Integrated Specialty Coverages, LLC
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

P
[redacted]

[redacted]

June 18, 2025

Dear [redacted]:

0000101102G0500

P

Integrated Specialty Coverages, LLC ("ISC" or "we") is writing to inform you of a recent security incident. ISC is an insurance program administrator that provides insurance products and underwriting services. Your information may have been provided to ISC by your employer, an insurance company or broker in connection with an insurance application, or as part of an insurance claim.

We have been working with external cybersecurity experts and federal law enforcement to investigate this situation. We have no evidence at this time that any information has been misused as a result of this incident.

What Happened? Our security tools detected suspicious activity in a portion of our environment that we determined to be a security incident. Upon discovering the incident, ISC promptly contained the incident, notified law enforcement, and engaged external cybersecurity experts to investigate. The investigation determined that an unauthorized third party accessed a limited portion of ISC's environment between February 16 and February 19, 2025.

What Information Was Involved? We have been performing a thorough review of the potentially impacted files to determine what data may have been involved. Based on this review, we have identified files containing your personal information, including your name, in combination with one or more of the following: social security and/or tax ID number, date of birth, driver's license or other government ID number, biometric data (fingerprint image or similar), and basic medical information provided to ISC in connection with an insurance application or claim.

What We Are Doing. In addition to the actions described above, we have taken steps to enhance our technical security measures. We are also providing you with resources and tools to help you protect your personal information, and we are offering credit monitoring and identity protection services to you for twelve (12) months free of charge. You can enroll in these services through Cyberscout, a TransUnion company, at no cost to you, and doing so will not hurt your credit score. **For more information, including instructions on how to activate your complimentary credit monitoring, please see the additional information provided in this letter.**

What You Can Do. While we have no evidence that your personal information has been misused, we encourage you to take advantage of the complimentary credit monitoring included in this letter. You can also find more information on steps that can be taken to protect against possible identity theft or fraud in the enclosed *Additional Important Information* sheet.

For More Information. We take the privacy of your personal information seriously here at ISC. For further information and assistance, please call [redacted] from 8:00 a.m. until 8:00 p.m. Eastern Time, Monday through Friday, excluding major U.S. holidays.

Sincerely,

Integrated Specialty Coverages, LLC

DETAILS REGARDING YOUR CYBERSCOUT MEMBERSHIP

We are offering you complimentary access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

To activate your membership and start monitoring your credit, please follow the steps below:

- Ensure that you **enroll within 90 days from the date of this letter** (Your code will not work after this date.)
- **Visit** the Cyberscout website to enroll: **www.mytrueidentity.com**
- **Unique code:** [redacted]
- 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 Important Information

1. Review your Credit Reports. We recommend that you monitor your credit reports for any activity you do not recognize. Under federal law, you are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To order your free annual credit report, visit www.annualcreditreport.com, call toll-free (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

If you see anything in your credit report that you do not understand, call the credit bureau at the telephone number on the report. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing.

2. Place Fraud Alerts. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. Please note that placing a fraud alert may delay you when seeking to obtain credit. You can learn more about fraud alerts by contacting the credit bureaus or by visiting their websites:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

It is only necessary to contact one of these bureaus and use only one of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You should receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review.

3. Place Security Freezes. By placing a security freeze, someone who fraudulently acquires your personally identifying information will not be able to use that information to open new accounts or borrow money in your name. Federal and state laws prohibit charges for placing, temporarily lifting, or removing a security freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze.

To place a security freeze, you must contact each of the three national credit reporting bureaus listed above and provide the following information: (1) your full name; (2) your social security number; (3) date of birth; (4) the addresses where you have lived over the past two years; (5) proof of current address, such as a utility bill or telephone bill; (6) a copy of a government issued identification card; and (7) if you are the victim of identity theft, include the police report, investigative report, or complaint to a law enforcement agency. If the request to place a security freeze is made by toll-free telephone or secure electronic means, the credit bureaus have one business day after receiving your request to place the security freeze on your credit report. If the request is made by mail, the credit bureaus have three business days to place the security freeze on your credit report after receiving your request. The credit bureaus must send confirmation to you within five business days and provide you with information concerning the process by which you may remove or lift the security freeze. There is no cost to place a security freeze.

4. Request an IP PIN from the IRS. Although the IRS is capable of identifying suspicious tax returns, taxpayers may choose to take proactive steps to prevent fraud, including obtaining an Identity Protection PIN (IP PIN) from the IRS. The IP PIN is a 6-digit number that, when active, will be required to file a tax return using the taxpayer's SSN or ITIN. To request an IP PIN, visit https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin.

In addition, taxpayers may opt in to ID.me, an identity verification service that requires a photo ID or live video session before logging in to submit a tax return online.

Finally, taxpayers may submit IRS Form 14039, Identity Theft Affidavit online if they received IRS correspondence indicating they might be a victim of tax-related identity theft or if their e-file tax return was rejected as a duplicate. After submitting the form, the IRS will refer the taxpayer's case to the Identity Theft Victim Assistance organization to investigate the case, remove fraudulent returns, and process the correct return and refund.

5. Monitor Your Account Statements. We encourage you to carefully monitor your financial account statements for fraudulent activity and report anything suspicious to the respective institution or provider.

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

District of Columbia Residents: District of Columbia residents can contact the Office of the Attorney general to obtain information about steps to take to avoid identity theft from the Office of the Attorney General for the District of Columbia at 441 4th Street, NW, Washington, DC 20001, 202-727-3400, oag@dc.gov, https://oag.dc.gov/. The District of Columbia law also allows consumers to place a security freeze on their credit reports without any charge.

Iowa Residents: Iowa residents can contact the Office of the Attorney general to obtain information about steps to take to avoid identity theft from the Iowa Attorney General's office at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines IA 50319, 515-281-5164.

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's office at: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, http://www.marylandattorneygeneral.gov/.

Massachusetts Residents: You have a right to file a police report and obtain a copy of your records. You can obtain additional information about identity theft prevention and protection from the Office of Consumer Affairs and Business Regulation, 501 Boylston Street, Suite 5100, Boston, MA 02116, (617) 973-8787, https://www.mass.gov/service-details/identity-theft.

New Mexico Residents: Individuals have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

New York State Residents: New York residents can obtain information about preventing identity theft from the New York Attorney General's Office at: Office of the Attorney General for the State of New York, Bureau of Consumer Frauds & Protection, The Capitol, Albany, New York 12224-0341; https://ag.ny.gov/consumer-frauds/identity-theft; (800) 771-7755.

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov.

Oregon Residents: Oregon residents are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General. Oregon residents can contact the Oregon Attorney General at 1162 Court St. NE, Salem, OR 97301-4096; 503-378-4400; https://www.doj.state.or.us/.

Rhode Island Residents: We believe that this incident affected [redacted] Rhode Island residents. Rhode Island residents can contact the Office of the Attorney general at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. 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.

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 802-656-3183 (800-649-2424 toll free in Vermont only).