

March 13, 2025

Via Email: Idtheft@oag.state.md.us

Attorney General Anthony G. Brown
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Preliminary Notice of Data Security Incident

Dear Office of the Attorney General:

Wilson Elser Moskowitz Edelman and Dicker, LLP (“Wilson Elser”) represents Cross Valley Federal Credit Union (“Cross Valley”), a healthcare company located at 640 Baltimore Drive Wilkes-Barre, PA 18702. Cross Valley takes the security and privacy of the information within its control very seriously and has taken steps to prevent a similar incident from occurring in the future. This letter will serve to inform you of the nature of the incident, what information may have been compromised, the number of Maryland residents being notified, and the steps that Cross Valley has taken in response to the incident.

1. Nature of the Incident

Cross Valley initially discovered a network intrusion on December 4, 2024, when several personnel found messages on their work machines. Cross Valley immediately initiated measures to contain the intrusion, secure its environment, and investigate the scope of the incident. Cross Valley has engaged Wilson Elser, LLP as its legal counsel along with a third-party cybersecurity firm to conduct a forensics investigation to determine the nature and scope of this incident. On February 10, 2025, Cross Valley completed a notification list and confirmed that information relating to Cross Valley FCU members had been impacted. Findings from the investigation indicated that the following data elements relating to Cross Valley members may have been subject to unauthorized access: names, addresses, and Social Security Numbers.

2. Number of Maryland Residents Affected

Based on investigation findings, Cross Valley identified and notified fifteen (15) Maryland residents whose information was impacted as a result of the incident. Notices were mailed to affected individuals on March 13, 2025. A sample notification letter is enclosed hereto as **Exhibit A**.

3. Steps taken in Response to the Incident

Cross Valley is committed to ensuring the security and privacy of all personal information in its control and is taking steps to prevent a similar incident from occurring in the future. When the incident was first discovered, Cross Valley immediately took steps to contain the intrusion and secure its environment. Since the discovery of the incident, Cross Valley acted quickly to isolate the intrusion and secure its network environment. Cross Valley also provided preliminary notice of the incident to regulators as required by law. Later, Cross Valley implemented a

number of security enhancements designed to prevent similar incidents from occurring in the future, including enhanced security training, additional protections on email links, and sandboxing potential email threats.

4. Contact information

Cross Valley remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Anjali.Das@WilsonElser.com or 312-821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

A handwritten signature in blue ink, appearing to read "Anjali C. Das". The signature is fluid and cursive, with the first name "Anjali" and last name "Das" clearly distinguishable.

Anjali C. Das

Cross Valley Federal Credit Union
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



Via First-Class Mail:



March 13, 2025

Re: Notice of Cybersecurity Incident

Dear [REDACTED],

Cross Valley Federal Credit Union ("Cross Valley") is writing to inform you of a recent data security incident that may have resulted in unauthorized access to your personal information. This letter provides you with information about the incident and the steps we are taking in response, as well as resources you can use to help you protect against the potential misuse of your information. While we do not have any evidence that anyone's personal information has been misused for identity theft or fraud in connection with this incident, we are offering free credit monitoring and identity theft protection services. This letter includes instructions for enrolling in those services.

What Happened?

On December 4, 2024, Cross Valley discovered a suspicious activity on its network and determined there had been unauthorized access. Upon discovery, Cross Valley immediately took steps to contain the intrusion and secure its environment. Cross Valley also engaged outside cybersecurity experts to conduct a comprehensive investigation into the nature and scope of the incident. Findings from the forensic investigation indicated that some data relating to Cross Valley Members may have been subject to unauthorized access. After a comprehensive review of the findings, Cross Valley identified a population of affected individuals and prepared to mail notices.

What Information Was Involved

Based on our investigation, the unauthorized actor may have accessed your [REDACTED]

What We Are Doing

Data privacy and security is among Cross Valley's highest priorities. Since the discovery of the incident, Cross Valley acted quickly to contain the intrusion and secure its network. Cross Valley also provided preliminary notice of the incident to regulators as required by law. Later, Cross Valley implemented a number of security enhancements designed to prevent similar incidents from occurring in the future. These enhancements include but are not limited to enhanced security training, additional verification clicks before emails links open, and sandboxing potential email threats.

In light of the incident, we are providing you with access to **Single Bureau Credit Monitoring, Credit report, and Credit Score** services at no charge. These services provide you with alerts for twelve 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 that specializes in fraud assistance and remediation services. Details on how to enroll in these complimentary services can be found below.

000010102G0500

P

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 credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and consider placing a fraud alert on your credit file. Please review the enclosed *Steps You Can Take to Help Protect Your Information* to learn more.

We also encourage you to enroll in the credit monitoring and identity theft protection services we are making available to you at no cost. To enroll in Credit Monitoring services at no charge, please log on to [REDACTED] 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. 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.

For More Information

If you have any questions or concerns not addressed in this letter, please call 1-833-799-3982 (toll free) Monday through Friday, during the hours of 8:00 a.m. and 8:00 p.m. Eastern Standard Time (excluding U.S. national holidays).

Sincerely,

A handwritten signature in cursive script, appearing to read "Traci Donahue".

Traci Donahue
Chief Executive Officer
Cross Valley Federal Credit Union

Steps You Can Take to Help Protect Your Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone or online. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years.

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742

TransUnion
P.O. Box 2000
Chester, PA 19016
1-800-680-7289

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-800-525-6285

www.experian.com/fraud/center.html www.transunion.com/fraud-alerts <https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>

Monitoring: You should always remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and by monitoring your credit report for suspicious or unusual activity.

Security Freeze: You have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742

TransUnion
P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-298-0045

www.experian.com/freeze/center.html www.transunion.com/credit-freeze <https://www.equifax.com/personal/credit-report-services/credit-freeze/>

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.



00001020280000

P

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), 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.

You can obtain further information on how to file such a complaint by way of the contact information listed above. Instances of known or suspected identity theft should also be reported to law enforcement.

For residents of Iowa: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Massachusetts: It is required by state law that you are informed of your right to obtain a police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For residents of New Mexico: State law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You 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 you to review your rights pursuant to the Fair Credit Reporting Act at 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.

For residents of Oregon: State law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Rhode Island: It is required by state law that you are informed of your right to file or obtain a police report in regard to this incident.

For residents of Arizona, Colorado, District of Columbia, Illinois, Maryland, New York, North Carolina, and Rhode Island: You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Federal Trade Commission - Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.identitytheft.gov

Arizona Office of the Attorney General Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

Colorado Office of the Attorney General Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 www.coag.gov

District of Columbia Office of the Attorney General - Office of Consumer Protection: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov

Illinois office of the Attorney General - 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; www.illinoisattorneygeneral.gov

Maryland Office of the Attorney General - Consumer Protection Division: 200 St. Paul Place, 16th floor, Baltimore, MD 21202; 1-888-743-0023; www.oag.state.md.us

New York Office of Attorney General - Consumer Frauds & Protection: The Capitol, Albany, NY 12224; 1-800-771-7755; <https://ag.ny.gov/consumer-frauds/identity-theft>

North Carolina Office of the Attorney General - Consumer Protection Division: 9001 Mail Service Center, Raleigh, NC 27699; 1-877-566-7226; www.ncdoj.com

Rhode Island Office of the Attorney General - Consumer Protection: 150 South Main St., Providence RI 02903; 1-401-274-4400; www.riag.ri.gov