



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Ryan C. Loughlin
Office: (267) 930-4786
Fax: (267) 930-4771
Email: rloughlin@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

January 17, 2025

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

To Whom It May Concern:

We represent Greater Lawrence Technical School District (“GLTSD”) located at 57 River Rd., Andover, Massachusetts 01810, and are writing to notify your office of an incident that may involve certain personal information relating to six (6) Maryland residents. By providing this notice, GLTSD does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On November 8, 2024, GLTSD became aware of unusual activity on its network resulting in a loss of network functionality. GLTSD promptly initiated an investigation into the nature and scope of the impact. The investigation determined the network had been subject to unauthorized access between November 4 and November 9, 2024, and that copies of certain files may have been taken from GLTSD’s network. GLTSD reviewed the potentially impacted information and on or around December 10, 2024, learned that the files contained personal information. On January 9, 2025, GLTSD completed efforts to locate address information for those individuals whose personal information may be in the files. The information that could have been subject to unauthorized access includes name, date of birth, health insurance information, and Social Security number.

Notice to Maryland Residents

On or about January 17, 2025, GLTSD provided written notice of this incident to six (6) Maryland 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, GLTSD moved quickly to investigate and respond to the incident, assess the security of GLTSD systems, and identify potentially affected individuals. GLTSD is also working to implement additional safeguards and training to its employees. GLTSD is providing access to credit monitoring services for 24 months, through Experian, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, GLTSD 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. GLTSD 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.

GLTSD is providing written notice of this incident to relevant state regulators, as necessary.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4786.

Very truly yours,

Ryan C. Loughlin of
MULLEN COUGHLIN LLC

RCL/kgj
Enclosure

EXHIBIT A



M7072 0000001 P001 T00001 *****SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01 INDIVIDUAL
123 ANY STREET
APT ABC
ANYTOWN, ST 12345-6789

A standard linear barcode representing the address information above it.

For More Information. GLTSD understands you may have questions about this event not addressed in the letter. If you have additional questions, please contact our dedicated assistance line at 833-918-5553. You may also write to 57 River Rd., Andover, Massachusetts 01810, Attn. Director of Human Resources.

Sincerely,

Greater Lawrence Technical School District

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for 24 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 24-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by April 30, 2025** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/credit
- Provide your **activation code**: ABCDEFGHI

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 833-918-5553 by April 30, 2025, Monday through Friday from 8 a.m. to 8 p.m. CST (excluding major U.S. holidays). Be prepared to provide engagement number B138584 as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*¹
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.



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/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 LLC, PO 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 LLC, PO Box 2000 Chester, PA 19016

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.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

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





MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Ryan C. Loughlin
Office: (267) 930-4786
Fax: (267) 930-4771
Email: rloughlin@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

March 5, 2025

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Supplemental Notice of Data Event

To Whom It May Concern:

We continue to represent Greater Lawrence Technical School District (“GLTSD”) located at 57 River Rd., Andover, Massachusetts 01810, and are writing to notify your office of an incident that may involve certain personal information relating to one (1) Maryland resident. By providing this notice, GLTSD does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On November 8, 2024, GLTSD became aware of unusual activity on its network resulting in a loss of network functionality. GLTSD promptly initiated an investigation into the nature and scope of the impact. The investigation determined the network had been subject to unauthorized access between November 4 and November 9, 2024 and that copies of certain files may have been taken from the network. GLTSD reviewed the potentially impacted information and on or around December 10, 2024, learned that the files contained personal information. GLTSD began providing written notice on January 17, 2025 as the investigation was ongoing. On January 30, 2025, GLTSD completed the review of all internal records to determine the full scope of individuals whose personal information may be in the files. The information that could have been subject to unauthorized access includes name, and Social Security number, date of birth, and health insurance information.

Notice to Maryland Residents

On or about March 5, 2025, GLTSD provided written notice of this incident to one (1) Maryland resident. 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, GLTSD moved quickly to investigate and respond to the incident, assess the security of GLTSD systems, and identify potentially affected individuals. GLTSD is also working to implement additional safeguards and training to its employees. GLTSD is providing access to credit monitoring services for twenty-four (24) months, through Experian, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, GLTSD is providing impacted individuals with guidance on how to better protect against identity theft and fraud. GLTSD 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.

GLTSD is providing written notice of this incident to relevant state regulators, as necessary.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4786.

Very truly yours,

A handwritten signature in blue ink, appearing to read "Ryan Loughlin", is enclosed in a light blue rectangular box.

Ryan C. Loughlin of
MULLEN COUGHLIN LLC

RCL/kgf
Enclosure

EXHIBIT A



Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

March 5, 2025



M9367-L01-0000001 P001 T00001 *****SCH 5-DIGIT 12345

SAMPLE A SAMPLE - L01 ADULT

APT ABC

123 ANY STREET

ANYTOWN, ST 12345-6789



NOTICE OF [SECURITY INCIDENT] / [DATA BREACH]

Dear Sample A. Sample:

Greater Lawrence Technical School District (“GLTSD”) writes to notify you of an event that involves some of your personal information. We take this event seriously and the privacy, security, and confidentiality of information in our care is among our highest priorities. While GLTSD is not aware of any actual or attempted misuse of your information, out of an abundance of caution, 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 November 8, 2024, GLTSD became aware of unusual activity on its network resulting in a loss of network functionality. GLTSD promptly initiated an investigation into the nature and scope of the impact. The investigation determined the network had been subject to unauthorized access between November 4 and November 9, 2024 and that copies of certain files may have been taken from our network. We reviewed the potentially impacted information and on or around December 10, 2024, we learned that the files contained personal information. On January 30, 2025, we completed our review of all internal records to determine the full scope of individuals whose personal information may be in the files.

What Information Was Involved? The information related to you in the files includes your name, date of birth, health insurance information, and Social Security number. Please note, there is currently no evidence of misuse of your information as a result of this event.

What We Are Doing. GLTSD takes this event and the security of information in our care very seriously. Upon learning of the event, we moved quickly to respond, secure the systems involved, assess the security of our network, and investigate the event. As part of our ongoing commitment to information security, we reviewed our policies, procedures, and security tools, and updated our employee training program.

Although we are not aware of any actual or attempted misuse of your information, we are also offering you access to 24 months of complimentary credit monitoring and identity protection services through Experian. Details of this offer and enrollment instructions may be found in the attached *Steps You Can Take to Protect Personal Information*. We encourage you to enroll in these services because we are unable to act on your behalf to do so.

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 over the next 12 to 24 months. You also can enroll to receive the complimentary credit monitoring services that we are offering to you. Please also review the information contained in the enclosed *Steps You Can Take to Protect Your Information*.

For More Information. GLTSD understands you may have questions about this event not addressed in the letter. If you have additional questions, please contact our dedicated assistance line at 1-833-931-7489 (toll free), Monday through Friday, from 9am - 9pm Eastern Time (excluding U.S. holidays). You may also write to 57 River Rd., Andover, Massachusetts 01810.

Sincerely,

Greater Lawrence Technical School District

B139891

0000001



M9367-L01

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for 24 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 24-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by May 30, 2025** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code**: ABCDEFGHI

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-833-931-7489 by May 30, 2025. Be prepared to provide engagement number B139891 as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

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/get-credit-report https://www.transunion.com/credit-freeze https://www.transunion.com/fraud-alerts
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud, 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, PO Box 2000 Chester, PA 19016

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.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.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.