

Sent on behalf of Atty. Sarah A. Sargent

Dear Attorney General Brown:

Our firm represents M&M Transport Services, LLC (“M&M”), a Massachusetts company. M&M hereby formally submits notification of a recent data incident pursuant to Md. Code Com. Law § 14-3501 et seq. M&M reserves the right to supplement this notice with any significant details learned subsequent to this submission. By providing this notice, M&M 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 M&M.

On June 30, 2024, M&M became aware that an unauthorized third party gained access to some of M&M’s systems on or around June 4, 2024, and subsequently deployed malicious software in the systems. Immediately upon learning of the incident, M&M isolated the impacted environment and began an investigation to determine what information was affected with the help of a leading forensic security firm that specializes in data security incidents, as well as a response team to begin recovering and restoring M&M’s systems. After the forensic investigation, it was determined that on July 12, 2024, that personal information of current and former employees of M&M may have been accessed and/or acquired by the unauthorized third party during this incident. The information impacted generally included name, date of birth, Social Security number, driver’s license number, I-9 information, and/or passport number. At this time, M&M 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, M&M has decided to notify your office (via this letter) and the 380 Maryland residents potentially affected by this incident via U.S. Mail on or about July 31, 2024. Samples of the notification letters are attached hereto as Exhibit A.

In addition to providing notice to you through this letter, M&M took immediate steps once notified to assess, isolate, and mitigate the impact of the incident. In addition to conducting a full investigation, M&M has also implemented additional security software, limited internet access to certain systems, and deployed further access management controls. M&M is also in the process of notifying individuals of the unauthorized access and acquisition.

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

Sincerely,

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



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.



Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

Postal Endorsement Line

<<Full Name>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<City>>, <<State>> <<Zip>>

<<Country>>

***Postal IMB Barcode

<Date>

Notice of Data Breach

Dear <<Full Name>>,

At M&M Transport Services, LLC, ("M&M"), we take your privacy seriously. For that reason, we are writing to provide you with notice of a recent cybersecurity incident that may have involved your personal information.

What Happened

On June 30, 2024, M&M became aware that an unauthorized third party gained access to and deployed malicious software in some of M&M's systems. Immediately upon learning of the incident, M&M isolated the impacted environment and began an investigation to determine what information was affected with the help of a leading forensic security firm that specializes in data security incidents, as well as a response team to begin recovering and restoring our systems. After the forensic investigation, it was determined that your personal information was accessed and/or acquired by the third party during the incident. While M&M does not have any evidence that your personal information has been used in a fraudulent manner at this time, we are nonetheless informing you of this incident because we take this matter seriously. This notice was not delayed at the request of law enforcement.

What Information Was Involved

You are receiving this letter because you were an employee of M&M. Your personal information that may have been impacted includes your name, date of birth, Social Security number, driver's license information, I-9 information, and/or passport number.

What We Are Doing

Upon discovery of the incident, M&M immediately took steps to assess, isolate, and mitigate the impact of the incident. We also worked quickly to restore and secure our impacted systems. 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, including implementing additional security software, limiting internet access to certain systems, and deploying further access management controls.

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for <<12/24 >> months. If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent.

Please note that Identity Restoration is available to you for <<12/24 >> months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as part of a complimentary <<12\24 >> -month membership. This product provides you with superior identity theft detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by 10/18/2024** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your **activation code**: <<Activation Code>>

If you have questions about the product, need assistance with Identity Restoration issues that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-877-288-8057 by 10/18/2024. Be prepared to provide engagement number <<Engagement Number>> as proof of eligibility for the Identity Restoration services by Experian.

What You Can Do

Please review the enclosed Additional Details Regarding Your Experian IdentityWorks Membership document for additional information on how to protect against identity theft and fraud. You may also take advantage of the complimentary identity protection services being offered.

For More Information

We sincerely apologize for this incident and regret any inconvenience it may cause you. If you have further questions or concerns, please call 833-215-2898, Monday through Friday, 9 AM to 9 PM Eastern Time.

Sincerely,

Mark Warsofsky

President
M&M Transport Services, LLC

Adam Warsofsky

SVP
M&M Transport Services, LLC

ADDITIONAL DETAILS REGARDING YOUR EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax, and TransUnion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

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

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 your state's 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 five 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.

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 Avenue NW, Washington, DC 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, IA 50319-0106.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118, Frankfort, KY 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, RI 02903, www.riag.ri.gov, Telephone: 401-274-4400. 293 Rhode Island residents were impacted by this incident.



Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

Postal Endorsement Line

<<Full Name>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<City>>, <<State>> <<Zip>>

<<Country>>

***Postal IMB Barcode

<Date>

Notice of Data Breach

Dear <<Full Name>>,

At M&M Transport Services, LLC, ("M&M"), we take your privacy seriously. For that reason, we are writing to provide you with notice of a recent cybersecurity incident that may have involved your personal information.

What Happened

On June 30, 2024, M&M became aware that an unauthorized third party gained access to and deployed malicious software in some of M&M's systems. Immediately upon learning of the incident, M&M isolated the impacted environment and began an investigation to determine what information was affected with the help of a leading forensic security firm that specializes in data security incidents, as well as a response team to begin recovering and restoring our systems. After the forensic investigation, it was determined that your personal information was accessed and/or acquired by the third party during the incident. While M&M does not have any evidence that your personal information has been used in a fraudulent manner at this time, we are nonetheless informing you of this incident because we take this matter seriously. This notice was not delayed at the request of law enforcement.

What Information Was Involved

You are receiving this letter because you are an employee of M&M. Your personal information that may have been impacted includes your name, date of birth, Social Security number, driver's license information, I-9 information, and/or passport number.

What We Are Doing

Upon discovery of the incident, M&M immediately took steps to assess, isolate, and mitigate the impact of the incident. We also worked quickly to restore and secure our impacted systems. 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, including implementing additional security software, limiting internet access to certain systems, and deploying further access management controls.

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for <<12\24 >> months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent.

Please note that Identity Restoration is available to you for <<12\24 >> months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as part of a complimentary <<12\24 >> -month membership. This product provides you with superior identity theft detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by 10/18/2024** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your **activation code**: <<Activation Code>>

If you have questions about the product, need assistance with Identity Restoration issues that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-877-288-8057 by 10/18/2024. Be prepared to provide engagement number <<Engagement Number>> as proof of eligibility for the Identity Restoration services by Experian.

What You Can Do

Please review the enclosed Additional Details Regarding Your Experian IdentityWorks Membership document for additional information on how to protect against identity theft and fraud. You may also take advantage of the complimentary identity protection services being offered.

For More Information

We sincerely apologize for this incident and regret any inconvenience it may cause you. If you have further questions or concerns, please call 833-215-2898, Monday through Friday, 9 AM to 9 PM Eastern Time.

Sincerely,

Mark Warsofsky

President
M&M Transport Services, LLC

Adam Warsofsky

SVP
M&M Transport Services, LLC

ADDITIONAL DETAILS REGARDING YOUR EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax, and TransUnion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

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

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 your state's 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 five 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.

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 Avenue NW, Washington, DC 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, IA 50319-0106.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118, Frankfort, KY 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, RI 02903, www.riag.ri.gov, Telephone: 401-274-4400. 293 Rhode Island residents were impacted by this incident.