

November 21, 2025

VIA EMAIL (DOJ-CPB@DOJ.NH.GOV)

Attorney General John Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Michelle N. Molner
TEL +1 512 322 5415
FAX +1 512 322 3617
michelle.molner@bakerbotts.com

Re: Notice of Security Incident

Dear Sir or Madam:

On behalf of our client, Kern Oil & Refining Inc. d/b/a Kern Energy (“Kern”), this letter serves to notify your office of an incident involving the personal information of one New Hampshire resident.

In August 2025, Kern experienced a security incident in which an unauthorized third party gained access to its systems. Upon discovery of the intrusion, Kern’s security team took immediate action to contain the threat and engaged third-party forensic experts to assist with response and remediation efforts. As a result of those efforts, we learned that the unauthorized third party *may* have gained access to systems containing personal information of individuals who currently have, or at one point had, a relationship with Kern (e.g., current or former employees, dependents, beneficiaries). To be clear, there is no evidence at this time that the third party *actually* accessed, stole, disclosed, or otherwise misused any such personal information.

Upon discovery, the company also immediately engaged legal counsel and took steps to mitigate any harm to potentially impacted individuals. This includes the provision of complementary credit monitoring and identity protection services through Epiq - Privacy Solutions ID Credit Monitoring - Plus for 24 months. Kern has also taken steps to minimize risk of similar incidents occurring in the future, including but not limited to assessing and updating relevant security policies and procedures, systems, tools, and configurations.

Kern has notified potentially impacted individuals consistent with its legal obligations. Specifically, the company mailed notices to potentially impacted individuals via U.S. Mail on November 12, 2025. This notice included factual details regarding the incident, guidance on how the individual can protect their own personal information, and a unique enrollment code for the 24-month credit monitoring and identity protection services. A copy of the individual notice template is attached to this letter as Appendix A.

Kern Energy is committed to safeguarding the personal information and interests of New Hampshire residents. If you have any questions or require further information regarding the incident, please feel free to contact me.

Sincerely,



Michelle Molner

Attorney General John Formella

APPENDIX A: Individual Notice Template



Secure Processing Center
P.O. Box 680
Central Islip, NY 11722-0680

Postal Endorsement Line

<<Full Name>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

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

<<Country>>

***Postal IMB Barcode

<<Date>>

RE: Notice of Security Incident

Dear <<Full Name>>:

We are writing to inform you of an incident that may have impacted some of your personal information and how you can minimize risk to yourself.

What Happened?

In August 2025, Kern Oil & Refining Inc. d/b/a Kern Energy (“Kern”, “we”, or “our”) experienced a security incident in which an unauthorized third party gained access to our systems. Upon discovery of the intrusion, our security team took immediate action to contain the threat and engaged third-party forensic experts to assist with response and remediation efforts. As a result of those efforts, we learned that the unauthorized third party *may* have gained access to systems containing personal information of individuals who currently have, or at one point had, a relationship with us (e.g., current or former employees, dependents, beneficiaries). To be clear, there is no evidence at this time that the third party *actually* accessed, stole, disclosed, or otherwise misused any such personal information.

Nevertheless, we are sending you this notice out of an abundance of caution to make you aware of the incident, explain the steps we have taken to respond and mitigate risk to you, and inform you of the additional steps you can take to protect yourself.

What Information Was Involved?

The types of personal information that may have been impacted include common employment and beneficiary information such as name, address, phone number, date of birth, Social Security Number, health insurance information, and other similar data.

What Are We Doing?

Upon discovery of the incident, Kern immediately took steps to identify the systems and information that may have been unlawfully accessed, and to contain those systems. We also notified law enforcement of the incident. Finally, we have reviewed our technical and administrative security measures and taken steps to further strengthen those measures and minimize the risk of similar incidents occurring in the future.

Out of an abundance of caution and to help protect your identity, we are offering a complimentary 24-month membership of **Epiq - Privacy Solutions ID 1B Credit Monitoring - Plus**. To activate your membership, please follow the steps below:

- Ensure that you **enroll by:** <<ENROLLMENT DEADLINE>> (Your code will not work after this date.)
- **Visit this website** to enroll: www.privacysolutionsid.com
- Provide your **activation code:** <<ACTIVATION CODE>>

More information about your membership is included in the attached handout titled **EPIQ – PRIVACY SOLUTIONS ID**. If you have further questions about the product, need assistance, or would like an alternative to enrolling online, please contact Epiq’s customer care team at the phone number below by <<ENROLLMENT DEADLINE>>. Be prepared to provide engagement number <<ACTIVATION CODE>> as proof of eligibility for the services.

Note that, for any impacted individual confirmed to be a minor as of the date of this notice, we have provided a minor activation code. For all other impacted individuals, we have provided an adult activation code. If you have been provided an adult code but instead require a minor code, or vice versa, please call the Epiq customer care team and notify the agent.

What Else Can You Do?

In addition to enrolling in the complimentary **Epiq - Privacy Solutions ID 1B Credit Monitoring - Plus**, we invite you to review the attached handout titled **STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION**, as well as the U.S. Federal Trade Commission’s safety tips for protecting against identity theft available at www.identitytheft.gov. Moreover, we encourage you to carefully review your accounts and credit reports to ensure that all of the account activity is valid. You should promptly report any questionable charges to the organization with which the account is maintained.

For More Information.

If you have further questions related to the incident, please contact Epiq’s customer care team at **855-720-3747**, Monday-Friday 9:00 a.m. to 9:00 p.m. EST.

Kern takes the privacy and security of your personal information seriously. We genuinely regret any inconvenience this incident may cause you and appreciate your understanding.

Sincerely,

Jennifer Haley
President and CEO
Kern Energy

EPIQ – PRIVACY SOLUTIONS ID

1B Credit Monitoring - Plus

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 including 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.

VantageScore® 3.0 Credit Score and Report¹

1-Bureau VantageScore® 3.0 (annual) and 1-Bureau Credit Report.

SSN Monitoring (High Risk Transaction Monitoring, Real-Time Authentication Alerts, Real-Time Inquiry Alerts)

Detect and prevent common identity theft events outside of what is on your credit report. Real-time monitoring of SSNs across situations like loan applications, employment and healthcare records, tax filings, online document signings and payment platforms, with alerts.

Dark Web Monitoring

Scans millions of servers, online chat rooms, message boards, and websites across all sides of the web to detect fraudulent use of your personal information, with alerts.

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.

Credit Protection

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

Personal Info Protection

Helps users find their exposed personal information on the surface web—specifically on people search sites and data brokers – so that the user can opt out/remove it. Helps protect members from ID theft, robo calls, stalkers, and other privacy risks.

Identity Restoration & Lost Wallet Assistance

Dedicated ID restoration specialists who assist with ID theft recovery and with canceling and reissuing credit and ID cards.

Up to \$1M Identity Theft Insurance²

Provides up to \$1,000,000 (\$0 deductible) Identity Theft Event Expense Reimbursement Insurance on a discovery basis. This insurance aids in the recovery of a stolen identity by helping to cover expenses normally associated with identity theft.

Unauthorized Electronic Funds Transfer- UEFT²

Provides up to \$1,000,000 (\$0 deductible) Unauthorized Electronic Funds Transfer Reimbursement. This aids in the recovery of stolen funds resulting from fraudulent activity (occurrence based).

If you need assistance with the enrollment process or have questions regarding Epiq - Privacy Solutions ID 1B Credit Monitoring - Plus, please call directly at **(866) 675-2006**, Monday-Friday 9:00 a.m. to 5:30 p.m. EST.

¹ The credit scores provided are based on the VantageScore® 3.0 model. For three-bureau VantageScore® credit scores, data from Equifax®, Experian®, and TransUnion® are used respectively. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness.

² Identity Theft Insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. or American Bankers Insurance Company of Florida, an Assurant company. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions, and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity

In addition to enrolling in credit monitoring services, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any suspected identity theft to local law enforcement, your state Attorney General, and the Federal Trade Commission. Be sure to file and obtain a copy of a police report, as many creditors will request a copy to absolve you of fraudulent debts.

To notify the FTC, go to www.ftc.gov/idtheft, call 1-877-ID-THEFT (877-438-4338), or submit a written report to Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your notice will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their further investigation.

Copy of Credit Report

Per federal law, you are entitled to obtain a free copy of your credit report from each of the three national credit reporting agencies (CRA) once every 12 months by visiting www.annualcreditreport.com, calling toll-free 877-322-8228, or completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at www.annualcreditreport.com/manualRequestForm.action. You may also elect to purchase additional copies of your credit report by contacting any of the three national CRAs directly:

Equifax
(800) 685-1111
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
(888) 397-3742
www.experian.com
P.O. Box 2002
Allen, TX 75013

TransUnion
(800) 916-8800
www.transunion.com
P.O. Box 200
Chester, PA 19016

Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, notify the relevant CRA and creditor.

Fraud Alert

You may also consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 12 months (with the option to extend longer for a price). A fraud alert informs creditors of possible fraudulent activity within your credit report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert and for more information, you may contact *any one* of the three national CRAs, the FTC, or visit www.annualcreditreport.com.

Security Freeze

In some U.S. states, you are entitled to place a security freeze on your credit file for free. This will prevent new credit from being opened in your name without the use of a PIN which is issued to you when you initiate the freeze. A security freeze prevents potential creditors from accessing your credit report without your consent or until you temporarily lift the freeze. Thus, using a security freeze may interfere with or delay your ability to obtain credit. Unlike a fraud alert, to place a security freeze, you must separately contact *each* of the three national CRAs. They may require you to provide information that identifies you (e.g., your full name, Social Security number, date of birth, current or previous addresses, copy of your state-issued identification card, recent utility bill, bank statement, or insurance statement). To temporarily lift or permanently remove the security freeze and allow an entity or individual access to your credit report, you must likewise submit a request to *each* CRA and provide the PIN from that specific CRA. For more information on security freezes in your state, you may contact the three national CRAs or the FTC.

District of Columbia Residents: You may contact the District of Columbia Attorney General's Office to obtain information on how to avoid identity theft by visiting www.oag.dc.gov or calling 202-727-3400.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft by visiting www.iowaattorneygeneral.gov, calling 515-281-5164, or via mail at Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319.

Maryland Residents: You may contact the Maryland Attorney General's Office to obtain information about preventing identity theft by visiting www.marylandattorneygeneral.gov, calling 888-743-0023, or via mail at Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202.

New Mexico Residents: You have certain rights under the federal Fair Credit Reporting Act (FCRA), including among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. Identity theft victims have specific additional rights pursuant to the FCRA. For more information about the FCRA, please visit www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or contact the FTC by visiting www.ftc.gov or via mail at Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: You may contact the New York Attorney General's Office by visiting www.ag.ny.gov, calling 800-771-7755, or via mail at Office of the Attorney General, The Capitol, Albany, NY 12224.

North Carolina Residents: You may contact the North Carolina Attorney General's Office to obtain information about preventing identity theft by visiting www.ncdoj.gov, calling 877-566-7226, or via mail at 9001 Mail Service Center, Raleigh, NC 27699.

Oregon Residents: State law advises you to report any suspected identity theft to law enforcement, the Oregon Attorney General, and the Federal Trade Commission. You may contact the Oregon Attorney General's Office to report suspected identity theft or obtain information about preventing identity theft by visiting www.doj.state.or.us, calling 877-877-9392, or via mail at Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301.

Rhode Island Residents: You may contact the Rhode Island Attorney General's Office to report suspected identity theft or obtain information about preventing identity theft by visiting www.riag.ri.gov, calling 401-274-4400, or via mail at 150 South Main Street, Providence, RI 02903. Per state law, you have the right to obtain any police report filed regarding this incident.