



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Gregory Lederman
Office: (267) 930-4637
Fax: (267) 930-4771
Email: glederman@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

February 18, 2025

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

To Whom It May Concern:

We represent Trident Maritime Systems LLC (“TMS”), located at 2011 Crystal Drive, Suite 1102, Arlington, VA 22202, and are writing to notify your Office of an incident that may affect the security of information relating to certain Maryland residents. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, TMS does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

In February 2023, TMS discovered suspicious activity on its computer network. In response, TMS took steps to ensure the security of its network and launched an investigation to determine the nature and scope of the activity. The investigation determined that an unauthorized actor gained access to TMS’ computer network between February 1, 2023 and February 10, 2023, and may have accessed or taken certain data from its systems. Following this investigation, TMS engaged in an extensive, time-consuming review of the involved data in order to identify what information was present and to whom it related to. Once this initial review was completed, TMS then conducted a manual review of its internal records to identify address information in order to notify potentially affected individuals. This review was recently completed and determined the information that could have been subject to unauthorized access includes name, and Social Security number, driver’s license number, passport number, health insurance information, and financial account information.

Notice to Maryland Residents

On or about February 18, 2025, TMS provided written notice of this incident to three hundred twenty-eight (328) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, TMS moved quickly to investigate and respond to the incident, assess the security of TMS systems, and identify potentially affected individuals. Further, TMS notified federal law enforcement regarding the event. TMS also worked to implement additional safeguards and training to its employees. TMS is providing access to complimentary credit monitoring services for twelve (12) months through TransUnion, to individuals whose information was potentially affected by this incident.

Additionally, TMS is providing impacted individuals with guidance on how to better protect against identity theft and fraud. TMS 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. TMS is providing written notice of this incident to relevant state regulators, as necessary.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4637.

Very truly yours,



Gregory Lederman of
MULLEN COUGHLIN LLC

GCL/jc2
Enclosure

EXHIBIT A



February 17, 2025

Notice of Data Breach

Dear _____ :

Trident Maritime Systems, LLC ("TMS") is writing to inform you of an event that may impact some of your information. We take this event very seriously and the confidentiality, privacy, and security of information in our care is one of our highest priorities. While we are not aware of any actual or attempted misuse of your information, we are providing information regarding the event, our response, and resources to help further protect your information, should you feel it necessary to do so.

What Happened? In February 2023, we discovered suspicious activity on our computer network. In response, we took steps to ensure the security of our network and launched an investigation to determine the nature and scope of the activity. The investigation determined that an unauthorized actor gained access to our computer network between February 1, 2023 and February 10, 2023, and may have accessed or taken certain data from our systems. Following this investigation, TMS engaged in an extensive, time-consuming review of the involved data in order to identify what information was present and to whom it related to. Once this initial review was completed, TMS then conducted a manual review of its internal records to identify address information in order to notify potentially affected individuals.

What Information Was Involved? Our investigation and review was completed in January 2025 and we are notifying you now because your name and Social Security number and date of birth were identified during the review. Please note that we are not aware of any identity theft or fraud as a result of this incident and are notifying you out of an abundance of caution.

What We Are Doing. We take this event and the security of information in our care very seriously. Upon learning of the event, we moved quickly to confirm the security of our network and investigate the scope of the event. As part of our ongoing commitment to information security, we reviewed existing security policies and have implemented additional security measures to further reduce the risk of a similar event moving forward. We will also be notifying relevant regulators, as required.

As an added precaution, we are also offering you 12 months of complimentary credit monitoring, through Cyberscout, a TransUnion company specializing in fraud assistance and remediation services. A description of these services and enrollment instructions can be found in the enclosed *Steps You Can Take to Help Protect Your Information*. We encourage you to enroll in these services as we are not able to do so on your behalf.

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 and to detect errors. Please review the enclosed *Steps You Can Take to Help Protect Your Information*, which includes further information on steps you can take, should you feel it necessary to do so. Additionally, we encourage you to enroll in the complimentary credit monitoring being offered.

000010102G0500

P

For More Information. We understand you may have questions about this event that are not addressed in this letter. If you have additional questions, please contact us at 1-833-799-4041 between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. We sincerely apologize for any inconvenience this may cause.

Sincerely,

Trident Maritime Systems, LLC

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Monitoring Services

To enroll in Credit 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:

. 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 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.



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 consumers 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 their 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; (202) 442-9828; and oag.dc.gov. You may also write to TMS at 2011 Crystal Drive, Suite 1102, Arlington, VA 22202.

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/>. You may also write to TMS at 2011 Crystal Drive, Suite 1102, Arlington, VA 22202.

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 2 Rhode Island residents that may be impacted by this event.