EXHIBIT 1

Nature of the Data Event

On September 7, 2024, Highline identified evidence of unauthorized activity in its network. Highline immediately took steps to secure its systems and an investigation was initiated into the nature and scope of the event with the assistance of third-party computer forensic specialists. The investigation determined that an unknown actor gained access to certain systems on Highline's network and took certain files from these systems. Following the forensic investigation, Highline undertook a time and labor-intensive review of the involved files to determine whether personal information was involved and, if so, to whom it belonged. This review recently completed.

The types of information involved varies by individual, but may include name, date of birth, Social Security number, driver's license number, financial account information, passport number, digital signature, medical information, and/or health insurance information.

Notice to Washington state Residents

On or about April 2, 2025, Highline will provide notice of the event to Washington state residents via notice to statewide media and a posting on its website. The notices shall be provided in substantially the same form as those attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, Highline moved quickly to investigate and respond to the incident, assess the security of Highline systems, and identify potentially affected individuals. Further, Highline notified federal law enforcement regarding the event. Highline also used this incident as an opportunity to build upon our pre-existing cybersecurity practices and implement additional safeguards and training to its employees. Highline is providing access to credit monitoring services for twelve (12) months, through IDX, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Highline is providing the individuals potentially involved 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. Highline 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.

EXHIBIT A

For Immediate Release

April 2, 2025
Contact: Tove Tupper
tove.tupper@highlineschools.org
(O) 206-631-3002

Highline Public Schools Provides Notice of Data Event

Burien, Wash. – Highline Public Schools is notifying the community of an incident involving personal information on its systems. This notice includes details about the incident, their response, and resources available to help protect personal information if individuals choose to do so.

On September 7, 2024, Highline identified unauthorized activity within its network. Actions were promptly taken to secure their systems, and an investigation was conducted with the support of third-party computer forensic specialists. The investigation determined that an unknown actor gained access to certain systems on their network and accessed certain files. After the forensic investigation, Highline performed a detailed review of the affected files to determine if personal information was involved and to identify the individuals associated with this information. This review has recently been completed.

The types of information impacted vary by individual and include name, address, date of birth, Social Security number, driver's license number, financial account information, passport number, digital signature, medical information, and health insurance information.

Confidentiality, privacy and security of personal information are among Highline's highest priorities. Upon becoming aware of this incident, the district immediately took steps to secure their systems and initiated a full investigation. Additional security measures are being implemented to further protect against similar incidents moving forward. This incident was also reported to federal law enforcement.

Additionally, Highline is offering credit monitoring and identity protection services for 12 months through IDX at no cost to individuals in the Highline community. Individuals will not be automatically enrolled in these services. Instructions on how to enroll in these services can be found below in the section titled *Steps You Can Take to Help Protect Personal Information*.

As a precautionary measure, individuals are encouraged to remain vigilant against incidents of identity theft by reviewing their account statements, credit reports, and explanations of benefits for unusual activity and to detect errors. Any suspicious activity should promptly be reported to the appropriate insurance company, health care provider, or financial institution. Interested individuals can also review the information below for further guidance.

If you have any questions or feel you or your student's data may have been impacted, please call our dedicated assistance line at 1-877-758-1726, Monday through Friday, from 6:00 am PT – 6 pm PT (excluding U.S. holidays). You may also write to Highline at 15675 Ambaum Blvd. SW, Burien, WA 98166.

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

We encourage those who feel their information may have been impacted to contact IDX to enroll in the free identity protection services being offered by calling 1-877-758-1726 or going to https://response.idx.us/HighlinePublicSchools. IDX representatives are available Monday through Friday from 6 am - 6 pm Pacific Time. Please note the deadline to enroll is July 2, 2025.

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 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 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 credit freeze or fraud alert, 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

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.

Highline School District Website Notice

Notice of Data Security Event

Highline Public Schools is notifying the community of an incident involving personal information on its systems. We are providing you with information about the incident, our response to it and resources we are making available to you to help protect your information, should you feel it appropriate to do so.

What happened? On September 7, 2024, we discovered we were the victim of a ransomware incident. We promptly took steps to secure our systems, and an investigation was conducted with the support of third-party computer forensic specialists. The investigation determined that an unknown actor gained access to certain systems on our network and accessed certain files. After the forensic investigation, Highline performed a detailed and labor-intensive review of the affected files to determine if personal information was involved and to identify the individuals associated with this information. This review has recently been completed.

What information was affected? The types of information impacted vary by individual and include name, address, date of birth, Social Security number, driver's license number, financial account information, passport number, digital signature, medical information, and health insurance information.

What is Highline doing in response? The confidentiality, privacy, and security of personal information is among our highest priorities. Upon becoming aware of this incident, we immediately took steps to secure our systems and initiated a full investigation. Additional security measures are being implemented to further protect against similar incidents moving forward. We also reported this incident to federal law enforcement. Additionally, we are offering credit monitoring and identity protection services for 12 months through IDX at no cost to you. Please note that you will not be automatically enrolled in these services. Should you wish to do so, you will need to enroll yourself in these services, as we are not able to do so on your behalf. You will find instructions on how to enroll in these services below in the section titled *Steps You Can Take to Help Protect Personal Information.*

What can Highline community members do to protect themselves? As a precautionary measure, individuals are encouraged to remain vigilant against incidents of identity theft by reviewing their account statements, credit reports and explanations of benefits for unusual activity and to detect errors. Any suspicious activity should promptly be reported to the appropriate insurance company, health care provider, or financial institution. Interested individuals can also review the information below for further guidance.

For More Information. If you have any questions or feel you or your student's data may have been impacted, please call our dedicated assistance line at 1-877-758-1726, Monday through Friday, from 6:00 am PT – 6 pm PT (excluding U.S. holidays). You may also write to Highline at 15675 Ambaum Blvd. SW, Burien, WA 98166.

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

We encourage you to contact IDX to enroll in the free identity protection services being offered by calling 1-877-758-1726 or going to https://response.idx.us/HighlinePublicSchools. IDX representatives are available Monday through Friday from 6 am - 6 pm Pacific Time. Please note the deadline to enroll is July 2, 2025.

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 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 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 credit freeze or fraud alert, 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

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.