



5 Waller Avenue • Suite 200 • White Plains, NY • 10601
tel (914) 353-3850 • fax (914) 353-3851 • wshblaw.com

RECEIVED

DEC 15 2025

John A. Darminio

direct dial (914) 353-3861

email jdarminio@wshblaw.com

CONSUMER PROTECTION

December 10, 2025

New Hampshire Department of Justice
Office of the Attorney General
1 Granite Place South
Concord, New Hampshire 03301

Re: Notice of Data Event

Dear Sir or Madam:

This office represents OTA Management, LLC (“OTA”) located One Manhattanville Road, Purchase, New York 10577, and are writing to provide your office with notice of a data security incident.

By providing this notice, OTA does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

OTA was the victim of an unknown third party gaining unauthorized access to the OTA network environment on March 23, 2025.

Upon learning of the issue, OTA immediately engaged the appropriate forensic consultants to investigate the root of the incident, notify relevant law enforcement, secure its systems, prevent this issue from reoccurring, and identify any sensitive or personal information that may have been impacted as a result.

The initial investigation determined that data stored on an impacted server may have been exposed without authorization. Thereafter, OTA conducted a thorough review of the contents of the impacted files to determine if they contained any sensitive information. On July 25, 2025, after completing the extensive and exhaustive review, OTA learned certain personal or sensitive information contained in its environment may have been exposed as result of the incident. Since that time, OTA has been working diligently to identify and obtain sufficient information in order to provide the appropriate notifications. The first wave of mailing commenced on September 2, 2025. A second wave of mailing occurred on October 3, 2025.

Notice to New Hampshire Residents

After identification of New Hampshire resident data that could be deemed reportable, OTA provided written notice of this incident to two (2) New Hampshire residents in its second wave of mailing, inclusive of a complimentary credit monitoring services through Privacy Solutions for 12-months. Written notice was provided in substantially the same form as the letter attached here.

Additionally, OTA is providing impacted individuals with guidance on how to better protect against identity theft and fraud. OTA is providing individuals with 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 encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

In response to this event, OTA is reviewing and enhancing its information security policies and procedures.

Should you have any questions regarding this notification or other aspects of the data security event, please feel free to contact the undersigned.

Respectfully submitted,

/s/John A. Darminio

John A. Darminio

Encl.

Return Processing Center:
PO Box 173071 | Milwaukee, WI 53217

<FirstName> <LastName>
<Address1> <Address2>
<City> <State> <PostalCode+4>

<Date>

RE: <<Important Security Notification or Notice of Data Breach>>

Please read this entire letter.

Dear <FirstName> <LastName>,

Notice of Data Incident

We are writing to inform you of an incident that may have affected some of your personal information. While there is currently no indication your personal information identified was used, there is reason to believe it may have been accessed during this incident.

What Happened

OTA Management LLC (hereinafter "OTA") was the victim of an unknown third party gaining unauthorized access to the OTA network environment on March 23, 2025. OTA discovered the incident on March 24, 2025 and immediately severed the unauthorized activity.

Upon learning of the issue, OTA immediately engaged the appropriate forensic consultants to investigate the root of the incident, secure its systems, prevent this issue from reoccurring, and identify any sensitive or personal information that may have been impacted as a result.

Our investigation determined that data may have been exposed without authorization. Thereafter, OTA conducted a thorough review of the contents of the files to determine if they contained any sensitive information. After completing the extensive and exhaustive review, OTA learned certain personal or sensitive information contained in its environment may have been exposed as result of the incident. Since that time, OTA has been working diligently to identify and obtain sufficient information in order to provide you with this notice.

What Information Was Involved

This incident involved a combination of your name and <Data Elements>. As a result, your personal information may have been potentially exposed to others.

What We Are Doing

Please be assured that we have taken every step necessary to address the incident. We take our obligation to safeguard the information we receive seriously. Once the incident was discovered, we quickly took action to minimize risks, including securing the compromised systems and initiating an investigation into the unauthorized access. We also aligned additional resources in an effort to assess the impact of the incident and better protect OTA from future instances like this one. We remain vigilant, continuously upgrading our already robust security measures to carefully safeguard against similar incidents.

In response to the incident, we are securing the services of Privacy Solutions to provide complimentary identity monitoring for <<12_24>> months at no charge.

What You Can Do

If you believe there was fraudulent use of your information as a result of this incident, please review the Reference Guide at the end of this letter for additional steps on how to protect against identity theft and fraud.

To enroll in the credit monitoring services at no charge, please visit www.privacysolutions.com and enter the following activation code, <<Activation Code>>, to activate your membership and start monitoring your personal information. Please note the deadline to enroll is January 15, 2026. Privacy Solutions provides credit monitoring through Equifax, credit report and score access, identity theft insurance with \$0 deductible, Identity Restoration services, and dark web monitoring.

We also recommend you review your credit reports and account statements over the next 12 to 24 months and notify your financial institution of any unauthorized transactions or incidents of suspected identity theft.

For More Information

We sincerely regret any inconvenience or concern caused by this incident. If you have any questions about this incident, please contact (866) 830-1451, Monday – Friday between 8:00 a.m. and 5:00 p.m. Central Time, excluding major U.S. holidays.

While call center representatives should be able to provide thorough assistance and answer most of your questions, you may still feel the need to speak with OTA regarding this incident. If so, please contact us at questions@otallc.com

Sincerely,

/s/Jim Santori

Jim Santori
OTA Management LLC

REFERENCE GUIDE

Review Your Account Statements

Carefully review statements sent to you from your healthcare providers, insurance company, and financial institutions to ensure that all of your account activity is valid. Report any questionable charges promptly to the provider or company with which you maintain the account.

Order Your Free Credit Report

To order your free annual credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 303485281. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

Upon receiving your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names; the credit bureau will be able to tell if this is the case. Look in the "personal information" section for any inaccuracies in information (such as home address and Social Security Number).

If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

Contact the U.S. Federal Trade Commission

If you detect any unauthorized transactions in any of your financial accounts, promptly notify the appropriate payment card company or financial institution. If you detect any incidents of identity theft or fraud, promptly report the matter to your local law enforcement authorities, state Attorney General and the FTC.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft by using the following contact information: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.ftc.gov/idtheft/.

Place a Fraud Alert on Your Credit File

To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect against the possibility of an identity thief opening new credit accounts in your name. When a credit grantor checks the credit history of someone applying for credit, the credit grantor gets a notice that the applicant may be the victim of identity theft. The alert notifies the credit grantor to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free fraud numbers provided below. You will reach an automated telephone system that allows flagging of your file with a fraud alert at all three credit bureaus.

Equifax	P.O. Box 105069 Atlanta, GA 30348	1-888-766-0008	www.equifax.com
Experian	P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	P.O. Box 2000 Chester, PA 19016	1-800-680-7289	www.transunion.com

Security Freezes

You have the right to request a credit freeze from a consumer reporting agency, free of charge, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit bureau. To place a security freeze on your credit report you must contact the credit reporting agency by phone, mail, or secure electronic means and provide proper identification of your identity. The following information must be included when requesting a security freeze (note that if you are requesting a security freeze 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, display your name and current mailing address, and the date of issue.

Below, please find relevant contact information for the three consumer reporting agencies:

Equifax Security Freeze	P.O. Box 105788 Atlanta, GA 30348	1-800-685-1111 www.equifax.com
Experian Security Freeze	P.O. Box 9554 Allen, TX 75013	1-888-397-3742 www.experian.com
TransUnion	P.O. Box 160 Woodlyn, PA 19094	1-888-909-8872 www.transunion.com

Once you have submitted your request, the credit reporting agency must place the security freeze no later than 1 business day after receiving a request by phone or secure electronic means, and no later than 3 business days after receiving a request by mail. No later than five business days after placing the security freeze, the credit reporting agency will send you confirmation and information on how you can remove the freeze in the future.

Provide Any Updated Personal Information to Your Health Care Provider

Your health care provider's office may ask to see a photo ID to verify your identity. Please bring a photo ID with you to every appointment if possible. Your provider's office may also ask you to confirm your date of birth, address, telephone, and other pertinent information so that they can make sure that all of your information is up to date. Please be sure and tell your provider's office when there are any changes to your information. Carefully reviewing this information with your provider's office at each visit can help to avoid problems and to address them quickly should there be any discrepancies.

Additional Information

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).

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

District of Columbia: Contact the District of Columbia Office of Attorney General for steps to avoid identity theft: (202) 727-3400, 400 6th Street, NW, Washington DC 20001, <http://oag.dc.gov>.

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: Maryland Attorney General: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

Massachusetts Residents: You have the right to obtain a police report and request a free security freeze as described above.

New York Residents: You can obtain information from the New York State Office of the Attorney General about how to protect yourself from identity theft and tips on how to protect your privacy online. You can contact the New York State Attorney General at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755 or 1-800-7889898; <https://ag.ny.gov/>. You also may contact the Bureau of Internet and Technology (BIT), 28 Liberty Street, New York, NY 10005; 212-416-8433; <https://ag.ny.gov/about/about-office/economic-justice-division#internet-technology>.

North Carolina Residents: You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6400; www.ncdoj.gov.

Oregon Residents: We encourage you to report suspected identity theft to the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096; 1-877-877-9392 or 1-503-378-4400; www.doj.state.or.us.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400.

South Carolina Residents: You can obtain information from the South Carolina Department of Consumer Affairs: 293 Greystone Blvd., Ste. 400, Columbia, SC 29210; 800-922-1594; www.consumer.sc.gov.

Texas Residents: You can obtain information from the Texas Attorney General can be reached at: 300 W. 15th Street, Austin, Texas 78701; 800-621-0508; www.texasattorneygeneral.gov/consumer-protection/.

Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

New Mexico: You have rights pursuant to the Fair Credit Reporting Act. These rights include knowing what is in your file and your credit score; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; to be told if information in your credit file has been used against you; as well as other rights. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. For more information about the FCRA, and your rights pursuant to the FCA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.