NOTICE OF POTENTIAL DATA EVENT

Issaquah Financial d/b/a for Highlands Insurance & Retirement Solutions LLC ("Issaquah Financial") is providing notice of an event that may affect the privacy of certain information. Although we are unaware of any identity theft or fraud in relation to the event, we are providing information about the event, our response, and additional measures individuals can take to help protect their information, should they feel it appropriate to do so. **Please note, not all Issaquah Financial clients are impacted by this event.**

What Happened? On October 3, 2024, Issaquah Financial began investigating suspicious activity concerning a single Issaquah Financial employee email account. Upon learning of the suspicious activity, we quickly disabled the account, revoked active sessions, reset the account's credentials, and launched an investigation with the assistance of third-party cybersecurity and data privacy specialists. On October 18, 2024, the investigation determined that an unauthorized actor logged into the email account from September 30, 2024, to October 3, 2024. Although the investigation was unable to confirm whether any sensitive Issaquah Financial client information was viewed by the unauthorized actor, we next conducted a thorough review of the email account's contents with the assistance of third-party specialists to identify potentially impacted individuals and associated types of data in an abundance of caution.

What Information Was Involved? While the actual types of information affected may vary by individual, our recently concluded review determined that the following types of personal information were stored within the impacted email account at the time of the event: name, date of birth, digital signature, driver's license and/or state ID number, financial account information, health information, payment card information, Social Security number, passport number, and biometric information. Again, Issaquah Financial is not aware of any actual or attempted identity theft or fraud in relation to this event.

What We Are Doing. The confidentiality, privacy, and security of information in our care is among our highest priorities. Upon learning of the suspicious activity, we quickly disabled the account, revoked active sessions, reset the account's credentials, and commenced an investigation to confirm the nature and scope of the event. We are reviewing existing security policies and have implemented additional cybersecurity measures to further protect against similar events moving forward. Additionally, we are also notifying potentially impacted individuals so they may take steps to best protect their information, should they feel it is appropriate to do so.

For More Information. If you have additional questions, please call (855) 659-0105 from 6:00 a.m. PT to 6:00 p.m. PT, Monday through Friday, excluding major U.S. holidays. You may also write to us at 185 2nd Avenue Southeast, Issaquah, Washington 98027.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements as well as monitoring your free credit reports for suspicious activity and to detect errors over the next twelve (12) to twenty-four (24) months. Under U.S. law, a consumer is entitled to one (1) free credit report annually from each of the three (3) major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit https://www.annualcreditreport.com or call, toll-free, 1 (877) 322-8228. Consumers may also directly contact the three (3) major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one (1) year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven (7) years. Should consumers wish to place a fraud alert, please contact any of the three (3) major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two (2) to five (5) years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three (3) major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/data-breach-help/
1 (888) 298-0045	1 (888) 397-3742	1 (833) 799-5355
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

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; https://www.identitytheft.gov; 1 (877) ID-THEFT (1 (877) 438-4338); and TTY: 1 (866) 653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be promptly reported to law enforcement, the relevant state Attorney General, and the Federal Trade Commission. This notice has not been delayed by law enforcement.