EXHIBIT 1

This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Issaquah Financial d/b/a for Highlands Insurance & Retirement Solutions LLC ("Issaquah Financial") does not waive any rights or defenses regarding the applicability of Washington law, the applicability of the Washington data event notification statute, or personal jurisdiction.

Nature of the Data Event

On October 3, 2024, Issaquah Financial began investigating suspicious activity concerning a single Issaquah Financial employee email account. Upon learning of the suspicious activity, Issaquah Financial 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, Issaquah Financial undertook a comprehensive and time-intensive review of the email account's contents with the assistance of third-party specialists to identify potentially impacted individuals whose personal information was potentially impacted within the email account. This review was completed on January 24, 2024. Issaquah Financial then worked to validate the results of this review and locate address information for potentially impacted individuals to notify them.

The potentially impacted types of information relating to Washington residents may vary by individual and include 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.

Notice to Washington Residents

On March 21, 2025, Issaquah Financial began mailing written notice of this incident to seven hundred ninety-five (795) Washington residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon learning of the suspicious activity, Issaquah Financial 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. Issaquah Financial is reviewing existing security policies and has implemented additional cybersecurity measures to further protect against similar events moving forward. As an added precaution, Issaquah Financial is providing access to complimentary credit monitoring services for twelve (12) months, through Epiq, to individuals whose personal information was potentially affected by this incident.

Additionally, Issaquah Financial is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Issaquah Financial is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Issaquah Financial is also providing written notice of this incident to other relevant state regulators, as necessary.

EXHIBIT A

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 <<Variable Data 1>>

Dear <<Full Name>>:

Issaquah Financial d/b/a for Highlands Insurance & Retirement Solutions LLC ("Issaquah Financial") writes to inform you of an event that may affect the privacy of some of your information. Although we are unaware of any identity theft or fraud in relation to the event, we are providing you with information about the event, our response, and additional measures you can take to help protect your information, should you feel it appropriate to do so.

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? 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: your <<Breached Elements>>. 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, including you, so they may take steps to best protect their information, should they feel it is appropriate to do so.

As an added precaution, we are offering you immediate access to credit monitoring and identity theft protection services for <<CM Duration>> at no cost to you, through Equifax. You can find information on how to enroll in these services in the enclosed *STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION*. We encourage you to enroll in these services as we are not able to do so on your behalf.

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. Please also review the information contained in the enclosed *STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION*.

For More Information. We understand that you may have questions about this event that are not addressed in this letter. 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. We take this event very seriously and sincerely regret any inconvenience or concern this event may cause you.

Sincerely,

Stephen J. Cooke
Issaquah Financial

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

EQUIFAX®

Enter your Activation Code: *<<Activation Code>>*
Enrollment Deadline: *<<Enrollment Deadline>>*

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications[1] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[2], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[3]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[4]

Enrollment Instructions

Go to **https://www.equifax.com/activate**

Enter your unique Activation Code of *<<ACTIVATION CODE>>* then click "Submit" and follow these four (4) steps:

1. **Register:**
   Complete the form with your contact information and click "Continue".
   If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. **Create Account:**
   Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
   To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout**:
   Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling.

   You're done!
   The confirmation page shows your completed enrollment.
   Click "View My Product" to access the product features.

[1]WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded. *[2]The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.* *[3]Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com* *[4]The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.*

Monitor Your Accounts

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

Additional Information

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.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1 (877) 566-7226 or 1 (919) 716-6000; and https://www.ncdoj.gov.