



0001543

Sadler Gibb & Associates
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
USBFS2981



[Redacted]
[Redacted]
[Redacted]



February 27, 2026

Dear [Redacted]:

Sadler Gibb & Associates (“Sadler Gibb”) writes to inform you of a recent data event that may affect certain information related to you. Please note, Massachusetts law restricts the information Sadler Gibb is permitted to include in this letter. However, we take this matter seriously, and write to provide you with the information we are able to provide, as well as information regarding resources we are making available to you. The information identified in connection with this data event may include your name and [Redacted].

In response to this event, we took steps to secure our network environment and conduct an investigation into the activity. We also notified federal law enforcement. Once the information that may have been impacted was identified, we diligently reviewed the information and began gathering resources to provide notification to identified individuals. We understand the importance of safeguarding information in our care and have taken steps to further enhance our existing infrastructure, as well as implement additional policies and procedures to help prevent a similar event from occurring in the future.

Additionally, out of an abundance of caution, we are offering you access to 24 months of credit monitoring and identity protection services through Cyberscout, a TransUnion company at no cost to you. Please understand that due to privacy laws, Sadler Gibb cannot activate these services for you directly. Additional information regarding how to activate the complimentary credit monitoring service is available in the “*Steps You Can Take to Help Protect Your Information*” section below. We have also provided additional information and resources below regarding protecting yourself against fraud and identity theft should you feel it appropriate to do so.

We encourage you to remain vigilant against incidents of fraud and identity theft by reviewing your credit reports/account statements for suspicious activity and to detect errors. If you discover suspicious or unusual activity on your account(s), it is encouraged that you promptly contact your financial institution or credit/debit card company. Additionally, you can enroll to receive the complimentary credit monitoring service we are making available to you.

We understand you may have additional questions about this matter. Should you have questions or concerns regarding this matter or offered monitoring service, please contact our dedicated assistance line through Cyberscout at 1-855-522-4532, which is available Monday to Friday between the hours of 6 a.m. and 6 p.m. Mountain Time.

Sincerely,

Sadler Gibb & Assoc.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enrollment Instructions for Offered Monitoring Services

We are providing you with access to single bureau credit monitoring/single bureau credit report/single bureau credit score services at no charge. To enroll in the monitoring services, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted please provide the following code to enroll in the offered monitoring services: [REDACTED].

These services provide you with alerts for 24 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. Below please find descriptions of the offered services we are providing through Cyberscout.

- Credit Monitoring
 - Provide you with alerts for 24 months from the date of enrollment when changes occur to your credit file. The alert will be sent to you the same day that the change or update takes place with the bureau.
- Identity Theft Insurance
 - Enrolled individuals will have access to \$1,000,000 in insurance coverage to protect against potential damages related to identity theft and fraud.
 - Available worldwide and includes coverage for identity theft expenses as well as unauthorized electronic fund transfer fraud.
- Fraud Remediation Services
 - Access to team of dedicated specialists at Cyberscout to help you in the event you experience fraud and assist with remediation.

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.

Request an Identity Protection PIN

An Identity Protection PIN (IP PIN) is a six-digit number that prevents someone else from filing a tax return using your Social Security (SSN) number or Individual Taxpayer Identification Number (ITIN). The IP PIN is known only to you and the IRS. It 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. Additional information regarding an IP PIN, including information on how to request an IP PIN, can be found at <http://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.

If you want to request an IP PIN, please note:

- You must pass an identity verification process.
- Spouses and dependents are eligible for an IP PIN if they can pass the identity verification process.
- Once you have opted in and obtained an IP PIN online, you will need to retrieve your IP PIN online each calendar year as a CP01A Notice will not be mailed.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.



You 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-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you 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 your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

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

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

<p>TransUnion 1-800-680-7289 www.transunion.com</p>	<p>Experian 1-888-397-3742 www.experian.com</p>	<p>Equifax 1-888-298-0045 www.equifax.com</p>
<p>TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000</p>	<p>Experian Fraud Alert P.O. Box 9554 Allen, TX 75013</p>	<p>Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069</p>
<p>TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094</p>	<p>Experian Credit Freeze P.O. Box 9554 Allen, TX 75013</p>	<p>Equifax Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788</p>

Additional Information

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

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, Massachusetts Attorney General, and the FTC. This notice has not been delayed by law enforcement.

