EXHIBIT 1

The investigation into this event is ongoing, and this notice will be supplemented with any significant new facts learned subsequent to its submission. By providing this notice, Prosser 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 July 3, 2024, Prosser identified suspicious activity on its computer network and observed malware encryption impacting certain systems. Prosser took quick steps to ensure the continued security of its network, restore systems safely, and investigate to understand what occurred. The investigation determined that an unknown actor accessed Prosser systems between June 29, 2024 and July 3, 2024 and copied certain files from the network.

As part of the investigation, Prosser launched a thorough and comprehensive review of the accessible data to determine whether it contained any sensitive information and to whom that information belonged. This preliminary review concluded on February 10, 2025 and determined that protected information related to individuals was included in the accessible data. Prosser then moved quickly to identify address information for the identified population. The address search and confirmation of those individuals due notice based on impacted data elements occurred on February 21, 2025.

The information that could have been subject to unauthorized access includes name, Social Security number, date of birth, student identification number, and medical/health information.

Notice to Washington Residents

On or about March 21, 2025, Prosser provided written notice of this event to nine hundred sixty-three (963) 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 discovering the event, Prosser moved quickly to investigate and respond to the event, assess the security of Prosser systems, and identify potentially affected individuals. Further, Prosser notified federal law enforcement regarding the event. Prosser is also working to implement additional safeguards and training to its employees. Prosser is providing access to credit monitoring services for twelve (12) months, through Experian, to individuals whose Social Security information was potentially affected by this event, at no cost to the individual.

Additionally, Prosser is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Prosser is also providing individuals with information on how to place fraud alerts and credit freezes on their credit files, 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. Prosser is providing written notice of this event to relevant state regulators, as necessary.

EXHIBIT A

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

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

March 21, 2025

Dear <<First Name>> <<Last Name>>:

Prosser School District ("Prosser") is writing to inform you of an event that may impact some of your information. Prosser takes this event seriously, and the privacy, security, and confidentiality of information in our care is among our highest priorities. Although Prosser is not aware of any actual or attempted identity theft as a result of this event, 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 July 3, 2024, Prosser identified suspicious activity on our computer network and observed malware encryption impacting certain systems. We took quick steps to ensure the continued security of the network, restore systems safely, and investigate to understand what occurred. The investigation determined that an unknown actor accessed Prosser systems between June 29, 2024 and July 3, 2024 and copied certain files from the network. As part of the investigation, Prosser launched a thorough and comprehensive review of the accessible data to determine whether it contained any sensitive information and to whom that information belonged. On February 21, 2025, we completed efforts to locate address information for identified individuals to provide notice directly to them.

What Information Was Involved.

The data review determined that some of your information was present within the accessible data. Based on the review, we located your name and the following information in the data: <<Variable Data 3>>. Please note, Prosser is not aware of any actual or attempted identity theft as a result of this event.

What We Are Doing.

Prosser takes this event and the security of information in our care very seriously. Upon learning of the event, we responded quickly, confirmed the security of our network, restored our systems, and investigated to understand what occurred. Prosser also reported this event to law enforcement and are notifying relevant regulators, as required. As part of our ongoing commitment to information security, we reviewed our policies, procedures, and security tools to reduce the risk of a similar event occurring in the future.

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 and suspicious activity. You may also review the information contained in the attached *Steps You Can Take to Help Protect Your Information.*

For More Information.

Prosser understands that you may have questions about this event that are not addressed in the letter. If you have additional questions, please contact our dedicated assistance line at 1-800-939-4170. IDX representatives are available Monday through Friday from 6:00 a.m. – 6:00 p.m. Pacific Time. You may also write to Prosser at 1203 Prosser Avenue, Prosser, WA 99350.

Sincerely,

Prosser School District

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

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 one-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 fraud alert or a credit freeze, 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

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.

EXHIBIT 1

The investigation into this event is ongoing, and this notice will be supplemented with any significant new facts learned subsequent to its submission. By providing this notice, Prosser 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 July 3, 2024, Prosser identified suspicious activity on its computer network and observed malware encryption impacting certain systems. Prosser took quick steps to ensure the continued security of its network, restore systems safely, and investigate to understand what occurred. The investigation determined that an unknown actor accessed Prosser systems between June 29, 2024 and July 3, 2024 and copied certain files from the network.

As part of the investigation, Prosser launched a thorough and comprehensive review of the accessible data to determine whether it contained any sensitive information and to whom that information belonged. This preliminary review concluded on February 10, 2025 and determined that protected information related to individuals was included in the accessible data. Prosser then moved quickly to identify address information for the identified population. The address search and confirmation of those individuals due notice based on impacted data elements occurred on February 21, 2025.

The information that could have been subject to unauthorized access includes name, Social Security number, date of birth, student identification number, and medical/health information.

Notice to Washington Residents

On or about March 21, 2025, Prosser provided written notice of this event to nine hundred sixty-three (963) 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 discovering the event, Prosser moved quickly to investigate and respond to the event, assess the security of Prosser systems, and identify potentially affected individuals. Further, Prosser notified federal law enforcement regarding the event. Prosser is also working to implement additional safeguards and training to its employees. Prosser is providing access to credit monitoring services for twelve (12) months, through Experian, to individuals whose Social Security information was potentially affected by this event, at no cost to the individual.

Additionally, Prosser is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Prosser is also providing individuals with information on how to place fraud alerts and credit freezes on their credit files, 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. Prosser is providing written notice of this event to relevant state regulators, as necessary.

EXHIBIT A

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

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

March 21, 2025

Dear <<First Name>> <<Last Name>>:

Prosser School District ("Prosser") is writing to inform you of an event that may impact some of your information. Prosser takes this event seriously, and the privacy, security, and confidentiality of information in our care is among our highest priorities. Although Prosser is not aware of any actual or attempted identity theft as a result of this event, 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 July 3, 2024, Prosser identified suspicious activity on our computer network and observed malware encryption impacting certain systems. We took quick steps to ensure the continued security of the network, restore systems safely, and investigate to understand what occurred. The investigation determined that an unknown actor accessed Prosser systems between June 29, 2024 and July 3, 2024 and copied certain files from the network. As part of the investigation, Prosser launched a thorough and comprehensive review of the accessible data to determine whether it contained any sensitive information and to whom that information belonged. On February 21, 2025, we completed efforts to locate address information for identified individuals to provide notice directly to them.

What Information Was Involved.

The data review determined that some of your information was present within the accessible data. Based on the review, we located your name and the following information in the data: <<Variable Data 3>>. Please note, Prosser is not aware of any actual or attempted identity theft as a result of this event.

What We Are Doing.

Prosser takes this event and the security of information in our care very seriously. Upon learning of the event, we responded quickly, confirmed the security of our network, restored our systems, and investigated to understand what occurred. Prosser also reported this event to law enforcement and are notifying relevant regulators, as required. As part of our ongoing commitment to information security, we reviewed our policies, procedures, and security tools to reduce the risk of a similar event occurring in the future.

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 and suspicious activity. You may also review the information contained in the attached *Steps You Can Take to Help Protect Your Information.*

For More Information.

Prosser understands that you may have questions about this event that are not addressed in the letter. If you have additional questions, please contact our dedicated assistance line at 1-800-939-4170. IDX representatives are available Monday through Friday from 6:00 a.m. – 6:00 p.m. Pacific Time. You may also write to Prosser at 1203 Prosser Avenue, Prosser, WA 99350.

Sincerely,

Prosser School District

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

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 one-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 fraud alert or a credit freeze, 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

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.