



First State Bank of Middlebury
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
USBFS2804



[REDACTED]

[REDACTED]

[REDACTED]



January 28, 2026

[REDACTED]

Dear [REDACTED]:

First State Bank of Middlebury (“FSB”) writes to inform you of a cyber security event which may affect certain information related to you. We take the privacy and security of all information in our care very seriously, and this letter provides information about the matter, our response, and resources we are making available to you.

What Happened? We recently detected unusual activity within an FSB employee’s email account. In response, we quickly took steps to secure the account and engaged third-party specialists to investigate and determine the full nature and scope of the matter. The investigation determined that a single email mailbox was accessed on October 30, 2025 without authorization. We then conducted a thorough review of the contents of the email mailbox. This was a time-intensive effort, involving the correlation of identified information to involved individuals, and to confirm correct contact information for notifications. Such efforts were completed on January 20, 2026.

What Information Was Involved? Our review determined an email or attachment within the email mailbox contained your name [REDACTED].

What We Are Doing. In response to this event, we took steps to secure the relevant email account and conducted a comprehensive investigation, which was aided by third-party forensic specialists. As the obligation to safeguard the information in our care is of paramount importance to us, we have implemented additional security measures to further enhance our cybersecurity infrastructure, and revised and implemented additional policies and procedures regarding data, and providing additional training to our workforce with a goal of minimizing the risk of a future similar incident.

Additionally, out of an abundance of caution, we are offering you access to 12 months of credit monitoring and identity protection services through Cyberscout, a TransUnion company. Please understand that due to privacy laws, we cannot activate these services for you directly. Additional information regarding how to activate the complimentary monitoring service is in the “*Steps You Can Take to Help Protect Your Information*” section below.

What You Can Do. We recommend that you 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. If you discover any suspicious or unusual activity on your account(s), it is recommended that you promptly contact the financial institution or credit/debit card company. Additionally, you can enroll to receive the complimentary credit monitoring service we are making available to you. You can also review the enclosed "*Steps You Can Take to Help Protect Your Information*" for additional information and resources.

For More Information. We understand you may have additional questions about this matter. Should you have questions or concerns regarding this matter, please contact our dedicated assistance line at [REDACTED], which is available Monday to Friday between 9:00 a.m. and 4:30 p.m. Eastern Time.

Sincerely,

First State Bank of Middlebury

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Offered Monitoring Services

We are providing you with access to credit monitoring services at no charge. If you have not enrolled already, 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]

Below please find descriptions of the offered services we are providing through Cyberscout, a TransUnion company.

- Credit Monitoring
 - o Provide you with alerts for 12 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
 - o Enrolled individuals will have access to \$1,000,000 in insurance coverage to protect against potential damages related to identity theft and fraud.
 - o Available worldwide and includes coverage for identity theft expenses as well as unauthorized electronic fund transfer fraud.
- Fraud Remediation Services
 - o Access to team of dedicated specialists at Cyberscout, a TransUnion company, 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.

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:

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

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, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For New York residents, the New York Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.