EXHIBIT 2

We are writing to supplement our May 15, 2023 and October 6, 2023 notifications to your office regarding an incident that may affect the privacy of certain personal information relating to an additional two (2) Maine residents. Our October 6, 2023 notification to your office is attached as **Exhibit AAA**. This notice will be supplemented with new significant facts learned subsequent to its submission. By providing this notice, Edmonds School District ("Edmonds") does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

On January 31, 2023, Edmonds identified suspicious activity in its environment and immediately launched an investigation to determine the nature and scope of the activity. The investigation, which was conducted with the assistance of third-party forensic specialists, determined that an unauthorized actor had the ability to view and acquire certain information stored on the network between January 16, 2023, and January 31, 2023. Therefore, Edmonds undertook a comprehensive review of the data at risk to assess if any sensitive information could be affected and to whom it relates. On September 5, 2023, Edmonds completed this review and began efforts to notify individuals directly. Edmonds provided individual notice to all individuals for whom it had sufficient address information on October 6, 2023. However, Edmonds' review did not identify the postal address for all affected individuals. As such, Edmonds sought the assistance of a third party to locate a mailing address for additional individuals and on December 19, 2023, Edmonds located additional addresses. The information that could have been subject to unauthorized access may include: name and Social Security number.

Notice to Maine Residents

On May 15, 2023, and October 6, 2023, Edmonds provided direct notice of this incident to eight (8) Maine residents. On January 5, 2023, Edmonds provided notice to an additional two (2) Maine residents. Written notice is being provided in substantially the same form as the letter attached here as **Exhibit BBB**.

Previously on February 10, 2023, Edmonds provided substitute notice of this incident by posting a notice of the event on the homepage of its website and publishing a media notice throughout the state of Washington while its investigation and data review were ongoing.

Other Steps Taken and To Be Taken

Upon discovering the event, Edmonds moved quickly to investigate, respond to the incident, assess the security of its systems, and identify potentially affected individuals. Further, Edmonds notified federal law enforcement regarding the event. Edmonds is providing individuals whose personal information was potentially impacted by this event access to credit monitoring services for one (1) year through IDX at no cost to the individuals.

Edmonds is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Moreover, Edmonds is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, 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. Edmonds also intends to provide written notice of this incident to state and federal regulators, as necessary.

EXHIBIT AAA

Maine Security Breach Reporting Form - Review

EDIT

Type of Organization (Please select one)	Education
Entity Name	Edmonds School District
Street Address	20420 68th Ave. W.
City	Lynnwood
State, or Country if outside the US	WA
Zip Code	98036
Name	Chris Bailey
Title	Director of IT
Telephone Number	425-431-7101
Email Address	baileym@edmonds.wednet.edu
Relationship to entity whose information was compromised	baileym@edmonds.wednet.edu
Total number of persons affected (including Maine residents)	91,325
Total number of Maine residents affected	7
Date(s) Breach Occurred	01/16/2023 - 01/31/2023
Date Breach Discovered	09/05/2023
Description of the Breach (please check all that apply)	External system breach (hacking)
Information Acquired - Name or other personal identifier in combination with (please check all that apply)	Social Security Number Financial Account Number or Credit/Debit Card Number (in combination with security code, access code, password or PIN for the account)
Type of notification	Written
Date(s) of consumer notification	5/15/2023, 10/6/2023
List dates of any previous (within 12 months) breach notifications	5/15/2023
Were identity theft protection services offered?	Yes
If yes, please provide the duration, the provider of the service and a brief description of the service	12 Months of credit monitoring and identity protection services through IDX.

Disclosure and Agreement

By checking the box below, you certify that all information supplied on this form is true and accurate to the best of your knowledge.

☐ The disclosure statement has been read and agreed to by the individual submitting this Maine Attorney General Reporting Form. *

PREVIOUS CONTINUE TO SUBMIT FORM

Maine Security Breach Reporting Form

Thank you for submitting the breach details through this reporting form. The information you have provided has been submitted to the agency.

Please close this browser window.

PREVIOUS FINISH

EXHIBIT 1

(From October 06, 2023)

We are writing to supplement the May 15, 2023, notification to your office regarding an incident that may affect the privacy of certain personal information relating to an additional seven (7) Maine residents. The previous notification to your office is attached as **Exhibit AA**. This notice will be supplemented with new significant facts learned subsequent to its submission. By providing this notice, Edmonds does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

On January 31, 2023, Edmonds identified suspicious activity in its environment and immediately launched an investigation to determine the nature and scope of the activity. The investigation, which was conducted with the assistance of third-party forensic specialists, determined that an unauthorized actor had the ability to view and acquire certain information stored on our network between January 16, 2023, and January 31, 2023. Therefore, Edmonds undertook a comprehensive review of the data at risk to assess if any sensitive information could be affected and to whom it relates. On September 5, 2023, Edmonds completed this review and began efforts to notify individuals directly. The information that could have been subject to unauthorized access may include: name and Social Security number.

Notice to Maine Residents

On October 6, 2023, Edmonds provided notice of this incident to an additional seven (7) Maine residents. Written notice is being provided in substantially the same form as the letter attached here as **Exhibit BB**. Edmonds continues to review its internal records to attempt to locate postal addresses for additional potentially affected individuals and may supplement this notice if additional residents of Maine are determined to be impacted.

Previously on February 10, 2023, Edmonds provided substitute notice of this incident by posting a notice of the event on the homepage of its website and publishing a media notice throughout the state of Washington.

Other Steps Taken and To Be Taken

Upon discovering the event, Edmonds moved quickly to investigate, respond to the incident, assess the security of its systems, and identify potentially affected individuals. Further, Edmonds notified federal law enforcement regarding the event. Edmonds is providing individuals whose personal information was potentially impacted by this event access to credit monitoring services for 1 year through IDX at no cost to the individuals.

Edmonds is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Moreover, Edmonds is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, 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. Edmonds is also providing written notice of this incident to state and federal regulators, as necessary.

EXHIBIT AA

OFFICE OF THE
Maine Attorney General

Maine Security Breach Reporting Form - Review

EDIT

Type of Organization (Please select one)	Education
Entity Name	Edmonds School District
Street Address	20420 68th Ave. W.
City	Lynnwood
State, or Country if outside the US	WA
Zip Code	98036
Name	Chris Bailey
Title	Director of IT
Firm name (if different than entity name)	Mullen Coughlin LLC
Telephone Number	425-431-7101
Email Address	baileym@edmonds.wednet.edu
Relationship to entity whose information was compromised	Director of IT
Total number of persons affected (including Maine residents)	833
Total number of Maine residents affected	1
Date(s) Breach Occurred	01/16/2023 -01/31/2023
Date Breach Discovered	04/26/2023
Description of the Breach (please check all that apply)	External system breach (hacking)
Information Acquired - Name or other personal identifier in combination with (please check all that apply)	Financial Account Number or Credit/Debit Card Number (in combination with security code, access code, password or PIN for the account)
Type of notification	Written
Date(s) of consumer notification	05/15/2023
List dates of any previous (within 12 months) breach notifications	02/10/2023

Were identity theft protection services offered?	Yes
If yes, please provide the duration, the provider of the service and a brief description of the service	12 Months of credit monitoring and identity protection services through IDX.

Disclosure and Agreement

By checking the box below, you certify that all information supplied on this form is true and accurate to the best of your knowledge.

The disclosure statement has been read and agreed to by the individual submitting this Maine Attorney General Reporting Form. *

Chris Bailey

PREVIOUS CONTINUE TO SUBMIT FORM

OFFICE OF THE
Maine Attorney General

Maine Security Breach Reporting Form

Thank you for submitting the breach details through this reporting form. The information you have provided has been submitted to the agency.

Please close this browser window.

PREVIOUS FINISH

EXHIBIT 1

(From May 15, 2023)

The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Edmonds School District ("Edmonds") does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about January 31, 2023, Edmonds identified suspicious activity in its environment and immediately launched an investigation to determine the nature and scope of the activity. The investigation, which was conducted with the assistance of third-party forensic specialists, determined that an unauthorized actor had the ability to view and acquire certain information stored on the network between January 16, 2023, and January 31, 2023. Therefore, Edmonds is undertaking a comprehensive review of the data at risk to assess if any sensitive information could be affected and to whom it relates. This review is still ongoing, but on April 26, 2023, Edmonds identified that the information of certain current and former employees could have been subject to unauthorized access. The information that could have been subject to unauthorized access includes name, address, financial account information, and employee identification number.

Notice to Maine Resident

On May 15, 2023, Edmonds began providing written notice of this incident to one (1) Maine resident. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***. Previously on February 10, 2023, Edmonds provided substitute notice of this incident by posting a notice of the event on the homepage of its website and by publishing a media notice throughout the state of Washington. A copy of the website notice is attached here as ***Exhibit B*** and the media notice is attached here as ***Exhibit C***.

Other Steps Taken and To Be Taken

Upon discovering the event, Edmonds moved quickly to investigate and respond to the incident, assess the security of its systems, and identify potentially affected individuals. Edmonds is providing individuals whose personal information was potentially affected by this incident access to credit monitoring services for twelve (12) months through IDX at no cost to the individuals.

Additionally, Edmonds is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Edmonds is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, 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. Edmonds is also providing written notice of this incident to state and federal regulators, as necessary.

EXHIBIT A

Edmonds School District
Return Mail to IDX
4145 SW Watson Ave, Suite 400
Beaverton, OR 97005

To Enroll, Please Call:
1-800-939-4170
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: <<XXXXXXXX>>

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

May 15, 2023

NOTICE OF DATA PRIVACY EVENT

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

Edmonds School District ("Edmonds") writes to notify you of an incident that may affect the privacy of some of your information. This letter provides details of the incident, our response, and steps you may take to better protect against the possible misuse of your information should you feel it is appropriate to do so.

What Happened? On January 31, 2023, Edmonds identified suspicious activity in its environment and immediately launched an investigation to determine the nature and scope of the activity. The investigation, which was conducted with the assistance of third-party forensic specialists, determined that an unauthorized actor had the ability to view and acquire certain information stored on our network between January 16, 2023, and January 31, 2023. Therefore, Edmonds is undertaking a comprehensive review of the data at risk to assess if any sensitive information could be affected and to whom it relates. While this review is still ongoing, Edmonds has determined that some of your data may be at risk and wanted to inform you as soon as possible. If additional information not listed in this letter is determined to be affected, you will receive a supplemental correspondence to confirm the same.

What Information Was Involved? We determined the type of information potentially impacted by this incident may include your: name, address, financial account information, and employee identification number.

What We Are Doing. We take the confidentiality, privacy, and security of information in our care seriously. Upon discovery of the incident, we immediately commenced an investigation and took steps to implement additional safeguards related to data privacy and security.

In an abundance of caution, we are providing you with access to twelve (12) months of credit monitoring and identity protection services through IDX at no cost to you. A description of the services and instructions on how to enroll can be found within the enclosed *Steps You Can Take to Protect Personal Information*. Please note that you must complete the enrollment process yourself as we are not permitted to enroll you in these services.

What You Can Do. You can review the enclosed *Steps You Can Take to Protect Personal Information* for general guidance. In addition, you can enroll in the complimentary credit monitoring and identity protection services being offered through IDX. We also encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity.

For More Information. We understand you may have questions about the incident that are not addressed in this letter. If you have questions, or need assistance, please call 1-800-939-4170, Monday through Friday from 6:00 a.m. to 6:00 p.m. Pacific Time. You may also write to Edmonds at 20420 68th Ave. W, Lynnwood, WA 98036.

Sincerely,

Dr. Rebecca Miner
Superintendent
Edmonds School District

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring and Identity Protection

1. Website and Enrollment. Go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll is August 15, 2023.

2. 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.

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 your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your 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 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 you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one 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 your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report 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 security freeze, you will need to provide 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 you are a victim of identity theft.

Should you wish to place 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/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
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

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 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. You can obtain further information on how to file such a complaint by way of the contact information listed above. 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 and your state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and marylandattorneygeneral.gov

For New Mexico residents, 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 bureaus 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 violator. 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 by visiting 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 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/.

For *North Carolina* residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC, 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

EXHIBIT B

Notice of Data Event (https://www.edmonds.wednet.edu/news/details/~board/district-2022-23-only-district/post/notice-of-data-event)

Feb 10 2023 2:00 PM

Edmonds School District ("Edmonds") recently discovered an incident that may have impacted the privacy of information related to certain students, staff and parents. While Edmonds is unaware of any actual or attempted misuse of information in relation to the incident, it is providing potentially affected individuals with information about the incident and steps individuals may take to help protect against the possible misuse of your information.

What Happened? On January 31, 2023, Edmonds identified suspicious activity in its environment and immediately launched an investigation to determine the nature and scope of the activity. The investigation, which is still ongoing and being conducted with the assistance of third-party forensic specialists, determined that an unauthorized actor had the ability to view and acquire certain information stored on the network between January 16, 2023, and January 31, 2023. Therefore, Edmonds is undertaking a comprehensive review of the data at risk to assess if any sensitive information could be affected and to whom it relates. While this review is still ongoing, Edmonds wanted to inform potentially affected individuals as soon as possible so that they could take affirmative steps to protect their information should they deem it appropriate to do so.

What Information Was Involved? Edmonds determined the type of information potentially impacted by this incident may include, but is not limited to, name, Social Security number, driver's license number, date of birth, student identification number, financial account information, medical information, and student records.

How Will Individuals Know If They Are Affected By This Incident? Edmonds is in the process of reviewing the data determined to be at risk and generating a list of potentially impacted individuals. Once this review is complete, Edmonds plans to mail notification letters to individuals whose protected information could have been impacted and for whom they have a valid mailing address.

What You Can Do. Edmonds encourages individuals to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your credit reports for any unauthorized or suspicious activity. You can also review the "Steps Individuals Can Take to Help Protect Personal Information" below for further guidance.

For More Information. Edmonds understands individuals may have questions about the incident that are not addressed in this notice. If you have questions, or need assistance, please call 425-431-7000, Monday through Friday from 8:00 a.m. to 4:30 p.m. Pacific Time. If you call outside the hours listed, please leave a message and someone will return your call as soon as possible. You may also write to Edmonds at 20420 68th Ave. W, Lynnwood, WA 98036.

STEPS INDIVIDUALS CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Skip To Main Content

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 your free credit report, visit www.annualcreditreport.com (http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. You may also directly contact the three (3) major credit reporting bureaus listed below to request a free copy of your 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 you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven (7) years. Should you wish to place a fraud alert, please contact any one 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 your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report 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 security freeze, you will need to provide 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, military identification, etc.); 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 (3) major credit reporting bureaus listed below:

Equifax
https://www.equifax.com/personal/credit-report-services/ (https://www.equifax.com/personal/credit-report-services/)
1-888-298-0045
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788

Skip To Main Content

Experian
https://www.experian.com/help/ (https://www.experian.com/help/)
1-888-397-3742
Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013
Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013
TransUnion
https://www.transunion.com/credit-help (https://www.transunion.com/credit-help)
1-800-916-8800
TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov (http://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. You can obtain further information on how to file such a complaint by way of the contact information listed above. 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 and your state Attorney General. This notice has not been delayed by law enforcement.

EXHIBIT C

EDMONDS SCHOOL DISTRICT PROVIDES NOTICE OF DATA EVENT – LYNNWOOD, WA.

Edmonds School District ("Edmonds") recently discovered an incident that may have impacted the privacy of information related to certain students, staff, and parents. While Edmonds is unaware of any actual or attempted misuse of information in relation to the incident, it is providing potentially affected individuals with information about the incident and steps individuals may take to help protect their information should they feel it is appropriate to do so.

On January 31, 2023, Edmonds became aware of suspicious activity related to certain Edmonds computer systems. Edmonds immediately launched an investigation, with the assistance of third-party forensic specialists, to determine the nature and scope of the activity. Through the investigation, it was determined that there was unauthorized access to Edmonds's network between January 16, 2023, and January 31, 2023, and the unauthorized actor had the ability to acquire certain information stored on the network during the period of access. Therefore, Edmonds is undertaking a comprehensive review of the data at risk to assess if any sensitive information could be affected and to whom it relates. While this review is still ongoing, Edmonds wanted to inform potentially affected individuals as soon as possible so that they could take affirmative steps to protect their information should they deem it appropriate to do so. Edmonds determined the type of information potentially impacted by this incident may include, but is not limited to, name, Social Security number, driver's license number, date of birth, student identification number, financial account information, medical information, and student records.

Once Edmonds's review is complete, it intends to mail notice letters to individuals whose protected information could have been affected and for whom it has valid mailing addresses. Interested individuals can find additional information about the event at Edmonds.wednet.edu. They may also write to Edmonds at 20420 68th Ave W, Lynnwood, WA 98036.

Edmonds takes the security of information in its care very seriously. Upon learning of this issue, Edmonds immediately took steps to secure its network by disabling internet access, deploying additional protections across its network, and conducting a diligent investigation to confirm the nature and scope of the incident. Edmonds is also working with third-party specialists to strengthen the security of its systems.

February 10, 2023

Media contact: Colin Scanlon – (267) 930-4259

EXHIBIT BB

Edmonds School District

PO Box 480149
Niles, IL 60714

<<First Name>> <<Last Name>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://response.idx.us/Edmonds-SD

October 6, 2023

NOTICE OF DATA <<Variable Data 2>>

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

Edmonds School District ("Edmonds") writes to notify you of an incident that may affect the privacy of some of your information. This letter provides details of the incident, our response, and steps you may take to better protect against the possible misuse of your information should you feel it is appropriate to do so.

What Happened? On January 31, 2023, Edmonds identified suspicious activity in its environment and immediately launched an investigation to determine the nature and scope of the activity. The investigation, which was conducted with the assistance of third-party forensic specialists, determined that an unauthorized actor had the ability to view and acquire certain information stored on our network between January 16, 2023, and January 31, 2023. Therefore, Edmonds undertook a comprehensive review of the data at risk to assess if any sensitive information could be affected and to whom it relates. On September 5, 2023, Edmonds completed this review and determined that some of your data may be at risk.

What Information Was Involved? We determined the type of information potentially impacted by this incident may include your <<Variable Data 1>>.

What We Are Doing. We take the confidentiality, privacy, and security of information in our care seriously. Upon discovery of the incident, we immediately commenced an investigation and took steps to implement additional safeguards related to data privacy and security.

In an abundance of caution, we are providing you with access to <<12 / 24>> months of credit monitoring and identity protection services through IDX at no cost to you. A description of the services and instructions on how to enroll can be found within the enclosed *Steps You Can Take to Protect Personal Information*. Please note that you must complete the enrollment process yourself as we are not permitted to enroll you in these services.

What You Can Do. You can review the enclosed *Steps You Can Take to Protect Personal Information* for general guidance. In addition, you can enroll in the complimentary credit monitoring and identity protection services being offered through IDX. We also encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity.

For More Information. We understand you may have questions about the incident that are not addressed in this letter. If you have questions, or need assistance, please call 1-888-861-6984, Monday through Friday from 6:00 a.m. to 6:00 p.m. Pacific Time. You may also write to Edmonds at 20420 68th Ave, W. Lynnwood, WA 98036.

Sincerely,

Dr. Rebecca Miner
Superintendent
Edmonds School District

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring

Scan the QR image or go to https://response.idx.us/Edmonds-SD and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll in services is January 6, 2024.

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 your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your 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 you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one 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 your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report 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., 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 you are a victim of identity theft.

Should you 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/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
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

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 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.

You can obtain further information on how to file such a complaint by way of the contact information listed above. 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 and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 1-202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

For Massachusetts residents, Under Massachusetts law, you have the right to obtain any 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 New Mexico residents, 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 bureaus 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 violator. 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 by visiting 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 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/.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are <<#>> Rhode Island residents impacted by this event.

EXHIBIT BBB

Edmonds School District
PO Box 480149
Niles, IL 60714

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://response.idx.us/Edmonds-SD

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

January 5, 2024

NOTICE OF DATA <<Variable Data 2>>

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

Edmonds School District ("Edmonds") writes to notify you of an incident that may affect the privacy of some of your information. This letter provides details of the incident, our response, and steps you may take to better protect against the possible misuse of your information should you feel it is appropriate to do so. Please note that in our review of the notice population, we discovered some instances of individuals with the same name and address but did not have other identifiers to confirm they were the same individuals. In an abundance of caution, we are providing notice to all of these individuals, but it may result in some individuals receiving multiple letters.

What Happened? On January 31, 2023, Edmonds identified suspicious activity in its environment and immediately launched an investigation to determine the nature and scope of the activity. The investigation, which was conducted with the assistance of third-party forensic specialists, determined that an unauthorized actor had the ability to view and acquire certain information stored on our network between January 16, 2023, and January 31, 2023. Therefore, Edmonds undertook a comprehensive review of the data at risk to assess if any sensitive information could be affected and to whom it relates. This review was completed on September 5, 2023, and Edmonds provided individual notice to all individuals which it had sufficient address information on October 6, 2023. Edmonds then began a multi-pronged approach to attempt to identify address information for the remaining potentially affected individuals. On December 19, 2023, we located an address for you.

What Information Was Involved? We determined the type of information potentially impacted by this incident includes your: <<Variable Data 1>>.

What We Are Doing. We take the confidentiality, privacy, and security of information in our care seriously. Upon discovery of the incident, we immediately commenced an investigation and took steps to implement additional safeguards related to data privacy and security.

In an abundance of caution, we are providing you with access to <<12 / 24>> months of credit monitoring and identity protection services through IDX at no cost to you. A description of the services and instructions on how to enroll can be found within the enclosed *Steps You Can Take to Protect Personal Information*. Please note that you must complete the enrollment process yourself as we are not permitted to enroll you in these services.

What You Can Do. You can review the enclosed *Steps You Can Take to Protect Personal Information* for general guidance. In addition, you can enroll in the complimentary credit monitoring and identity protection services being offered through

IDX. We also encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity.

For More Information. We understand you may have questions about the incident that are not addressed in this letter. If you have questions, or need assistance, please call 1-888-861-6984, Monday through Friday from 6:00 a.m. to 6:00 p.m. Pacific Time. You may also write to Edmonds at 20420 68th Ave, W. Lynnwood, WA 98036 or visit https://www.edmonds.wednet.edu/idx.

Sincerely,

Dr. Rebecca Miner
Superintendent
Edmonds School District

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring

Scan the QR image or go to https://response.idx.us/Edmonds-SD and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll in services is April 5, 2024.

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 your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your 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 you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one 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 your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report 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., 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 you are a victim of identity theft.

Should you 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/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
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

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 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.

You can obtain further information on how to file such a complaint by way of the contact information listed above. 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 and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 1-202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

For Massachusetts residents, Under Massachusetts law, you have the right to obtain any 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 New Mexico residents, 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 bureaus 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 violator. 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 by visiting 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 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/.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are <<#>> Rhode Island residents impacted by this event.