

Martin Energy Group
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



April 30, 2025

Dear [REDACTED]

We are writing to inform you of a cyber security incident experienced by Martin Energy Group (“Martin Energy”) that may have involved your information described below. While we have no evidence of attempted or actual misuse of your information, we are providing you with information about the incident, our response, and steps you can take to help protect your information, should you feel it appropriate to do so.

What Happened: On February 13, 2025, we discovered we were victimized by a sophisticated ransomware attack. Upon discovery, we immediately began working with our I.T. team and third-party forensic specialists to secure the network, restore our systems to operability, and investigate the full nature and scope of the incident. We also worked with the U.S. Department of Homeland Security and the Cybersecurity and Infrastructure Security Agency to respond to this incident. Through the investigation, on February 27, 2025, it was determined that certain Martin Energy data, kept in the normal course of business, may have been subject to unauthorized access during the attack. We then immediately began a review of the potentially impacted files to identify what type of information was contained therein, and to whom that information belonged. This review was recently completed on April 1, 2025. At that time, we learned that current and former employee data may have been potentially impacted. Although we are unable to confirm the specific information that may be affected at this time, we are providing you with notification in an abundance of caution as we value the security of our employees’ information.

What Information Was Involved: The information believed to potentially be at risk may include your first and last name, in combination with one or more of the following: Social Security number and/or driver’s license or state identification number.

What We Are Doing: Upon discovery, we engaged third-party forensic specialists to investigate this matter. Out of an abundance of caution, we have arranged for you to activate, at no cost to you, **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services for 12 months provided by Cyberscout, a TransUnion company. Due to privacy laws, we cannot activate these services for you directly. Additional information regarding how to activate the complimentary credit monitoring service is enclosed. We have also provided additional information about steps you can take to help protect yourself against fraud and identity theft.

What You Can Do: We recommend that you remain vigilant in regularly reviewing and monitoring all of your account statements and credit history to guard against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on your accounts, please promptly contact your financial institution or company. Additionally, you can enroll to receive the complimentary credit monitoring services we are making available to you. You can also review the enclosed “Steps You Can Take to Help Protect Your Information” for additional resources.

000010102G0500

P

For More Information: Should you have additional questions or concerns regarding this matter, please do not hesitate to contact our dedicated call center agents at 1-800-405-6108 between the hours of 8:00 am to 8:00 pm, excluding major US holiday. You may also write to us at 70150 Hwy 50, Tipton, MO 65081-3128.

We take the privacy and security of the information in our care seriously and sincerely regret any worry or inconvenience this incident may cause you and your family.

Sincerely,

A handwritten signature in dark ink, appearing to read "Marcus Martin", is written over a faint, light-colored circular stamp or watermark.

Marcus Martin
Chief Executive Officer

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

How do I enroll for the free 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.



ADDITIONAL ACTIONS TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You 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, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you 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 your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

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

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

TransUnion 1-800-680-7289 www.transunion.com	Experian 1-888-397-3742 www.experian.com	Equifax 1-888-298-0045 www.equifax.com
---	---	--

TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000	Experian Fraud Alert P.O. Box 9554 Allen, TX 75013	Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069
TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	Equifax Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

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.