



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>>

NOTICE OF DATA BREACH

Dear <<Full Name>>:

At Insurance Office of America ("IOA"), we value and respect the privacy of your information, which is why we are writing to provide an update to you about a recent incident that may have involved some of your information. Although we have no evidence to suggest that your information was or will be misused in any way, we are notifying you out of an abundance of caution and to provide you with information and resources to help protect your personal information.

WHAT HAPPENED?

On May 14, 2026, while sending a routine benefits-related email to individuals who participated in one or more IOA benefit plans during the 2024–2025 plan year, an IOA employee inadvertently attached a document containing some personal information to the email. Upon discovering the error, we immediately took steps to address the error, including initiating the recall process within minutes of the original email being sent, and promptly commenced an internal investigation.

WHAT INFORMATION WAS INVOLVED?

Our investigation determined that the attached report included your name and certain personal information, including protected health information. The information contained in the shared file included your name, Social Security number, and health insurance and benefit plan enrollment information, such as insurance elections, coverage, and contribution amounts.

WHAT WE ARE DOING

Upon learning of this incident, we took immediate action to contain and remediate the situation. We successfully recalled and deleted the message from internal mailboxes, and our investigation confirmed that the recall was effective for internal recipients. We also obtained signed attestations from the majority of recipients confirming that the information was permanently deleted and was not saved, copied, transferred, or otherwise disclosed. In addition, we have implemented enhanced safeguards, including additional training for our team and strengthened review procedures for outbound communications containing sensitive information.

Although we have no information to date indicating that your information involved in this incident was or will be used for any unintended purposes, we wanted to notify you of the incident out of an abundance of caution. In addition, to help relieve concerns and restore confidence following this incident, we have arranged for you to enroll, at no cost to you, in complimentary credit monitoring and identity protection services for 24 months through Epiq. Please carefully read the remainder of this letter to learn about these services and instructions on how to enroll within the "Other Important Information" document enclosed.

WHAT YOU CAN DO

Please review the enclosed "Other Important Information" document for further steps you can take to protect your information, including recommendations from the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or security freeze on your credit file. It is also recommended that you remain vigilant for incidents of fraud and identity theft by reviewing your account statements and monitoring your credit reports for unauthorized activity. If you discover any suspicious or unusual activity on your accounts, promptly notify the financial institution or company with which your account is maintained.

Although we have no information to date indicating that your health information has been or will be used for any unintended purposes, as a general matter, the following practices can help protect you from medical identity theft:

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help with your medical care.
- Review your Explanation of Benefits ("EOB") statements from your health insurance company and follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider listed on the EOB and ask for copies of medical records from the time frame of the incident (noted above) to the current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary and follow up with your insurance company or care provider for any items you do not recognize.

FOR MORE INFORMATION

If you have questions or need assistance, please call our dedicated incident response line at 1-866-659-7141 between 8:00 a.m. and 8:00 p.m. Central Time, Monday through Friday, excluding holidays.

Sincerely,

Robert Peters
Chief Operating Officer
Insurance Office of America

OTHER IMPORTANT INFORMATION

Free Credit Report. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the nationwide credit reporting agencies. To order your annual free credit report please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's (FTC) website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Contact information for the national credit reporting agencies for the purpose of requesting a copy of your credit report and other general inquiries is provided below:

- **Equifax**, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- **Experian**, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742
- **TransUnion**, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213
- **Innovis**, PO Box 1689, Pittsburgh, PA 15230-1689, www.innovis.com, 1-800-540-2505

Fraud Alert. You have the right to place an initial or extended "fraud alert" on your file at no cost by contacting any of the nationwide credit reporting agencies. Contact information for the national credit reporting agencies for the purposes of placing a fraud alert on your file is provided below. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert displayed on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. For this reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. If you are a victim of identity theft and have filed an identity theft report with law enforcement, you may want to consider placing an extended fraud alert, which lasts for 7 years, on your credit file.

- **Equifax**, PO Box 105069, Atlanta, GA 30348-5069, www.equifax.com/personal/credit-report-services/credit-fraud-alerts, 1-800-525-6285
- **Experian**, PO Box 9554, Allen, TX 75013, www.experian.com/fraud/center.html, 1-888-397-3742
- **TransUnion**, PO Box 2000, Chester, PA 19016, www.transunion.com/fraud-alerts, 1-800-680-7289
- **Innovis Consumer Assistance**, PO Box 26, Pittsburgh, PA 15230-0026, <https://www.innovis.com/personal/fraudActiveDutyAlerts>, 1-800-540-2505

Security Freeze. You have the right to place, lift, or remove a "security freeze" on your credit report, free of charge. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. Under federal law, you cannot be charged to place, lift, or remove a security freeze. You must place your request for a freeze separately with each of the consumer reporting agencies. To place a security freeze on your credit report, you may do so by contacting each of the consumer reporting agencies through the contact information below:

- **Equifax**, PO Box 105788, Atlanta, GA 30348-5788, www.equifax.com/personal/credit-report-services/credit-freeze, 1-800-298-0045
- **Experian**, PO Box 9554, Allen, TX 75013, www.experian.com/freeze/center.html, 1-888-397-3742
- **TransUnion**, PO Box 160, Woodlyn, PA 19094, www.transunion.com/credit-freeze, 1-888-909-8872
- **Innovis**, PO Box 26, Pittsburgh, PA 15230-0026, www.innovis.com/personal/securityFreeze, 1-800-540-2505

In order to request a security freeze, you will need to provide some or all of the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past 5 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have 1 business day after receiving your request by toll-free telephone or secure electronic means, or up to 3 business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within 5 business days and may provide you with a unique personal identification number (PIN) or password (or both) that can be used by you to authorize the removal or lifting of the security freeze. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have 1 business day after receiving your request by toll-free telephone or secure electronic means, or 3 business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the credit bureaus and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have 1 business day after receiving your request by toll-free telephone or secure electronic means, or 3 business days after receiving your request by mail, to remove the security freeze.

Federal Trade Commission and State Attorneys General Offices. 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 FTC, proper law enforcement authorities and/or your state attorney general. You may also contact these agencies for information on how to prevent or avoid identity theft and to obtain additional information about fraud alerts and security freezes. You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (438-4338).

- **California residents:** You may also wish to review the information provided by the California Attorney General at <https://oag.ca.gov/idtheft>.
- **District of Columbia residents:** You may also obtain information about avoiding identity theft from the Office of the Attorney General for the District of Columbia at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.
- **Iowa residents:** You are advised to report suspected incidents of identity theft to law enforcement or the Iowa Attorney General's Office at Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, tel.: (515) 281-5926 or (888) 777-4590.
- **Maryland residents:** You may obtain information about avoiding identity theft from the Maryland Office of the Attorney General at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.
- **For Massachusetts residents,** you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. You also have the right to request a security freeze, as described above.
- **New Mexico residents:** Consumers have rights pursuant to the Fair Credit Reporting Act ("FCRA"), such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the FCRA, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the FCRA not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the FCRA. We encourage consumers to review their rights pursuant to the FCRA by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, FTC, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.
- **New York residents:** You may obtain additional information about security breach response and identity theft prevention and protection from the New York State Office of the Attorney General by calling 1-800-771-7755 or visiting <https://ag.ny.gov>; the New York State Police by calling 1-518-457-6721 or visiting <https://troopers.ny.gov/>; and/or the New York Department of State by calling 1-800-697-1220 or visiting <https://www.dos.ny.gov>.
- **North Carolina residents:** You may obtain additional information about preventing identity theft provided by the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.
- **Oregon residents:** You are advised to report any suspected incidents of identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General at <https://doj.state.or.us>, by calling (877) 877-9392, or writing to Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096.
- **Rhode Island residents:** You may contact the Rhode Island Attorney General at: Rhode Island Office of the Attorney General, 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. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. There are approximately 2 Rhode Island residents who may be impacted by this event.
- **Vermont residents:** If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-828-3171.



Activation Code: <<ACTIVATION CODE>>
Enrollment Deadline: <<ENROLLMENT DEADLINE>>
Coverage Length: 24 Months

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 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.

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 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 1B Credit Monitoring - Plus, 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.