# EXHIBIT 1

By providing this notice, Zalaznik & Associates 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 March 11, 2026, Zalaznik & Associates detected suspicious activity within their virtual office tax e-file system. Upon learning of the activity, Zalaznik & Associates quickly took actions to ensure their network and systems were secure and launched an investigation into the nature and scope of the event. The investigation determined that an unauthorized actor gained access to their systems between September 22, 2025 and March 11, 2026 and accessed certain files.

As part of the investigation, Zalaznik & Associates conducted a thorough review of the impacted data to determine what information was involved and to whom it relates. On April 29, 2026, the review determined that information related to individuals was within the accessed files.

The information that could have been impacted includes name, Social Security number, and financial account information.

## Notice to Washington Residents

On or about May 29, 2026, Zalaznik & Associates provided written notice of this incident to six hundred eighty-five (685) 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 identifying the event, Zalaznik & Associates moved quickly to report the event to the IRS, investigate and respond to the incident, assess the security of Zalaznik & Associates systems, and identify potentially affected individuals. Further, Zalaznik & Associates notified federal law enforcement regarding the event. Zalaznik & Associates is also working to implement additional safeguards and training to its employees. Zalaznik & Associates is providing access to credit monitoring services for 1 year, through TransUnion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Zalaznik & Associates is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Zalaznik & Associates is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, 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. Zalaznik & Associates is providing written notice of this incident to relevant state and federal regulators, as necessary.

# EXHIBIT A

Zalaznik & Associates, PLLC
c/o Cyberscout
P.O. Box 3826
Suwanee, GA 30024

Zalaznik & Associates, PLLC
Accountants and Business Consultants

5 1 821 *******************AUTO**MIXED AADC 302
[redacted]

May 29, 2026

**NOTICE OF SECURITY INCIDENT**

Dear [redacted]:

Zalaznik & Associates, PLLC ("Zalaznik & Associates") writes to inform you of a recent event that impacts some of your information. Zalaznik & Associates takes this event very seriously, and the confidentiality, privacy, and security of information in our care is among our highest priorities. We are providing you with an overview of the event, our response, and resources to help further protect your information, should you feel it necessary to do so.

**What Happened?**

On March 11, 2026, Zalaznik & Associates detected suspicious activity within our virtual office tax e-file system. Upon learning of this activity, Zalaznik & Associates quickly took actions to ensure our network and systems were secure and launched an investigation into the nature and scope of the event. The investigation determined that an unauthorized actor gained access to our system between September 22, 2025 and March 11, 2026 and accessed certain files.

As part of the investigation, Zalaznik & Associates conducted a thorough review of the impacted data to determine what information may be involved and to whom the information relates. The review concluded on April 29, 2026, and determined that information related to you was within the accessed files.

**What Information Was Involved?**

The information related to you that was identified in the review includes your name and the following data elements: Social Security number, financial account information.

**What We Are Doing**.

Zalaznik & Associates takes this event and the security of information in our care very seriously. Upon learning of the event, Zalaznik & Associates took quick steps to ensure the security of its system, respond to the event, and launch an investigation. Zalaznik & Associates is also notifying relevant regulators, as required. Additionally, Zalaznik & Associates reported this event to the IRS and is taking steps with appropriate IRS departments to ensure all returns filed by our office are secure. As part of our ongoing commitment to information security, we are reviewing our policies and procedures and have bolstered our system security measures to reduce the risk of a similar event from occurring in the future.

Zalaznik & Associates is also offering twelve (12) months of complimentary credit monitoring through Cyberscout, a TransUnion company specializing in fraud assistance and remediation services. You must enroll in these services yourself as Zalaznik & Associates cannot do so on your behalf. Enrollment instructions can be found in the enclosed *Steps You Can Take to Help Protect Your Information* below.

**What You Can Do.**

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors over the next 12 to 24 months. We also encourage you to report instances of suspected tax fraud or return issues to our team and the IRS. Please review the enclosed *Steps You Can Take to Help Protect Personal Information*, which includes further information on what you can do to protect your information against misuse, should you feel it necessary to do so. Additionally, Zalaznik & Associates encourages you to enroll in the complimentary credit monitoring being offered.

**For More Information.**

Zalaznik & Associates understands that you may have questions about this event not addressed in the letter. Should you have additional questions, please contact our dedicated assistance line at 1-800-405-6108. Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. You may also write to Zalaznik & Associates at PO Box 1724, Walla Walla, WA 99362.

We sincerely apologize for any inconvenience this may cause.

Sincerely,

*Zalaznik & Associates, PLLC*

**STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION**

**Enroll in Monitoring Services**

To enroll in Credit Monitoring services at no charge, please log on to https://bfs.cyberscout.com/activate and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. 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.

**Monitor Your Accounts**

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three 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 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 years. Should consumers wish to place a fraud alert, please contact any of the three 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 to five 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 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, 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, P.O. Box 160, Woodlyn, PA 19094 |

**Internal Revenue Service Identity Protection PIN (IP PIN)**

You may also obtain an Identity Protection PIN (IP PIN) from the Internal Revenue Service, a six-digit number that prevents someone else from filing a tax return using your Social Security number or Individual Taxpayer Identification Number. The IP PIN is known only to you and the IRS, and helps the IRS verify your identity when you file your electronic or paper tax return. Even though you may not have a filing requirement, an IP PIN still protects your account. If you do not already have an IP PIN, you may get an IP PIN as a proactive step to protect yourself from tax-related identity theft either online, by paper application or in-person. Information about the IP PIN program can be found here: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin. You may also visit https://www.irs.gov/identity-theft-fraud-scams/identity-theft-guide-for-individuals for additional information and resources on how to protect against tax fraud.

**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; 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 reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

*For Maryland residents*, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

*For New Mexico residents*, consumers have rights pursuant to the Fair Credit Reporting Act, 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 Fair Credit Reporting Act, 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 Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.