

APPENDIX

illumifin Corporation (“illumifin”) is an insurance technology company that provides third-party administration services to insurance carriers. illumifin is providing this notice on behalf of its insurance-carrier clients that delegated their notification obligations to illumifin.

On November 4, 2025, illumifin identified unusual activity in a portion of its network. illumifin immediately implemented its incident response protocols, which involved taking steps to contain the activity and launching an investigation with assistance from a third-party forensic firm. illumifin also notified law enforcement. The investigation determined that an unauthorized person gained access to illumifin’s network and acquired copies of certain files stored on its system. On November 10, 2025, illumifin learned that some of the files may have contained information it received from or on behalf of its insurance carrier-clients in connection with the administration services it provides. Accordingly, illumifin conducted a comprehensive, multi-phase review and analysis of the files to identify the individuals whose information was contained therein and the insurance carrier from whom illumifin received the information. illumifin began informing applicable data owners (*i.e.*, its insurance carrier-clients) on January 9, 2026, and provided them with their list of involved individuals on or around February 25, 2026. Since that time, illumifin has been working with its insurance carrier-clients to prepare to notify involved individuals.

Today, March 13, 2026, on behalf of its insurance-carrier clients, illumifin began mailing notification letters via First-Class mail in accordance with the Health Insurance Portability and Accountability Act (45 CFR § 164.404) and/or Neb. Rev. Stat. § 87-803 to three Nebraska residents, whose names and Social Security numbers were contained in the files. A copy of the notification letter template is enclosed. illumifin is offering the Nebraska residents a complimentary membership to credit monitoring and identity protection services. Additionally, illumifin has established a dedicated, toll-free call center that individuals can call to obtain more information about the incident.

To help prevent something like this from happening again, illumifin has implemented, and will continue to adopt, additional safeguards to further protect and monitor its systems.



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>>:

illumifin Corporation (“illumifin”) is an insurance technology company and third-party administrator who provides services for <<Variable Data 2>>, on whose behalf we are sending this letter. We are committed to protecting the confidentiality and security of the information we maintain related to those services. Regrettably, we are writing to inform you of an incident involving some of your information. This letter explains the incident, measures we have taken in response, and steps you can take to further protect your information.

What Happened? On November 4, 2025, we identified unusual activity in a portion of our network. We immediately implemented our incident response protocols, which involved taking steps to contain the activity and launching an investigation with assistance from a third-party forensic firm. We also notified law enforcement. The investigation determined that an unauthorized person gained access to our network and acquired copies of certain files stored on our system. On November 10, 2025, we learned that some of the files may have contained information we received from or on behalf of our clients in connection with the administration services we provide. Accordingly, we conducted a comprehensive review and analysis of the files to determine what information they contained. We informed <<Variable Data 2>> of the incident on January 9, 2026, and, following completion of our comprehensive review, provided them with their list of affected individuals on or around February 25, 2026.

What Information Was Involved? Through our review, we identified files containing some of your information, including your <<Breached Elements>>.

What We Are Doing. We wanted to notify you of this incident and assure you we take this matter very seriously. As a precaution, we have arranged for you to receive a <<CM Duration>> month complimentary membership to identity monitoring services through Epiq - Privacy Solutions ID. Additionally, to help prevent a similar incident from occurring in the future, we have implemented, and will continue to adopt, additional safeguards to further protect and monitor our systems.

What You Can Do. Remain vigilant for incidents of fraud or identity theft by regularly reviewing your account statements and free credit reports for any unauthorized activity. For additional guidance on identity theft prevention and Epiq - Privacy Solutions ID, including instructions on how to activate your complimentary membership, please see the pages that follow this letter.

For More Information. We regret that this incident occurred and apologize for any inconvenience. If you have questions, please call 844-558-4433, Monday through Friday, between 8:00 a.m. and 8:00 p.m., Central Time.

Sincerely,
illumifin Corporation



<<Full Name>>

Activation Code: <<ACTIVATION CODE>>

Enrollment Deadline: <<ENROLLMENT DEADLINE>>

Coverage Length: <<CM Duration>> 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.

ADDITIONAL STEPS YOU CAN TAKE

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, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

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: 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.

illumifin Corporation can be reached by mail at 7805 Hudson Road, Suite 180, Woodbury, MN 55125 or by phone at (877) 431-5824.

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*, 441 4th Street NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov

Maryland: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

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

Rhode Island: Approximately <<RI Count>> residents are receiving notice of this incident. Under Rhode Island 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: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street NW, Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.

- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.