

Appendix

On February 21, 2026, Murray's Cheese LLC ("Murray's") detected unusual activity within its network that caused certain devices to become unavailable. Murray's immediately implemented its response protocols, took measures to contain the activity, and launched an investigation. A cybersecurity firm that has assisted other companies in similar situations also was engaged.

The evidence showed there was unauthorized activity within the Murray's network between February 15, 2026 and February 21, 2026. During this period, an unauthorized actor viewed and obtained files stored in the network. Murray's conducted a careful review of the files and, on April 3, 2026 determined that one or more of the files contained information relating to five Maine residents. The information included their names, Social Security numbers, dates of birth, and health insurance plan enrollment information. The information also may have included their health insurance member numbers, driver's license numbers or state-issued identification card numbers, passport numbers, other government-issued identification numbers, financial account information, and, if they filed a claim for workers compensation or disability, medical information related to their claim.

Today, April 21, 2026, Murray's is mailing notification letters pursuant to the Health Insurance Portability and Accountability Act and, if applicable, state law via United States Postal Service First-Class mail to the involved Maine residents. A copy of the letter template is enclosed. Murray's is offering one year of complimentary credit monitoring and identity theft protection services to the individuals whose Social Security numbers, driver's license numbers, or state identification card numbers were involved. Murray's also has established a toll-free call center that individuals can call with questions.

To help prevent something like this from happening again, Murray's has taken and is taking steps to enhance its existing security measures.



Secure Processing Center
25 Route 111, P.O. Box 1048
Smithtown, NY 11787

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>>:

Murray's Cheese LLC ("Murray's") understands the importance of protecting information. We are writing to inform you that we recently identified and addressed a data security incident involving your information. This notice explains the incident, measures we have taken, and additional steps you may consider taking in response.

What Happened?

On February 21, 2026, we detected unusual activity within our network that caused certain devices to become unavailable. We immediately implemented our response protocols, took measures to contain the activity, and launched an investigation. A cybersecurity firm that has assisted other companies in similar situations also was engaged.

The evidence showed there was unauthorized activity within our network between February 15, 2026 and February 21, 2026. During this period, an unauthorized actor viewed and obtained files stored in our network, including information related to our employee health plan. We conducted a careful review of the files and, on April 3, 2026, determined that one or more of the files contained your information.

What Information Was Involved?

The information included your name, Social Security number, date of birth, and health insurance plan enrollment information. The information also may have included your health insurance member number, driver's license number or state-issued identification card number, passport number, other government-issued identification number, financial account information, and, if you filed a claim for workers compensation or disability, medical information related to your claim.

What We Are Doing.

We wanted to notify you of this incident and to assure you that we take it seriously. We have arranged for you to receive <<CM Duration>> of access to Epiq Privacy Solutions ID Credit Monitoring, as discussed below. Additionally, to help prevent something like this from happening again, we have taken and are taking steps to enhance our existing security measures.

What You Can Do.

You can enroll in the complimentary credit monitoring product we have arranged for you. This product helps detect possible misuse of your information and provides you with identity protection solutions focused on immediate identification and resolution of identity theft. Activating this product will not hurt your credit score. For more information on identity theft prevention and Epiq Privacy Solutions ID Credit Monitoring, including instructions on how to activate your access, as well as some additional steps you can take in response, please review the pages that follow this letter.

For More Information.

We regret that this occurred and apologize for any inconvenience. If you have any questions, please contact us at 888-504-8280, Monday through Friday, between 9:00 a.m. and 9:00 p.m. ET

Sincerely,

Murray's Cheese LLC



<<Full Name>>

Activation Code: <<ACTIVATION CODE>>

Enrollment Deadline: <<ENROLLMENT DEADLINE>>

Coverage Length: <<CM Duration>>

Epiq - Privacy Solutions ID 3B Credit Monitoring

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:

3-Bureau Credit Monitoring with Alerts

Monitors your credit file(s) with each of the 3 Credit Bureaus for key changes, with alerts such as credit inquiries, new accounts, and public records.

VantageScore® 3.0 Credit Score with Score Tracker¹

1-Bureau VantageScore®3.0 (monthly) and Credit Score Tracker.

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 assist 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 3B Credit Monitoring, please call directly at **866.675.2006**, Monday-Friday 9:00 a.m. to 5:30 p.m., ET.

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.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-888-378-4329
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-833-799-5355

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.identitytheft.gov

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Protecting Health Insurance or Medical Information: It is always advisable to review any statements you may receive from your health insurer or healthcare providers. If you see charges for services that you did not receive, contact your insurer or provider immediately.

Murray's Cheese LLC is located at 254 Bleecker St., New York, NY 10014 and can be reached at 212-243-3289.

Additional Information for Residents of the Following States:

Connecticut: You may contact and obtain information from your state attorney general at: *Connecticut Attorney General's Office*, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

District of Columbia: You may contact and obtain information from your attorney general at: Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov

Massachusetts: Under Massachusetts law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

New York: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov