Michele Veltri
Office: (267) 930-2297
Fax: (267) 930-4771
Email: mveltri@mullen.law

411 Theodore Fremd, Ste 206S
Rye, NY 10580

November 17, 2025

VIA E-MAIL

Office of the New Hampshire Attorney General
Consumer Protection & Antitrust Bureau
33 Capitol Street
Concord, NH 03301
E-mail: DOJ-CPB@doj.nh.gov

Re: Notice of Data Event

To Whom It May Concern:

We represent Drivestream, Inc. ("Drivestream") located at 1602 Village Market Blvd. SE, Suite 400 Leesburg, Virginia 20175, and are writing to notify your office of an incident that may affect the security of certain personal information relating to seventeen (17) New Hampshire residents. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Drivestream 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

On or around December 9, 2024, Drivestream observed suspicious activity at its data center. Drivestream immediately took steps to secure its computer system and launched an investigation. The investigation included working with third-party forensic investigators and determined that an unknown, unauthorized actor accessed certain systems between December 4, 2024, and December 9, 2024, and potentially exfiltrated certain data from the Drivestream data center. Upon determining that data was potentially exfiltrated from its data center, Drivestream began notifying potentially affected customers of the incident on or around January 10, 2025. Drivestream also commenced a programmatic and manual review of the potentially affected data with the assistance of third-party forensic investigators in order to determine the types of protected information present at the time of the incident and to whom the information relates. Drivestream began providing its customers with the results of the review on or around August 6, 2025. Drivestream

offered to provide notice to individuals and relevant regulatory authorities and is notifying your Office on behalf of, and at the direction of, requesting customers.

While the information varies for each individual, the information that could have been subject to unauthorized access includes name, Social Security number, and financial account information. Drivestream is unaware of any actual or attempted identity theft or fraud occurring in connection with this incident.

Notice to New Hampshire Residents

On or around November 17, 2025, Drivestream began providing written notice of this incident to affected individuals, which includes seventeen (17) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***. Drivestream continues to receive address information for the potentially impacted population from certain customers. As notification to impacted individuals is ongoing as Drivestream receives information from customers, Drivestream may supplement this notification if it is determined that a significant amount of additional New Hampshire residents will receive notice.

Other Steps Taken and To Be Taken

Upon discovering the incident, Drivestream initiated its incident response procedures, assessed the security of Drivestream systems, and began an investigation to identify potentially affected individuals. Further, Drivestream notified federal law enforcement regarding the incident. As part of its ongoing commitment to the privacy of personal information in its care, Drivestream is reviewing its policies, procedures, and processes related to the storage of, and access to, personal information to reduce the likelihood of a similar future incident. Drivestream is also working to implement additional safeguards and training to its employees. Drivestream is providing access to credit monitoring and identity theft protection services for twelve (12) months, through Epiq, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Drivestream is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Drivestream 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.

Drivestream is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-2297.

Very truly yours,

Michele Veltri

Michele Veltri of
MULLEN COUGHLIN LLC

MTV/lcf
Enclosure

EXHIBIT A

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>>

<<Variable data 1 >>

Dear <<Full Name>>:

Drivestream Inc. ("Drivestream") writes to notify you of an incident that may affect the privacy of some of your information. Drivestream assists companies with migrating employee data into Oracle. This letter provides details of the incident that affected our data center, our response, and resources available to you to help protect your information from possible misuse, should you feel it is appropriate to do so.

What Happened? On or around December 9, 2024, Drivestream observed suspicious activity at its data center. Drivestream launched an investigation and determined between December 4, 2024, and December 9, 2024, an unauthorized actor accessed certain systems within the data center that stored information and downloaded certain files from those systems. Although we have no evidence of any identity theft or fraud occurring in connection with this incident, Drivestream conducted a review of relevant systems. We are now notifying you because we determined your information was present within our systems.

What Information Was Involved? Our investigation determined the following type of information related to you may have been impacted by this incident: <<Breached elements>>, in combination with your name. At this time, we have no indication that your information was subject to actual or attempted misuse as a result of this incident.

What We Are Doing. Drivestream treats its responsibility to safeguard information as an utmost priority. Upon discovery, Drivestream promptly commenced an investigation to confirm the nature and scope of this incident. This investigation and response included confirming the security of our systems, reviewing the contents of relevant data for sensitive information, and notifying impacted individuals associated with that sensitive information. As part of our ongoing commitment to the privacy of personal information in our care, we are reviewing our policies, procedures, and processes related to the storage of and access to personal information to reduce the likelihood of a similar future event. We reported the incident to law enforcement and are cooperating with their investigation. We will also notify applicable regulatory authorities, as required by law.

As an added precaution, we are also offering <<12/24>> months of complimentary access to credit monitoring and identity theft protection services through Epiq - Privacy Solutions ID. Although we are covering the cost of these services, due to privacy restrictions, you will need to complete the enrollment process yourself.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity. You may also review the information contained in the attached *Steps You Can Take to Help Protect Your Personal Information*. There you will also find more information regarding the complimentary credit monitoring services we are making available to you. While Drivestream will cover the cost of these services, you will need to enroll yourself in the services we are offering, if you would like to do so.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 877-396-3249 between the hours of 9:00 a.m. and 9:00 p.m. EST, Monday - Friday, excluding major U.S. holidays. You may also write to Drivestream at 1602 Village Market Blvd. SE, Suite 400, Leesburg, Virginia, 20175.

Sincerely,

Drivestream Inc.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR PERSONAL INFORMATION

Enroll in Monitoring Services

Activation Code: <<ACTIVATION CODE>>
Enrollment Deadline: <<ENROLLMENT DEADLINE>>
Coverage Length: <<12/24>> Months

Epiq - Privacy Solutions ID
1B Credit Monitoring - Basic

How To Enroll:

1) Visit www.privacysolutionsid.com and click "Activate Account"
2) Enter the following activation code, **<<Activation Code>>** and complete the enrollment form
3) Complete the identity verification process
4) You will receive a separate email from noreply@privacysolutions.com confirming your account has been set up successfully and will include an Access Your Account link in the body of the email that will direct you to the log-in page
5) Enter your log-in credentials
6) You will be directed to your dashboard and activation is complete!

Product Features:

1-Bureau Credit Monitoring with Alerts
Monitors your credit file(s) for key changes, with alerts such as credit inquiries, new accounts, and public records.

Dark Web Monitoring (Basic)
Monitors one email address, phone, name, DOB, and SSN on the dark web. Includes retrospective report as well as ongoing monitoring.

Credit Protection
3-Bureau credit security freeze assistance with blocking access to the credit file for the purposes of extending credit (with certain exceptions).

Change of Address Monitoring
Monitors the National Change of Address (NCOA) database and the U.S. Postal Service records to catch unauthorized changes to users' current or past addresses.

Identity Restoration & Lost Wallet Assistance
Dedicated ID restoration specialists who assist with ID theft recovery and assist with canceling and reissuing credit and ID cards.

If you need assistance with the enrollment process or have questions regarding Epiq – Privacy Solutions ID 1B Credit Monitoring - Basic, please call directly at **866.675.2006**, Monday-Friday 9:00 a.m. to 5:30 p.m., ET.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report.

To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should you wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/data-breach-help
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and 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.

Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 1-202-442-9828; and https://oag.dc.gov/.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may

have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_yourrights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately 9 Rhode Island residents that may be impacted by this event.