

Sent on behalf of Atty. Sarah A. Sargent

Dear Attorney General Brown:

Our firm represents Manitou Equipment America, LLC and Manitou North America, LLC (“Manitou”), Wisconsin-based manufacturing companies. Manitou hereby formally submits notification of a recent data incident pursuant to Md. Code Com. Law § 14-3501 et seq. Manitou reserves the right to supplement this notice with any significant details learned subsequent to this submission. By providing this notice, Manitou does not waive any rights or defenses regarding the applicability of Maryland law, including the applicability of Md. Code Com. Law § 14-3501 et seq., the applicability of any other laws of this or any other state, or the existence of personal jurisdiction over Manitou.

On December 24, 2023, Manitou became aware that an unauthorized third party had gained access to some of Manitou’s systems and deployed ransomware on December 8, 2023. Immediately upon learning of the incident, Manitou isolated the impacted environment and began an investigation with the help of a leading forensic security firm that specializes in data security incidents to analyze the impacted data and identify potentially impacted individuals. After restoring its systems and servers, reviewing the results of the investigation, and assessing what information was impacted, Manitou determined on April 30, 2024, that personal information of current and former employees of Manitou, current or former dealers and suppliers of Manitou, and dependents of the foregoing was accessed and/or acquired by the unauthorized third party during this incident. The impacted information varied for each individual but generally included name, date of birth, address, Social Security Number, credit or debit card number, financial account number, employee benefits information and related records, driver’s license number, passport number, Taxpayer Identification Number, or other government issues identification number. At this time, Manitou does not have evidence that any fraud or identity theft has occurred as a result of this incident.

In light of the foregoing and out of an abundance of caution, Manitou has decided to notify your office (via this letter) and the 57 Maryland residents potentially affected by this incident via U.S. Mail on or about June 27, 2024. Samples of the notification letters are attached hereto as Exhibit A.

In addition to providing notice to you through this letter, Manitou took immediate steps once notified to assess, isolate, and mitigate the impact of the incident. In addition to conducting a full investigation and providing notice to impacted individuals, Manitou also took additional actions to improve and monitor the security of its systems.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

Sarah A. Sargent

Sarah Sargent, CIPP/US, CIPP/E, CIPM | Attorney (she/her/hers)
414.287.9450 direct | SSargent@gklaw.com

GODFREY & KAHN

This is a transmission from the law firm of Godfrey & Kahn, S.C. and may contain information which is privileged, confidential, and protected by the attorney-client or attorney work product privileges. If you are not the addressee, note that any disclosure, copying, distribution, or use of the contents of this message is prohibited. If you have received this transmission in error, please destroy it and notify us immediately at (414) 273-3500.

Manitou Equipment America, LLC
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



June 27, 2024

Notice of Data Breach

Dear [REDACTED],

At Manitou North America, LLC ("Manitou"), we take your privacy seriously. For that reason, we are writing to provide you with notice of a December 2023 cybersecurity incident that may have involved your personal information. Although we do not have any evidence at this time that your personal information has been used in an unauthorized way, we, as a precautionary measure, are notifying you of the incident and the additional protections that are available to you listed below.

What Happened

On December 24, 2023, Manitou became aware that an unauthorized third party had gained access to some of Manitou's systems on December 8, 2023. Immediately upon learning of the incident, Manitou isolated the impacted environment and began an investigation with the help of a leading forensic security firm that specializes in data security incidents. As part of the investigation, Manitou also worked with third-party data mining experts to identify who was impacted by this incident. These experts analyzed the impacted data to determine what personal information may have been accessed. This process took time. After the investigation, it was determined that your personal information was accessed and/or acquired by the third party during the incident. While Manitou does not have any evidence of fraud using your personal information at this time, we are nonetheless informing you of this incident because we take this matter seriously. While Manitou did notify law enforcement of this incident, this notice was not delayed at the request of law enforcement.

What Information Was Involved

You are receiving this letter because either you or your family member applied for a line of credit and/or financing with Manitou or were a personal guarantor of a line of credit or financing.

Your personal information that was impacted includes [REDACTED].

What We Are Doing

Upon discovery of the incident, Manitou immediately took steps to assess isolate, and mitigate the impact of the incident. In addition to conducting a full investigation and providing notice to you through this letter, we have taken additional actions to improve and monitor the security of our systems.

In response to the incident, we are providing you with access to **Triple Bureau Credit Monitoring/Triple Bureau Credit Report/Triple Bureau Credit Score** services at no charge. These services provide you with alerts for [REDACTED] from the date of enrollment when changes occur to any of one of your Experian, Equifax or TransUnion credit files. This notification is sent to you the same day that the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring services at no charge, please log on to **www.mytrueidentity.com** 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 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 18. 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.

What You Can Do

We encourage you to contact Cyberscout with any questions and for guidance regarding enrollment in the free identity protection services. In addition, please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. We encourage you to take full advantage of this service offering.

For More Information

We sincerely apologize for this incident and regret any inconvenience it may cause you. Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 am to 8:00 pm Eastern time, Monday through Friday, excluding holidays. Please call the help line at 1-833-566-5954 and supply the fraud specialist with your unique code listed above or go to **www.mytrueidentity.com**.

Sincerely,

Ilmars Nartish
Managing Director

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

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

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

Free Credit Report: It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit www.annualcreditreport.com or call toll free at 1-877-322-8228.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

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

Filing a Police Report: You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

Fraud Alerts: There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud--an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze: You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past 5 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.



00001020280000

P

Federal Trade Commission and State Attorneys General Offices: If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission, the Attorney General's office in your home state, or your local law enforcement.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

Fair Credit Reporting Act: You have certain rights pursuant to the Fair Credit Reporting Act. If you would like additional information regarding your rights under the Fair Credit Reporting Act, you can review your rights by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or by writing the Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

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

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, <https://www.marylandattorneygeneral.gov/Pages/CPD/default.aspx>, Telephone: 1-888-743-0023.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>. You can also contact the New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General. Oregon Attorney General, 1162 Court St. NE, Salem, OR 97301, <https://justice.oregon.gov>, Telephone 1-877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. 7 Rhode Island residents were impacted by this incident.

Manitou Equipment America, LLC
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



June 27, 2024

Notice of Data Breach

Dear [REDACTED],

We take your privacy seriously at Manitou Equipment America, LLC and Manitou North America, LLC (successors-in-interest to Gehl Company, and collectively referred to herein as “Manitou”). For that reason, we are writing to provide you with notice of a recent cybersecurity incident that may have involved your personal information. Although we do not have any evidence at this time that your personal information has been used in an unauthorized way, we, as a precautionary measure, are notifying you of the incident and the additional protections that are available to you listed below.

What Happened

On December 24, 2023, Manitou became aware that an unauthorized third party had gained access to some of Manitou’s systems on December 8, 2023. Immediately upon learning of the incident, Manitou isolated the impacted environment and began an investigation with the help of a leading forensic security firm that specializes in data security incidents. As part of the investigation, Manitou also worked with third-party data mining experts to identify who was impacted by this incident. These experts analyzed the impacted data to determine what personal information may have been accessed. This process took time. After the investigation, it was determined that your personal information was accessed and/or acquired by the third party during the incident. While Manitou does not have any evidence of fraud using your personal information at this time, we are nonetheless informing you of this incident because we take this matter seriously. While Manitou did notify law enforcement of this incident, this notice was not delayed at the request of law enforcement.

What Information Was Involved

You are receiving this letter because either you or a family member were an employee or supplier of Manitou or one of its affiliated companies, or because you or your family member applied for a line of credit or dealer financing with Manitou, or you or a family member were a personal guarantor of a line of credit or financing. Your personal information that was impacted includes [REDACTED].

What We Are Doing

Upon discovery of the incident, Manitou immediately took steps to assess isolate, and mitigate the impact of the incident. In addition to conducting a full investigation and providing notice to you through this letter, we have taken additional actions to improve and monitor the security of our systems.

Additionally, to help protect your identity, we are providing you with access to **Triple Bureau Credit Monitoring/Triple Bureau Credit Report/Triple Bureau Credit Score** services at no charge. These services provide you with alerts for [REDACTED] from the date of enrollment when changes occur to any of one of your Experian, Equifax, or TransUnion credit files. This notification is sent to you the same day that the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring services at no charge, please log on to **www.mytrueidentity.com** 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 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 18. 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.

What You Can Do

We encourage you to contact Cyberscout with any questions and for guidance regarding enrollment in the free identity protection services. In addition, please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. We encourage you to take full advantage of this service offering.

For More Information

We sincerely apologize for this incident and regret any inconvenience it may cause you. Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 am to 8:00 pm Eastern time, Monday through Friday, excluding holidays. Please call the help line at 1-833-566-5954 and supply the fraud specialist with your unique code listed above or go to **www.mytrueidentity.com**.

Sincerely,

Alexandre Caharel
Managing Director MEA

Ilmars Nartish
Managing Director MNA

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

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

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

Free Credit Report: It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit www.annualcreditreport.com or call toll free at 1-877-322-8228.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

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

Filing a Police Report: You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

Fraud Alerts: There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud--an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze: You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past 5 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.



00001020280000

P

Federal Trade Commission and State Attorneys General Offices: If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission, the Attorney General's office in your home state, or your local law enforcement.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

Fair Credit Reporting Act: You have certain rights pursuant to the Fair Credit Reporting Act. If you would like additional information regarding your rights under the Fair Credit Reporting Act, you can review your rights by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or by writing the Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

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

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, <https://www.marylandattorneygeneral.gov/Pages/CPD/default.aspx>, Telephone: 1-888-743-0023.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>. You can also contact the New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General. Oregon Attorney General, 1162 Court St. NE, Salem, OR 97301, <https://justice.oregon.gov>, Telephone 1-877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. 7 Rhode Island residents were impacted by this incident.

Manitou Equipment America, LLC
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



June 27, 2024

Notice of Data Breach

Dear Parent or Guardian of [REDACTED],

At Manitou Equipment America, LLC and Manitou North America, LLC (collectively, "Manitou"), we take privacy seriously. For that reason, we are writing to provide you with notice of a recent cybersecurity incident that may have involved your child's personal information. Although we do not have any evidence at this time that your child's personal information has been used in an unauthorized way, we, as a precautionary measure, are notifying you of the incident and the additional protections that are available as listed below.

What Happened

On December 24, 2023, Manitou became aware that an unauthorized third party had gained access to some of Manitou's systems on December 8, 2023. Immediately upon learning of the incident, Manitou isolated the impacted environment and began an investigation with the help of a leading forensic security firm that specializes in data security incidents. As part of the investigation, Manitou also worked with third-party data mining experts to identify who was impacted by this incident. These experts analyzed the impacted data to determine what personal information may have been accessed. This process took time. After the investigation, it was determined that your child's personal information was accessed and/or acquired by the third party during the incident. While Manitou does not have any evidence of fraud using your child's personal information at this time, we are nonetheless informing you of this incident because we take this matter seriously. While Manitou did notify law enforcement of this incident, this notice was not delayed at the request of law enforcement.

What Information Was Involved

You are receiving this letter because either your child is a dependent of a current or former employee of Manitou or one of its affiliated companies, you or your family member applied for a dealer line of credit or financing with Manitou, or you are or a family member were a personal guarantor for a line of Manitou credit or one of its affiliated companies.

Your child's personal information that was impacted includes [REDACTED].

What We Are Doing

Upon discovery of the incident, Manitou immediately took steps to assess, isolate, and mitigate the impact of the incident. In addition to conducting a full investigation and providing notice to you through this letter, we have taken additional actions to improve and monitor the security of our systems.

Additionally, to help protect your child's identity, we are providing the parents of impacted minor dependents with access to **Cyber Monitoring** services for you and your minor child for [REDACTED] at no charge. Cyber monitoring will look out for your and your child's personal information 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 Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Cyber Monitoring services at no charge, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED]. Once you have completed the enrollment for yourself, click on your name in the top right of your dashboard and then "Add Family Member" to enroll your child. To complete the child's enrollment, click on the child's name and provide the requested information for monitoring. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and an email account and will require enrollment by a parent or guardian first. 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.

What You Can Do

We encourage you to contact Cyberscout with any questions and for guidance regarding enrollment in the free identity protection services. In addition, please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect your child's identity, including recommendations by the Federal Trade Commission regarding identity theft protection. We encourage you to take full advantage of this service offering.

For More Information

We sincerely apologize for this incident and regret any inconvenience it may cause you. Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call 1-833-566-5954 and supply the fraud specialist with your unique code listed above or go to <https://bfs.cyberscout.com/activate>.

Sincerely,

Alexandre Caharel
Managing Director MEA

Ilmars Nartish
Managing Director MNA

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

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

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

Free Credit Report: It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.



To order your annual free credit report please visit www.annualcreditreport.com or call toll free at 1-877-322-8228.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

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

Filing a Police Report: You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

Fraud Alerts: There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud--an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze: You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past 5 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

00001020280000

P

Federal Trade Commission and State Attorneys General Offices: If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission, the Attorney General's office in your home state, or your local law enforcement.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

Fair Credit Reporting Act: You have certain rights pursuant to the Fair Credit Reporting Act. If you would like additional information regarding your rights under the Fair Credit Reporting Act, you can review your rights by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or by writing the Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

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

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, <https://www.marylandattorneygeneral.gov/Pages/CPD/default.aspx>, Telephone: 1-888-743-0023.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>. You can also contact the New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General. Oregon Attorney General, 1162 Court St. NE, Salem, OR 97301, <https://justice.oregon.gov>, Telephone 1-877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. 7 Rhode Island residents were impacted by this incident.