as a result of this incident.

What Information Was Involved?

Although TPSC has no evidence that any personal information has been misused by the unauthorized user or any other third parties as a result of this incident, we are notifying you for purposes of full transparency. Based on the forensic investigation, the following information related to you may have been subject to unauthorized access: REDACTED REDACTED

What We Are Doing

Data privacy and security are among TPSC's highest priorities, and we are committed to doing everything we can to protect the privacy and security of the personal information within our care. Since the discovery of the incident, TPSC moved quickly to investigate, respond, and confirm the security of our systems. Specifically, TPSC disconnected all access to our network, changed administrative credentials, restored operations in a safe and secure mode, enhanced the security measures, and took steps (and will continue to take steps) to mitigate the risk of future harm.

In light of the incident, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for 12 months months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the single bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by HaystackID, a company specializing in fraud assistance and remediation services.

What You Can Do

To enroll in the free Credit Monitoring services noted above, please log on to REDACTED and follow the instructions provided. When prompted, please provide the following unique code to receive services: REDACTED. In order for you to receive the monitoring services described above, you must enroll within ninety (90) days from the date of this letter. Enrollment requires an internet connection and e-mail address and may not be available to minors under the age of eighteen (18) years of age. Please note that, when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

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 or unauthorized activity. Additionally, security experts suggest that you contact your financial institutions and all major credit bureaus to inform them of the incident and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert or freeze on your credit file. Please review the enclosed resource, *ADDITIONAL RESOURCES TO HELP PROTECT YOUR INFORMATION*, to learn more about how to protect against the possibility of personal information misuse.

We would like to reiterate that, at this time, there is no evidence that your personal information was misused. However, we encourage you to take full advantage of the services offered.

For More Information

If you have any questions or concerns not addressed in this letter, please call 888.844.0928 (toll free) during the hours of 9:00 am to 9:00 pm Eastern time, Monday through Friday and 9:00 am to 6:00 pm Saturday (excluding U.S. national holidays).

TPSC sincerely regrets any concern or inconvenience this matter may cause and remains dedicated to ensuring the privacy and security of all information in our control.

Sincerely,

Trusteed Plans Service Corporation

ADDITIONAL RESOURCES TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts We recommend that you remain vigilant for incidents of fraud or identity theft by regularly reviewing your credit reports and financial accounts for any suspicious activity. You should contact the reporting agency using the phone number on the credit report if you find any inaccuracies with your information or if you do not recognize any of the account activity.

You may obtain a free copy of your credit report by visiting www.annualcreditreport.com, calling toll-free at 1-877-322-8228, or by mailing a completed Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report for a fee by contacting one or more of the three national credit reporting agencies.

You have rights under the federal Fair Credit Reporting Act (FCRA). The FCRA governs the collection and use of information about you that is reported by consumer reporting agencies. You can obtain additional information about your rights under the FCRA by visiting https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act.

Credit Freeze You have the right to add, temporarily lift and remove a credit freeze, also known as a security freeze, on your credit report at no cost. A credit freeze prevents all third parties, such as credit lenders or other companies, whose use is not exempt under law, from accessing your credit file without your consent. If you have a freeze, you must remove or temporarily lift it to apply for credit. Spouses can request freezes for each other as long as they pass authentication. You can also request a freeze for someone if you have a valid Power of Attorney. If you are a parent/guardian/representative you can request a freeze for a minor 15 and younger. To add a security freeze on your credit report you must make a separate request to each of the three national consumer reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The following information must be included when requesting a security freeze: (i) full name, with middle initial and any suffixes; (ii) Social Security number; (iii) date of birth (month, day, and year); (iv) current address and any previous addresses for the past five (5) years; (v) proof of current address (such as a copy of a government-issued identification card, a recent utility or telephone bill, or bank or insurance statement); and (vi) other personal information as required by the applicable credit reporting agency.

Fraud Alert You have the right to add, extend, or remove a fraud alert on your credit file at no cost. A fraud alert is a statement that is added to your credit file that will notify potential credit grantors that you may be or have been a victim of identity theft. Before they extend credit, they should use reasonable procedures to verify your identity. Please note that, unlike a credit freeze, a fraud alert only notifies lenders to verify your identity before extending new credit, but it does not block access to your credit report. Fraud alerts are free to add and are valid for one year. Victims of identity theft can obtain an extended fraud alert for seven years. You can add a fraud alert by sending your request to any one of the three national reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The agency you contact will then contact the other credit agencies.

Federal Trade Commission For more information about credit freezes and fraud alerts and other steps you can take to protect yourself against identity theft, you can contact the Federal Trade Commission (FTC) 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 by way of the contact information listed above.

You should also report instances of known or suspected identity theft to local law enforcement and the Attorney General's office in your home state and you have the right to file a police report and obtain a copy of your police report.

You may also review helpful sites to learn more about medical identity theft. Helpful information may be found in the Federal Trade Commission's What to Know About Medical Identity Theft Article for consumers, which can be found at https://consumer.ftc.gov/articles/what-know-about-medical-identity-theft.

Contact Information Below is the contact information for the three national credit reporting agencies (Experian, Equifax, and TransUnion) if you would like to add a fraud alert or credit freeze to your credit report.

Credit Reporting Agency	Access Your Credit Report	Add a Fraud Alert	Add a Security Freeze
Experian	P.O. Box 2002 Allen, TX 75013-9701 1-866-200-6020 www.experian.com	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 https://www.experian.com/fraud/center.html	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 www.experian.com/freeze/center.html
Equifax	P.O. Box 740241 Atlanta, GA 30374-0241 1-866-349-5191 www.equifax.com	P.O. Box 105069 Atlanta, GA 30348-5069 1-800-525-6285 www.equifax.com/personal/credit-report-services/credit-fraud-alerts	P.O. Box 105788 Atlanta, GA 30348-5788 1-888-298-0045 www.equifax.com/personal/credit--report-services

TransUnion	P.O. Box 1000 Chester, PA 19016-1000 1-800-888-4213 www.transunion.com	P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-alerts	P.O. Box 160 Woodlyn, PA 19094 1-800-916-8800 www.transunion.com/credit-freeze

Iowa and Oregon residents are advised to report suspected incidents of identity theft to local law enforcement, to their respective Attorney General, and the FTC.

Massachusetts residents are advised of their right to obtain a police report in connection with this incident.

District of Columbia residents are advised of their right to obtain a security freeze free of charge and can obtain information about steps to take to avoid identity theft by contacting the FTC (contact information provided above) and the Office of the Attorney General for the District of Columbia, Office of Consumer Protection, at 400 6th St. NW, Washington, D.C. 20001, by calling the Consumer Protection Hotline at (202) 442-9828, by visiting https://oag.dc.gov, or emailing at consumer.protection@dc.gov.

Maryland residents can obtain information about steps they can take to avoid identity theft by contacting the FTC (contact information provided above) or the Maryland Office of the Attorney General, Consumer Protection Division Office at 44 North Potomac Street, Suite 104, Hagerstown, MD 21740, by phone at 1-888-743-0023 or 410-528-8662, or by visiting http://www.marylandattorneygeneral.gov/Pages/contactus.aspx.

New Mexico residents, state law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach.

New York residents are advised that in response to this incident they can place a fraud alert or security freeze on their credit reports and may report any incidents of suspected identity theft to law enforcement, the FTC, the New York Attorney General, or local law enforcement. Additional information is available at the website of the New York Department of State Division of Consumer Protection at https://dos.nysits.acsitefactory.com/consumerprotection; by visiting the New York Attorney General at https://ag/ny.gov or by phone at 1-800-771-7755; or by contacting the FTC at www.ftc.gov/bcp/edu/microsites/idtheft/ or https://www.identitytheft.gov/#/.

North Carolina residents are advised to remain vigilant by reviewing account statements and monitoring free credit reports and may obtain information about preventing identity theft by contacting the FTC (contact information provided above) or the North Carolina Office of the Attorney General, Consumer Protection Division at 9001 Mail Service Center, Raleigh, NC 27699-9001, or visiting www.ncdoj.gov, or by phone at 1-877-5-NO-SCAM (1-877-566-7226) or (919) 7166000.

Rhode Island residents are advised that they may file or obtain a police report in connection with this incident and place a security freeze on their credit file and that fees may be required to be paid to the consumer reporting agencies.

Trusteed Plans Service Corp.
c/o HaystackID
PO Box 5012
Branchburg NJ 08876

0001084**000005*****SCH 5-DIGIT 98233*****000002**000002

REDACTED

0001084

September 15, 2025

Notice of Data Security Incident

Dear Representative of the Estate of REDACTED

Trusteed Plans Service Corporation ("TPSC") is writing to inform you of a recent data security incident that may have resulted in unauthorized access to the deceased's personal information. TPSC collected the deceased's information for purposes of processing custom healthcare benefit solutions for plan sponsors/health plans that provide certain health and welfare benefits. While we are unaware of any fraudulent misuse of the deceased's personal information at this time, we are providing you with details about the incident, steps we are taking in response, and resources available to help you protect against the potential misuse of the deceased's information.

What Happened?

On December 26, 2024, TPSC detected unusual activity within its computer environment. Upon discovery of this Incident, TPSC promptly engaged a specialized third-party cybersecurity firm to secure its computer systems and conduct a comprehensive investigation to determine the initial cause and scope of the unauthorized activity. The forensic investigation determined that an unauthorized user gained access and obtained information from within TPSC's environment.

Based on the findings of the forensic investigation, TPSC conducted a data mining exercise with the assistance of a third-party vendor to identify the specific individuals impacted and the specific types of information that may have been acquired by the unauthorized user. The data mining exercise was completed on August 7, 2025. Following its review of the data mining results, TPSC contacted the plan sponsor/ health plan to report that the deceased's information may have been impacted as a result of the incident. We are now providing you with this related notice.

Please note that, to date, the investigation has found no evidence of actual or attempted misuse of information as a result of this incident.

What Information Was Involved?

Although TPSC has no evidence that any personal information has been misused by the unauthorized user or any other third parties as a result of this incident, we are notifying you for purposes of full transparency. Based on the forensic investigation, the following information related to the deceased may have been subject to unauthorized access: REDACTED

REDACTED

What We Are Doing

Data privacy and security are among TPSC's highest priorities, and we are committed to doing everything we can to protect the privacy and security of the personal information within our care. Since the discovery of the incident, TPSC moved quickly to investigate, respond, and confirm the security of our systems. Specifically, TPSC disconnected all access to our network, changed administrative credentials, restored operations in a safe and secure mode, enhanced the security measures, and took steps (and will continue to take steps) to mitigate the risk of future harm.

In response to the incident, we are providing you with access to **Cyber Monitoring** services for the deceased at no charge. These services provide you with alerts for 12 months from the date of enrollment. Cyber monitoring will look out for the deceased's personal data on the dark web and alert you if the deceased's personally identifiable information is found online. These services will be provided by HaystackID; a company specializing in fraud assistance and remediation services.

What You Can Do

To enroll in the free Cyber Monitoring services, please log on to REDACTED and follow the instructions provided. When prompted please provide the following unique code to receive services: REDACTED

In order for you to receive the monitoring services described above, you must enroll within ninety (90) days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of eighteen (18) years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information to confirm your identity for the protection of the deceased's estate.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review the deceased's account statements, and to monitor the deceased's credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact the deceased's financial institutions and all major credit bureaus to inform them of the incident and then take whatever steps are recommended to protect the deceased's interests. Please review the enclosed resource, *ADDITIONAL RESOURCES TO HELP PROTECT THE DECEASED'S INFORMATION*, to learn more about how to protect against the possibility of personal information misuse.

We would like to reiterate that, at this time, there is no evidence that the deceased's personal information was misused. However, we encourage you to take full advantage of the services offered.

For More Information

If you have any questions or concerns not addressed in this letter, please call 888.844.0928 (toll free) during the hours of 9:00 am to 9:00 pm Eastern time, Monday through Friday and 9:00 am to 6:00 pm Saturday (excluding U.S. national holidays).

TPSC sincerely regrets any concern or inconvenience this matter may cause and remains dedicated to ensuring the privacy and security of all information in our control.

Sincerely,

Trusteed Plans Service Corporation

ADDITIONAL RESOURCES TO HELP PROTECT THE DECEASED'S INFORMATION

Monitor Your Accounts We recommend that you remain vigilant for incidents of fraud or identity theft by regularly reviewing your credit reports and financial accounts for any suspicious activity. You should contact the reporting agency using the phone number on the credit report if you find any inaccuracies with your information or if you do not recognize any of the account activity.

You may obtain a free copy of your credit report by visiting www.annualcreditreport.com, calling toll-free at 1-877-322-8228, or by mailing a completed Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report for a fee by contacting one or more of the three national credit reporting agencies.

You have rights under the federal Fair Credit Reporting Act (FCRA). The FCRA governs the collection and use of information about you that is reported by consumer reporting agencies. You can obtain additional information about your rights under the FCRA by visiting https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act.

Credit Freeze You have the right to add, temporarily lift and remove a credit freeze, also known as a security freeze, on your credit report at no cost. A credit freeze prevents all third parties, such as credit lenders or other companies, whose use is not exempt under law, from accessing your credit file without your consent. If you have a freeze, you must remove or temporarily lift it to apply for credit. Spouses can request freezes for each other as long as they pass authentication. You can also request a freeze for someone if you have a valid Power of Attorney. If you are a parent/guardian/representative you can request a freeze for a minor 15 and younger. To add a security freeze on your credit report you must make a separate request to each of the three national consumer reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The following information must be included when requesting a security freeze: (i) full name, with middle initial and any suffixes; (ii) Social Security number; (iii) date of birth (month, day, and year); (iv) current address and any previous addresses for the past five (5) years; (v) proof of current address (such as a copy of a government-issued identification card, a recent utility or telephone bill, or bank or insurance statement); and (vi) other personal information as required by the applicable credit reporting agency.

Fraud Alert You have the right to add, extend, or remove a fraud alert on your credit file at no cost. A fraud alert is a statement that is added to your credit file that will notify potential credit grantors that you may be or have been a victim of identity theft. Before they extend credit, they should use reasonable procedures to verify your identity. Please note that, unlike a credit freeze, a fraud alert only notifies lenders to verify your identity before extending new credit, but it does not block access to your credit report. Fraud alerts are free to add and are valid for one year. Victims of identity theft can obtain an extended fraud alert for seven years. You can add a fraud alert by sending your request to any one of the three national reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The agency you contact will then contact the other credit agencies.

Federal Trade Commission For more information about credit freezes and fraud alerts and other steps you can take to protect yourself against identity theft, you can contact the Federal Trade Commission (FTC) 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 by way of the contact information listed above.

You should also report instances of known or suspected identity theft to local law enforcement and the Attorney General's office in your home state and you have the right to file a police report and obtain a copy of your police report.

You may also review helpful sites to learn more about medical identity theft. Helpful information may be found in the Federal Trade Commission's What to Know About Medical Identity Theft Article for consumers, which can be found at https://consumer.ftc.gov/articles/what-know-about-medical-identity-theft.

Contact Information Below is the contact information for the three national credit reporting agencies (Experian, Equifax, and TransUnion) if you would like to add a fraud alert or credit freeze to your credit report.

Credit Reporting Agency	Access Your Credit Report	Add a Fraud Alert	Add a Security Freeze
Experian	P.O. Box 2002 Allen, TX 75013-9701 1-866-200-6020 www.experian.com	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 https://www.experian.com/fraud/center.html	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 www.experian.com/freeze/center.html
Equifax	P.O. Box 740241 Atlanta, GA 30374-0241 1-866-349-5191 www.equifax.com	P.O. Box 105069 Atlanta, GA 30348-5069 1-800-525-6285 www.equifax.com/personal/credit-report-services/credit-fraud-alerts	P.O. Box 105788 Atlanta, GA 30348-5788 1-888-298-0045 www.equifax.com/personal/credit--report-services

TransUnion	P.O. Box 1000 Chester, PA 19016-1000 1-800-888-4213 www.transunion.com	P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-alerts	P.O. Box 160 Woodlyn, PA 19094 1-800-916-8800 www.transunion.com/credit-freeze

Iowa and Oregon residents are advised to report suspected incidents of identity theft to local law enforcement, to their respective Attorney General, and the FTC.

Massachusetts residents are advised of their right to obtain a police report in connection with this incident.

District of Columbia residents are advised of their right to obtain a security freeze free of charge and can obtain information about steps to take to avoid identity theft by contacting the FTC (contact information provided above) and the Office of the Attorney General for the District of Columbia, Office of Consumer Protection, at 400 6th St. NW, Washington, D.C. 20001, by calling the Consumer Protection Hotline at (202) 442-9828, by visiting https://oag.dc.gov, or emailing at consumer.protection@dc.gov.

Maryland residents can obtain information about steps they can take to avoid identity theft by contacting the FTC (contact information provided above) or the Maryland Office of the Attorney General, Consumer Protection Division Office at 44 North Potomac Street, Suite 104, Hagerstown, MD 21740, by phone at 1-888-743-0023 or 410-528-8662, or by visiting http://www.marylandattorneygeneral.gov/Pages/contactus.aspx.

New Mexico residents, state law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach.

New York residents are advised that in response to this incident they can place a fraud alert or security freeze on their credit reports and may report any incidents of suspected identity theft to law enforcement, the FTC, the New York Attorney General, or local law enforcement. Additional information is available at the website of the New York Department of State Division of Consumer Protection at https://dos.nysits.acsitefactory.com/consumerprotection; by visiting the New York Attorney General at https://ag/ny.gov or by phone at 1-800-771-7755; or by contacting the FTC at www.ftc.gov/bcp/edu/microsites/idtheft/ or https://www.identitytheft.gov/#/.

North Carolina residents are advised to remain vigilant by reviewing account statements and monitoring free credit reports and may obtain information about preventing identity theft by contacting the FTC (contact information provided above) or the North Carolina Office of the Attorney General, Consumer Protection Division at 9001 Mail Service Center, Raleigh, NC 27699-9001, or visiting www.ncdoj.gov, or by phone at 1-877-5-NO-SCAM (1-877-566-7226) or (919) 7166000.

Rhode Island residents are advised that they may file or obtain a police report in connection with this incident and place a security freeze on their credit file and that fees may be required to be paid to the consumer reporting agencies.

Anjali C. Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

September 15, 2025

Via Online Portal:

Attorney General Nick Brown
Washington Attorney General's Office
1125 Washington St SE
PO Box 40100
Olympia, WA 98504

Re: Notice of Cybersecurity Incident

Dear Attorney General Brown:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents Trusteed Plans Service Corporation ("TPSC"), a custom health benefit solution provider for corporate employers located at 1101 Pacific Ave, Tacoma, Washington, with respect to a recent cybersecurity incident that was first discovered by TPSC on December 26, 2024 (hereinafter, the "Incident"). TPSC takes the security and privacy of the information in its control very seriously and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the Incident, what information may have been compromised, the number of Washington residents being notified, and the steps that TPSC has taken in response to the Incident. We have also enclosed hereto a sample of the notice letter mailed to the potentially impacted individuals, which includes an offer for complimentary credit monitoring services.

1. Nature of the Incident

On December 26, 2024, TPSC detected unusual activity within its computer environment. Upon discovery of this Incident, TPSC promptly engaged a specialized third-party cybersecurity firm to secure its computer systems and conduct a comprehensive investigation to determine the initial cause and scope of the Incident. The forensic investigation determined that an unauthorized user gained access and obtained information from within TPSC's environment.

Based on the findings of the forensic investigation, TPSC conducted a data mining exercise with the assistance of a third-party vendor to identify the individuals impacted and the specific types of information that may have been acquired by the unauthorized user. The data mining exercise was completed on August 7, 2025. Upon completion of the data mining project TPSC took the time necessary to obtain the contact information for the impacted individuals and engage a third-party notification vendor to provide affected individuals with complimentary credit monitoring services to help secure their personal information.

Although TPSC is unaware of any fraudulent misuse of information, it is possible that individuals' names, addresses, dates birth, Social Security numbers, health insurance information, medical treatment information, medical diagnosis information, medical procedure information, Medicare/Medicaid numbers, may have been exposed as a result of this unauthorized activity.

As of this writing, TPSC has not received any reports of related identity theft since the date of the incident (December 26, 2024, to present).

2. Number of Washington residents affected.

Based on its investigation, TPSC identified and notified 13,659 Washington residents whose information was impacted as a result of the Incident. Notification letters to these individuals were mailed on September 15, 2025, by U.S. First Class Mail. A sample copy of the notification letter is included with this letter under **Exhibit A**.

3. Steps taken in response to the Incident.

TPSC is committed to ensuring the security and privacy of all personal information in its control and is taking steps to prevent a similar incident from occurring in the future. Upon discovery of the Incident, TPSC moved quickly to investigate and respond to the Incident, assessed the security of its systems, and notified the potentially affected individuals. Further, TPSC implemented the following security measures to prevent a similar incident from occurring in the future: upgraded desktop operating systems, increased firewall security, further implementation of multi-factor authentication, deployed additional security agents to monitor server and desktop activity, engaged third-party vendor for internal assessments and external penetration testing, and encrypted data at rest.

Although TPSC is not aware of any actual or attempted misuse of the affected personal information, TPSC offered twelve (12) months of complimentary credit monitoring and identity theft restoration services through HaystackID to Washington residents to help protect their identity. Additionally, TPSC provided guidance on how to better protect against identity theft and fraud, including providing information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and the contact details for the Federal Trade Commission.

4. Contact information

TPSC remains dedicated to protecting the sensitive information within its control. Should you have any questions or need additional information, please do not hesitate to contact me at Anjali.Das@WilsonElser.com or 312-821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Anjali C. Das

EXHIBIT A

Trusteed Plans Service Corp.
c/o HaystackID
PO Box 5012
Branchburg NJ 08876

0000009**000002*****SCH 5-DIGIT 98206*****000002**000002

REDACTED

0000009

September 15, 2025

Notice of Data Security Incident

Dear Parent/Guardian of REDACTED,

Trusteed Plans Service Corporation ("TPSC") is writing to inform you of a recent data security incident that may have resulted in unauthorized access to your child's personal information. TPSC collected yours and your child's information for purposes of processing custom healthcare benefit solutions for your plan sponsor/health plan, which provides certain health and welfare benefits. While we are unaware of any fraudulent misuse of your child's personal information at this time, we are providing you with details about the incident, steps we are taking in response, and resources available to help you protect against the potential misuse of your child's information.

What Happened?

On December 26, 2024, TPSC detected unusual activity within its computer environment. Upon discovery of this Incident, TPSC promptly engaged a specialized third-party cybersecurity firm to secure its computer systems and conduct a comprehensive investigation to determine the initial cause and scope of the unauthorized activity. The forensic investigation determined that an unauthorized user gained access and obtained information from within TPSC's environment.

Based on the findings of the forensic investigation, TPSC conducted a data mining exercise with the assistance of a third-party vendor to identify the specific individuals impacted and the specific types of information that may have been acquired by the unauthorized user. The data mining exercise was completed on August 7, 2025. Following its review of the data mining results, TPSC contacted your plan sponsor/ health plan to report that your information may have been impacted as a result of the incident. We are now providing you with this related notice.

Please note that, to date, the investigation has found no evidence of actual or attempted misuse of information as a result of this incident.

What Information Was Involved?

Although TPSC has no evidence that any personal information has been misused by the unauthorized user or any other third parties as a result of this incident, we are notifying you for purposes of full transparency. Based on the forensic investigation, the following information related to you may have been subject to unauthorized access: REDACTED.

What We Are Doing

Data privacy and security are among TPSC's highest priorities, and we are committed to doing everything we can to protect the privacy and security of the personal information within our care. Since the discovery of the incident, TPSC moved quickly to investigate, respond, and confirm the security of our systems. Specifically, TPSC disconnected all access to our network, changed administrative credentials, restored operations in a safe and secure mode, enhanced the security measures, and took steps (and will continue to take steps) to mitigate the risk of future harm.

In response to the incident, we are providing you with access to **Cyber Monitoring** services for you and your minor child for 12 months at no charge. Cyber monitoring will look out for your and your child's personal data on the dark web and alert you if your personally identifiable information or your child's is found online. These services will be provided by HaystackID; a company specializing in fraud assistance and remediation services.

What You Can Do

To enroll in the free Cyber Monitoring services, please log on to REDACTED and follow the instructions provided. When prompted please provide the following unique code to receive services: REDACTED.

Once you have enrolled yourself, click on your name in the top right of your dashboard and select "Manage Family Protection" then "Add Family Member" to enroll your child. In order for you to receive the monitoring services described above, you must enroll within ninety (90) days from the date of this letter. The enrollment requires an internet connection and e-mail account. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

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 or unauthorized activity. Additionally, security experts suggest that you contact your financial institutions and all major credit bureaus to inform them of the incident and then take whatever steps are recommended to protect yours and your child's interests, including the possible placement of a fraud alert or freeze on your and your child's credit file. Please review the enclosed resource, *ADDITIONAL RESOURCES TO HELP PROTECT YOUR CHILD'S INFORMATION*, to learn more about how to protect against the possibility of personal information misuse.

We would like to reiterate that, at this time, there is no evidence that your child's personal information was misused. However, we encourage you to take full advantage of the services offered.

For More Information

If you have any questions or concerns not addressed in this letter, please call 888.844.0928 (toll free) during the hours of 9:00 am to 9:00 pm Eastern time, Monday through Friday and 9:00 am to 6:00 pm Saturday (excluding U.S. national holidays).

TPSC sincerely regrets any concern or inconvenience this matter may cause and remains dedicated to ensuring the privacy and security of all information in our control.

Sincerely,

Trusteed Plans Service Corporation

ADDITIONAL RESOURCES TO HELP PROTECT YOUR CHILD'S INFORMATION

Monitor Your Accounts We recommend that you remain vigilant for incidents of fraud or identity theft by regularly reviewing your credit reports and financial accounts for any suspicious activity. You should contact the reporting agency using the phone number on the credit report if you find any inaccuracies with your information or if you do not recognize any of the account activity.

You may obtain a free copy of your credit report by visiting www.annualcreditreport.com, calling toll-free at 1-877-322-8228, or by mailing a completed Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report for a fee by contacting one or more of the three national credit reporting agencies.

You have rights under the federal Fair Credit Reporting Act (FCRA). The FCRA governs the collection and use of information about you that is reported by consumer reporting agencies. You can obtain additional information about your rights under the FCRA by visiting https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act.

Credit Freeze You have the right to add, temporarily lift and remove a credit freeze, also known as a security freeze, on your credit report at no cost. A credit freeze prevents all third parties, such as credit lenders or other companies, whose use is not exempt under law, from accessing your credit file without your consent. If you have a freeze, you must remove or temporarily lift it to apply for credit. Spouses can request freezes for each other as long as they pass authentication. You can also request a freeze for someone if you have a valid Power of Attorney. If you are a parent/guardian/representative you can request a freeze for a minor 15 and younger. To add a security freeze on your credit report you must make a separate request to each of the three national consumer reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The following information must be included when requesting a security freeze: (i) full name, with middle initial and any suffixes; (ii) Social Security number; (iii) date of birth (month, day, and year); (iv) current address and any previous addresses for the past five (5) years; (v) proof of current address (such as a copy of a government-issued identification card, a recent utility or telephone bill, or bank or insurance statement); and (vi) other personal information as required by the applicable credit reporting agency.

Fraud Alert You have the right to add, extend, or remove a fraud alert on your credit file at no cost. A fraud alert is a statement that is added to your credit file that will notify potential credit grantors that you may be or have been a victim of identity theft. Before they extend credit, they should use reasonable procedures to verify your identity. Please note that, unlike a credit freeze, a fraud alert only notifies lenders to verify your identity before extending new credit, but it does not block access to your credit report. Fraud alerts are free to add and are valid for one year. Victims of identity theft can obtain an extended fraud alert for seven years. You can add a fraud alert by sending your request to any one of the three national reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The agency you contact will then contact the other credit agencies.

Federal Trade Commission For more information about credit freezes and fraud alerts and other steps you can take to protect yourself against identity theft, you can contact the Federal Trade Commission (FTC) 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 by way of the contact information listed above.

You should also report instances of known or suspected identity theft to local law enforcement and the Attorney General's office in your home state and you have the right to file a police report and obtain a copy of your police report.

You may also review helpful sites to learn more about medical identity theft. Helpful information may be found in the Federal Trade Commission's What to Know About Medical Identity Theft Article for consumers, which can be found at https://consumer.ftc.gov/articles/what-know-about-medical-identity-theft.

Contact Information Below is the contact information for the three national credit reporting agencies (Experian, Equifax, and TransUnion) if you would like to add a fraud alert or credit freeze to your credit report.

Credit Reporting Agency	Access Your Credit Report	Add a Fraud Alert	Add a Security Freeze
Experian	P.O. Box 2002 Allen, TX 75013-9701 1-866-200-6020 www.experian.com	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 https://www.experian.com/fraud/center.html	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 www.experian.com/freeze/center.html
Equifax	P.O. Box 740241 Atlanta, GA 30374-0241 1-866-349-5191 www.equifax.com	P.O. Box 105069 Atlanta, GA 30348-5069 1-800-525-6285 www.equifax.com/personal/credit-report-services/credit-fraud-alerts	P.O. Box 105788 Atlanta, GA 30348-5788 1-888-298-0045 www.equifax.com/personal/credit--report-services

TransUnion	P.O. Box 1000 Chester, PA 19016-1000 1-800-888-4213 www.transunion.com	P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-alerts	P.O. Box 160 Woodlyn, PA 19094 1-800-916-8800 www.transunion.com/credit-freeze

Iowa and Oregon residents are advised to report suspected incidents of identity theft to local law enforcement, to their respective Attorney General, and the FTC.

Massachusetts residents are advised of their right to obtain a police report in connection with this incident.

District of Columbia residents are advised of their right to obtain a security freeze free of charge and can obtain information about steps to take to avoid identity theft by contacting the FTC (contact information provided above) and the Office of the Attorney General for the District of Columbia, Office of Consumer Protection, at 400 6th St. NW, Washington, D.C. 20001, by calling the Consumer Protection Hotline at (202) 442-9828, by visiting https://oag.dc.gov, or emailing at consumer.protection@dc.gov.

Maryland residents can obtain information about steps they can take to avoid identity theft by contacting the FTC (contact information provided above) or the Maryland Office of the Attorney General, Consumer Protection Division Office at 44 North Potomac Street, Suite 104, Hagerstown, MD 21740, by phone at 1-888-743-0023 or 410-528-8662, or by visiting http://www.marylandattorneygeneral.gov/Pages/contactus.aspx.

New Mexico residents, state law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach.

New York residents are advised that in response to this incident they can place a fraud alert or security freeze on their credit reports and may report any incidents of suspected identity theft to law enforcement, the FTC, the New York Attorney General, or local law enforcement. Additional information is available at the website of the New York Department of State Division of Consumer Protection at https://dos.nysits.acsitefactory.com/consumerprotection; by visiting the New York Attorney General at https://ag/ny.gov or by phone at 1-800-771-7755; or by contacting the FTC at www.ftc.gov/bcp/edu/microsites/idtheft/ or https://www.identitytheft.gov/#/.

North Carolina residents are advised to remain vigilant by reviewing account statements and monitoring free credit reports and may obtain information about preventing identity theft by contacting the FTC (contact information provided above) or the North Carolina Office of the Attorney General, Consumer Protection Division at 9001 Mail Service Center, Raleigh, NC 27699-9001, or visiting www.ncdoj.gov, or by phone at 1-877-5-NO-SCAM (1-877-566-7226) or (919) 7166000.

Rhode Island residents are advised that they may file or obtain a police report in connection with this incident and place a security freeze on their credit file and that fees may be required to be paid to the consumer reporting agencies.

Trusteed Plans Service Corp.
c/o HaystackID
PO Box 5012
Branchburg NJ 08876

0000001**000001*****ALL FOR AADC 070*****000001**000001

0000001

REDACTED

September 15, 2025

Notice of Data Security Incident

Dear REDACTED

Trusteed Plans Service Corporation ("TPSC") is writing to inform you of a recent data security incident that may have resulted in unauthorized access to your personal information. TPSC collected your information for purposes of processing custom healthcare benefit solutions for your plan sponsor/health plan, which provides certain health and welfare benefits. While we are unaware of any fraudulent misuse of your personal information at this time, we are providing you with details about the incident, steps we are taking in response, and resources available to help you protect against the potential misuse of your information.

What Happened?

On December 26, 2024, TPSC detected unusual activity within its computer environment. Upon discovery of this Incident, TPSC promptly engaged a specialized third-party cybersecurity firm to secure its computer systems and conduct a comprehensive investigation to determine the initial cause and scope of the unauthorized activity. The forensic investigation determined that an unauthorized user gained access and obtained information from within TPSC's environment.

Based on the findings of the forensic investigation, TPSC conducted a data mining exercise with the assistance of a third-party vendor to identify the specific individuals impacted and the specific types of information that may have been acquired by the unauthorized user. The data mining exercise was completed on August 7, 2025. Following its review of the data mining results, TPSC contacted your plan sponsor/ health plan to report that your information may have been impacted as a result of the incident. We are now providing you with this related notice.

Please note that, to date, the investigation has found no evidence of actual or attempted misuse of information as a result of this incident.

What Information Was Involved?

Although TPSC has no evidence that any personal information has been misused by the unauthorized user or any other third parties as a result of this incident, we are notifying you for purposes of full transparency. Based on the forensic investigation, the following information related to you may have been subject to unauthorized access: REDACTED REDACTED

What We Are Doing

Data privacy and security are among TPSC's highest priorities, and we are committed to doing everything we can to protect the privacy and security of the personal information within our care. Since the discovery of the incident, TPSC moved quickly to investigate, respond, and confirm the security of our systems. Specifically, TPSC disconnected all access to our network, changed administrative credentials, restored operations in a safe and secure mode, enhanced the security measures, and took steps (and will continue to take steps) to mitigate the risk of future harm.

In light of the incident, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for 12 months months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the single bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by HaystackID, a company specializing in fraud assistance and remediation services.

What You Can Do

To enroll in the free Credit Monitoring services noted above, please log on to REDACTED and follow the instructions provided. When prompted, please provide the following unique code to receive services: REDACTED. In order for you to receive the monitoring services described above, you must enroll within ninety (90) days from the date of this letter. Enrollment requires an internet connection and e-mail address and may not be available to minors under the age of eighteen (18) years of age. Please note that, when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

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 or unauthorized activity. Additionally, security experts suggest that you contact your financial institutions and all major credit bureaus to inform them of the incident and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert or freeze on your credit file. Please review the enclosed resource, *ADDITIONAL RESOURCES TO HELP PROTECT YOUR INFORMATION*, to learn more about how to protect against the possibility of personal information misuse.

We would like to reiterate that, at this time, there is no evidence that your personal information was misused. However, we encourage you to take full advantage of the services offered.

For More Information

If you have any questions or concerns not addressed in this letter, please call 888.844.0928 (toll free) during the hours of 9:00 am to 9:00 pm Eastern time, Monday through Friday and 9:00 am to 6:00 pm Saturday (excluding U.S. national holidays).

TPSC sincerely regrets any concern or inconvenience this matter may cause and remains dedicated to ensuring the privacy and security of all information in our control.

Sincerely,

Trusteed Plans Service Corporation

ADDITIONAL RESOURCES TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts We recommend that you remain vigilant for incidents of fraud or identity theft by regularly reviewing your credit reports and financial accounts for any suspicious activity. You should contact the reporting agency using the phone number on the credit report if you find any inaccuracies with your information or if you do not recognize any of the account activity.

You may obtain a free copy of your credit report by visiting www.annualcreditreport.com, calling toll-free at 1-877-322-8228, or by mailing a completed Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report for a fee by contacting one or more of the three national credit reporting agencies.

You have rights under the federal Fair Credit Reporting Act (FCRA). The FCRA governs the collection and use of information about you that is reported by consumer reporting agencies. You can obtain additional information about your rights under the FCRA by visiting https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act.

Credit Freeze You have the right to add, temporarily lift and remove a credit freeze, also known as a security freeze, on your credit report at no cost. A credit freeze prevents all third parties, such as credit lenders or other companies, whose use is not exempt under law, from accessing your credit file without your consent. If you have a freeze, you must remove or temporarily lift it to apply for credit. Spouses can request freezes for each other as long as they pass authentication. You can also request a freeze for someone if you have a valid Power of Attorney. If you are a parent/guardian/representative you can request a freeze for a minor 15 and younger. To add a security freeze on your credit report you must make a separate request to each of the three national consumer reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The following information must be included when requesting a security freeze: (i) full name, with middle initial and any suffixes; (ii) Social Security number; (iii) date of birth (month, day, and year); (iv) current address and any previous addresses for the past five (5) years; (v) proof of current address (such as a copy of a government-issued identification card, a recent utility or telephone bill, or bank or insurance statement); and (vi) other personal information as required by the applicable credit reporting agency.

Fraud Alert You have the right to add, extend, or remove a fraud alert on your credit file at no cost. A fraud alert is a statement that is added to your credit file that will notify potential credit grantors that you may be or have been a victim of identity theft. Before they extend credit, they should use reasonable procedures to verify your identity. Please note that, unlike a credit freeze, a fraud alert only notifies lenders to verify your identity before extending new credit, but it does not block access to your credit report. Fraud alerts are free to add and are valid for one year. Victims of identity theft can obtain an extended fraud alert for seven years. You can add a fraud alert by sending your request to any one of the three national reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The agency you contact will then contact the other credit agencies.

Federal Trade Commission For more information about credit freezes and fraud alerts and other steps you can take to protect yourself against identity theft, you can contact the Federal Trade Commission (FTC) 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 by way of the contact information listed above.

You should also report instances of known or suspected identity theft to local law enforcement and the Attorney General's office in your home state and you have the right to file a police report and obtain a copy of your police report.

You may also review helpful sites to learn more about medical identity theft. Helpful information may be found in the Federal Trade Commission's What to Know About Medical Identity Theft Article for consumers, which can be found at https://consumer.ftc.gov/articles/what-know-about-medical-identity-theft.

Contact Information Below is the contact information for the three national credit reporting agencies (Experian, Equifax, and TransUnion) if you would like to add a fraud alert or credit freeze to your credit report.

Credit Reporting Agency	Access Your Credit Report	Add a Fraud Alert	Add a Security Freeze
Experian	P.O. Box 2002 Allen, TX 75013-9701 1-866-200-6020 www.experian.com	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 https://www.experian.com/fraud/center.html	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 www.experian.com/freeze/center.html
Equifax	P.O. Box 740241 Atlanta, GA 30374-0241 1-866-349-5191 www.equifax.com	P.O. Box 105069 Atlanta, GA 30348-5069 1-800-525-6285 www.equifax.com/personal/credit-report-services/credit-fraud-alerts	P.O. Box 105788 Atlanta, GA 30348-5788 1-888-298-0045 www.equifax.com/personal/credit--report-services

TransUnion	P.O. Box 1000 Chester, PA 19016-1000 1-800-888-4213 www.transunion.com	P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-alerts	P.O. Box 160 Woodlyn, PA 19094 1-800-916-8800 www.transunion.com/credit-freeze

Iowa and Oregon residents are advised to report suspected incidents of identity theft to local law enforcement, to their respective Attorney General, and the FTC.

Massachusetts residents are advised of their right to obtain a police report in connection with this incident.

District of Columbia residents are advised of their right to obtain a security freeze free of charge and can obtain information about steps to take to avoid identity theft by contacting the FTC (contact information provided above) and the Office of the Attorney General for the District of Columbia, Office of Consumer Protection, at 400 6th St. NW, Washington, D.C. 20001, by calling the Consumer Protection Hotline at (202) 442-9828, by visiting https://oag.dc.gov, or emailing at consumer.protection@dc.gov.

Maryland residents can obtain information about steps they can take to avoid identity theft by contacting the FTC (contact information provided above) or the Maryland Office of the Attorney General, Consumer Protection Division Office at 44 North Potomac Street, Suite 104, Hagerstown, MD 21740, by phone at 1-888-743-0023 or 410-528-8662, or by visiting http://www.marylandattorneygeneral.gov/Pages/contactus.aspx.

New Mexico residents, state law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach.

New York residents are advised that in response to this incident they can place a fraud alert or security freeze on their credit reports and may report any incidents of suspected identity theft to law enforcement, the FTC, the New York Attorney General, or local law enforcement. Additional information is available at the website of the New York Department of State Division of Consumer Protection at https://dos.nysits.acsitefactory.com/consumerprotection; by visiting the New York Attorney General at https://ag/ny.gov or by phone at 1-800-771-7755; or by contacting the FTC at www.ftc.gov/bcp/edu/microsites/idtheft/ or https://www.identitytheft.gov/#/.

North Carolina residents are advised to remain vigilant by reviewing account statements and monitoring free credit reports and may obtain information about preventing identity theft by contacting the FTC (contact information provided above) or the North Carolina Office of the Attorney General, Consumer Protection Division at 9001 Mail Service Center, Raleigh, NC 27699-9001, or visiting www.ncdoj.gov, or by phone at 1-877-5-NO-SCAM (1-877-566-7226) or (919) 7166000.

Rhode Island residents are advised that they may file or obtain a police report in connection with this incident and place a security freeze on their credit file and that fees may be required to be paid to the consumer reporting agencies.

Trusteed Plans Service Corp.
c/o HaystackID
PO Box 5012
Branchburg NJ 08876

0001084**000005*****SCH 5-DIGIT 98233*****000002**000002

REDACTED

0001084

September 15, 2025

Notice of Data Security Incident

Dear Representative of the Estate of REDACTED

Trusteed Plans Service Corporation ("TPSC") is writing to inform you of a recent data security incident that may have resulted in unauthorized access to the deceased's personal information. TPSC collected the deceased's information for purposes of processing custom healthcare benefit solutions for plan sponsors/health plans that provide certain health and welfare benefits. While we are unaware of any fraudulent misuse of the deceased's personal information at this time, we are providing you with details about the incident, steps we are taking in response, and resources available to help you protect against the potential misuse of the deceased's information.

What Happened?

On December 26, 2024, TPSC detected unusual activity within its computer environment. Upon discovery of this Incident, TPSC promptly engaged a specialized third-party cybersecurity firm to secure its computer systems and conduct a comprehensive investigation to determine the initial cause and scope of the unauthorized activity. The forensic investigation determined that an unauthorized user gained access and obtained information from within TPSC's environment.

Based on the findings of the forensic investigation, TPSC conducted a data mining exercise with the assistance of a third-party vendor to identify the specific individuals impacted and the specific types of information that may have been acquired by the unauthorized user. The data mining exercise was completed on August 7, 2025. Following its review of the data mining results, TPSC contacted the plan sponsor/ health plan to report that the deceased's information may have been impacted as a result of the incident. We are now providing you with this related notice.

Please note that, to date, the investigation has found no evidence of actual or attempted misuse of information as a result of this incident.

What Information Was Involved?

Although TPSC has no evidence that any personal information has been misused by the unauthorized user or any other third parties as a result of this incident, we are notifying you for purposes of full transparency. Based on the forensic investigation, the following information related to the deceased may have been subject to unauthorized access: REDACTED

REDACTED

What We Are Doing

Data privacy and security are among TPSC's highest priorities, and we are committed to doing everything we can to protect the privacy and security of the personal information within our care. Since the discovery of the incident, TPSC moved quickly to investigate, respond, and confirm the security of our systems. Specifically, TPSC disconnected all access to our network, changed administrative credentials, restored operations in a safe and secure mode, enhanced the security measures, and took steps (and will continue to take steps) to mitigate the risk of future harm.

In response to the incident, we are providing you with access to **Cyber Monitoring** services for the deceased at no charge. These services provide you with alerts for 12 months from the date of enrollment. Cyber monitoring will look out for the deceased's personal data on the dark web and alert you if the deceased's personally identifiable information is found online. These services will be provided by HaystackID; a company specializing in fraud assistance and remediation services.

What You Can Do

To enroll in the free Cyber Monitoring services, please log on to REDACTED and follow the instructions provided. When prompted please provide the following unique code to receive services: REDACTED

In order for you to receive the monitoring services described above, you must enroll within ninety (90) days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of eighteen (18) years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information to confirm your identity for the protection of the deceased's estate.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review the deceased's account statements, and to monitor the deceased's credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact the deceased's financial institutions and all major credit bureaus to inform them of the incident and then take whatever steps are recommended to protect the deceased's interests. Please review the enclosed resource, *ADDITIONAL RESOURCES TO HELP PROTECT THE DECEASED'S INFORMATION*, to learn more about how to protect against the possibility of personal information misuse.

We would like to reiterate that, at this time, there is no evidence that the deceased's personal information was misused. However, we encourage you to take full advantage of the services offered.

For More Information

If you have any questions or concerns not addressed in this letter, please call 888.844.0928 (toll free) during the hours of 9:00 am to 9:00 pm Eastern time, Monday through Friday and 9:00 am to 6:00 pm Saturday (excluding U.S. national holidays).

TPSC sincerely regrets any concern or inconvenience this matter may cause and remains dedicated to ensuring the privacy and security of all information in our control.

Sincerely,

Trusteed Plans Service Corporation

ADDITIONAL RESOURCES TO HELP PROTECT THE DECEASED'S INFORMATION

Monitor Your Accounts We recommend that you remain vigilant for incidents of fraud or identity theft by regularly reviewing your credit reports and financial accounts for any suspicious activity. You should contact the reporting agency using the phone number on the credit report if you find any inaccuracies with your information or if you do not recognize any of the account activity.

You may obtain a free copy of your credit report by visiting www.annualcreditreport.com, calling toll-free at 1-877-322-8228, or by mailing a completed Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report for a fee by contacting one or more of the three national credit reporting agencies.

You have rights under the federal Fair Credit Reporting Act (FCRA). The FCRA governs the collection and use of information about you that is reported by consumer reporting agencies. You can obtain additional information about your rights under the FCRA by visiting https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act.

Credit Freeze You have the right to add, temporarily lift and remove a credit freeze, also known as a security freeze, on your credit report at no cost. A credit freeze prevents all third parties, such as credit lenders or other companies, whose use is not exempt under law, from accessing your credit file without your consent. If you have a freeze, you must remove or temporarily lift it to apply for credit. Spouses can request freezes for each other as long as they pass authentication. You can also request a freeze for someone if you have a valid Power of Attorney. If you are a parent/guardian/representative you can request a freeze for a minor 15 and younger. To add a security freeze on your credit report you must make a separate request to each of the three national consumer reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The following information must be included when requesting a security freeze: (i) full name, with middle initial and any suffixes; (ii) Social Security number; (iii) date of birth (month, day, and year); (iv) current address and any previous addresses for the past five (5) years; (v) proof of current address (such as a copy of a government-issued identification card, a recent utility or telephone bill, or bank or insurance statement); and (vi) other personal information as required by the applicable credit reporting agency.

Fraud Alert You have the right to add, extend, or remove a fraud alert on your credit file at no cost. A fraud alert is a statement that is added to your credit file that will notify potential credit grantors that you may be or have been a victim of identity theft. Before they extend credit, they should use reasonable procedures to verify your identity. Please note that, unlike a credit freeze, a fraud alert only notifies lenders to verify your identity before extending new credit, but it does not block access to your credit report. Fraud alerts are free to add and are valid for one year. Victims of identity theft can obtain an extended fraud alert for seven years. You can add a fraud alert by sending your request to any one of the three national reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The agency you contact will then contact the other credit agencies.

Federal Trade Commission For more information about credit freezes and fraud alerts and other steps you can take to protect yourself against identity theft, you can contact the Federal Trade Commission (FTC) 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 by way of the contact information listed above.

You should also report instances of known or suspected identity theft to local law enforcement and the Attorney General's office in your home state and you have the right to file a police report and obtain a copy of your police report.

You may also review helpful sites to learn more about medical identity theft. Helpful information may be found in the Federal Trade Commission's What to Know About Medical Identity Theft Article for consumers, which can be found at https://consumer.ftc.gov/articles/what-know-about-medical-identity-theft.

Contact Information Below is the contact information for the three national credit reporting agencies (Experian, Equifax, and TransUnion) if you would like to add a fraud alert or credit freeze to your credit report.

Credit Reporting Agency	Access Your Credit Report	Add a Fraud Alert	Add a Security Freeze
Experian	P.O. Box 2002 Allen, TX 75013-9701 1-866-200-6020 www.experian.com	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 https://www.experian.com/fraud/center.html	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 www.experian.com/freeze/center.html
Equifax	P.O. Box 740241 Atlanta, GA 30374-0241 1-866-349-5191 www.equifax.com	P.O. Box 105069 Atlanta, GA 30348-5069 1-800-525-6285 www.equifax.com/personal/credit-report-services/credit-fraud-alerts	P.O. Box 105788 Atlanta, GA 30348-5788 1-888-298-0045 www.equifax.com/personal/credit--report-services

TransUnion	P.O. Box 1000 Chester, PA 19016-1000 1-800-888-4213 www.transunion.com	P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-alerts	P.O. Box 160 Woodlyn, PA 19094 1-800-916-8800 www.transunion.com/credit-freeze

Iowa and Oregon residents are advised to report suspected incidents of identity theft to local law enforcement, to their respective Attorney General, and the FTC.

Massachusetts residents are advised of their right to obtain a police report in connection with this incident.

District of Columbia residents are advised of their right to obtain a security freeze free of charge and can obtain information about steps to take to avoid identity theft by contacting the FTC (contact information provided above) and the Office of the Attorney General for the District of Columbia, Office of Consumer Protection, at 400 6th St. NW, Washington, D.C. 20001, by calling the Consumer Protection Hotline at (202) 442-9828, by visiting https://oag.dc.gov, or emailing at consumer.protection@dc.gov.

Maryland residents can obtain information about steps they can take to avoid identity theft by contacting the FTC (contact information provided above) or the Maryland Office of the Attorney General, Consumer Protection Division Office at 44 North Potomac Street, Suite 104, Hagerstown, MD 21740, by phone at 1-888-743-0023 or 410-528-8662, or by visiting http://www.marylandattorneygeneral.gov/Pages/contactus.aspx.

New Mexico residents, state law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach.

New York residents are advised that in response to this incident they can place a fraud alert or security freeze on their credit reports and may report any incidents of suspected identity theft to law enforcement, the FTC, the New York Attorney General, or local law enforcement. Additional information is available at the website of the New York Department of State Division of Consumer Protection at https://dos.nysits.acsitefactory.com/consumerprotection; by visiting the New York Attorney General at https://ag/ny.gov or by phone at 1-800-771-7755; or by contacting the FTC at www.ftc.gov/bcp/edu/microsites/idtheft/ or https://www.identitytheft.gov/#/.

North Carolina residents are advised to remain vigilant by reviewing account statements and monitoring free credit reports and may obtain information about preventing identity theft by contacting the FTC (contact information provided above) or the North Carolina Office of the Attorney General, Consumer Protection Division at 9001 Mail Service Center, Raleigh, NC 27699-9001, or visiting www.ncdoj.gov, or by phone at 1-877-5-NO-SCAM (1-877-566-7226) or (919) 7166000.

Rhode Island residents are advised that they may file or obtain a police report in connection with this incident and place a security freeze on their credit file and that fees may be required to be paid to the consumer reporting agencies.