Innovate Collaborate Inspire

P.O. Box 989728
West Sacramento, CA 95798-9728

Person's Mailing Address

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:

DATE

NOTICE OF SECURITY INCIDENT

Dear _____:

Marysville Exempted Village School District ("MEVSD") writes to inform you of a recent cybersecurity event that may affect the privacy of some of your personal 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 resources available to help you protect your information, should you feel it appropriate to do so.

What Happened? MEVSD recently became aware of suspicious activity within our network. Upon learning of the suspicious activity, we immediately took steps to secure our systems and launched an investigation into the nature and scope of the activity with the assistance of third-party cybersecurity and data privacy specialists. The investigation determined that an unauthorized actor accessed our network at various times between October 5, 2024 and October 26, 2024, and that certain information contained within those systems was copied and may have been viewed by the unauthorized actor during that time. Upon becoming aware of these findings, we undertook a comprehensive and time-intensive review of the data at risk to determine what information was potentially affected, and to whom that information related. Those efforts were recently completed, and MEVSD is notifying you because the investigation determined that certain information relating to you was contained within the impacted files.

What Information Was Involved? The following types of information related to you were found in the impacted files: your _____ At this time, MEVSD is not aware of your information being used to commit identity theft or fraud in relation to this event.

What We Are Doing. We take this event seriously, and the confidentiality, privacy, and security of information in our care are among our highest priorities. Upon learning of this event, we moved quickly to investigate and respond, assess the security of our network, and notify affected individuals. Additionally, we notified state and federal law enforcement of the event and are cooperating with their investigations. As part of our ongoing commitment to information security, we are reviewing existing security policies and dedicating significant resources to implement additional cybersecurity measures to further protect against similar events moving forward. We are also notifying 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 twelve (12) months at no cost to you, through IDX. You can find information on how to enroll in these services in the enclosed *STEPS YOU CAN TAKE TO HELP PROTECT YOUR 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 and monitoring your free credit reports for suspicious activity and to detect errors. As a best practice,

you should frequently change your passwords for all online accounts. You can review the enclosed *STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION* to learn helpful tips on steps you can take to protect against possible information misuse, should you feel it appropriate to do so. You may also enroll in the complimentary credit monitoring services we are offering to you.

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 1 (855) 202-5928 from 9:00 a.m. ET to 9:00 p.m. ET, Monday through Friday, excluding major U.S. holidays.

Sincerely,

Marysville Exempted Village School District

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Monitoring Services

Website and Enrollment. Scan the QR image or go to_____and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

Telephone. Contact IDX at _____ to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

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 http://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 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 their 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 reported to law enforcement, the relevant state Attorney General, and the Federal Trade Commission. This notice has not been delayed by law enforcement.