



Aubrey L. Weaver
550 E. Swedesford Road, Suite 270
Wayne, Pennsylvania 19087
Aubrey.Weaver@lewisbrisbois.com
Direct: 215.253.7506

December 15, 2022

VIA ELECTRONIC MAIL

Attorney General Brian Frosh
Maryland Attorney General's Office
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-Mail: ldtheft@oag.state.md.us

Re: Notice of Data Security Incident

Dear Attorney General Frosh:

We represent the School Town of Munster ("STM"), a school district located in Munster, Indiana. This letter is being sent because personal information belonging to certain current and former STM students may have been involved in a recent data security incident, including an individual who may now reside in Maryland.

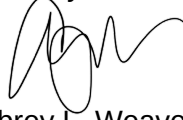
On October 26, 2022, STM became aware that a student gained access to and copied an administrative file from a food services system in April 2022. Through conducting an investigation of the issue, STM learned that the administrative file may have also been shared with other members of the school community. In response, STM began gathering information needed to notify the students whose information may have been involved.

On November 30, 2022, STM identified one (1) potentially affected Maryland resident whose name and Social Security number may have been involved.

STM notified the Maryland resident of this incident via U.S. Mail on December 6, 2022. In so doing, STM offered the notified Maryland resident one year of complimentary identity protection services through IDX. These services include \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration. Adults whose information may have been involved were also provided one year of complimentary credit monitoring services. A sample copy of the notification letter is attached to this correspondence.

STM takes the privacy and security of all information in its possession very seriously. If you have any questions or need additional information, please do not hesitate to contact me at (215) 253-7506 or aubrey.weaver@lewisbrisbois.com.

Sincerely,

A handwritten signature in black ink, appearing to read 'Aubrey L. Weaver', with a stylized, flowing script.

Aubrey L. Weaver of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enc.: Sample Consumer Notification Letter



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

To Enroll, Please Call:
1-833-896-9468
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: [REDACTED]

To the Parent or Guardian of
[REDACTED]
[REDACTED]
[REDACTED]

December 6, 2022

Re: Notice of Data Incident

Dear Parent or Guardian of [REDACTED],

We are writing to provide you with information about a recent data incident involving your student's personal information. At the School Town of Munster ("STM"), we strive to maintain the privacy and security of all information within our possession. Out of an abundance of caution, we are writing to notify you that this incident occurred and offering complimentary identity protection services as well as informing you about steps you can take to help safeguard your student's personal information.

What Happened. On October 26, 2022, STM became aware that a student gained access to and copied an administrative file from a food services system in April 2022. Through investigating this issue, STM learned that the administrative file may have also been shared with other members of the school community.

What Information Was Involved. The administrative file included your student's name, Social Security number, date of birth, student ID, address, as well as parents' names and email addresses.

What We Are Doing. As soon as we discovered this incident, we took steps to further secure our network systems and confirm appropriate access controls are in place for all systems. STM is working with the students involved, as well as their parent(s), to confirm that all copies of the administrative file have been deleted and none of the information reflected therein has been retained. STM has also taken appropriate disciplinary measures related to this matter.

Additionally, out of an abundance of caution, STM is providing you with information about steps that you can take to help protect your student's personal information and, as an added precaution, is offering complimentary identity theft protection services through IDX. IDX identity protection services include: 12 months of CyberScan monitoring, a \$1,000,000 insurance reimbursement policy and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your student's identity is compromised. The deadline to enroll is March 6, 2023.

What You Can Do. We recommend that you enroll your student in the complimentary IDX services using the enrollment code provided above. A description of the services being provided are included with this letter. We also recommend that you review the guidance included with this letter about steps you can take to protect your student's personal information.

For More Information. If you have questions or need assistance, please contact IDX at 1-833-896-9468, Monday through Friday from 8:00 am to 8:00 pm Central Time, excluding major U.S. holidays. IDX representatives are fully versed on this incident and can answer any questions you may have regarding the protection of your student's personal information.

STM takes this matter very seriously. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "Bret Heller", with a long horizontal flourish extending to the right.

Bret Heller, Superintendent
School Town of Munster

School Town of Munster
Administration Center
8616 Columbia Ave
Munster, IN 46321

Steps You Can Take to Protect Your Child's Information

Review Any Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant and review statements from your child's accounts closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

Personal Information of a Minor: You can request that each of the three national consumer reporting agencies perform a manual search for a minor's Social Security number to determine if there is an associated credit report. Copies of identifying information for the minor and parent/guardian may be required, including birth or adoption certificate, Social Security card, and government issued identification card. If a credit report exists, you should request a copy of the report and immediately report any fraudulent accounts to the consumer reporting agency. You can also report any misuse of a minor's information to the FTC at <https://www.identitytheft.gov/>. For more information about Child Identity Theft and instructions for requesting a manual Social Security number search, visit the FTC website: <https://www.consumer.ftc.gov/articles/0040-child-identity-theft>. Contact information for the three national credit reporting agencies is below.

Security Freeze: You may place a free credit freeze for minors under age 16. By placing a security freeze, someone who fraudulently acquires the minor's personal identifying information will not be able to use that information to open new accounts or borrow money in their name. You will need to contact the 3 national credit reporting bureaus listed below to place the freeze. Keep in mind that when you place the freeze, the minor will not be able to borrow money, obtain instant credit, or get a new credit card until the freeze is temporarily lifted or permanently removed. You must separately place a security freeze on the minor's credit file with each credit reporting agency. There is no charge to place, lift, or remove a security freeze on the minor's credit files. In order to place a security freeze, you may be required to provide the credit reporting agency with information that identifies you and/or the minor, including birth or adoption certificate, Social Security card, and government issued identification card.

Equifax
P.O. Box 105788
Atlanta, GA 30348
1-888-378-4329
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-800-831-5614
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on the minor's credit report. An initial fraud alert is free and will stay on the minor's credit file for at least one year. The alert informs creditors of possible fraudulent activity within the minor's report and requests that the creditor contact you prior to establishing any accounts in the minor's name. To place a fraud alert on the minor's credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov
1-877-438-4338

Maryland Attorney General
St. Paul Plaza
200 St. Paul Place
Baltimore, MD 21202
marylandattorneygeneral.gov
1-888-743-0023

New York Attorney General
Bureau of Internet & Technology Resources
28 Liberty Street
New York, NY 10005
ag.ny.gov
1-212-416-8433 / 1-800-771-7755

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in the minor's file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and

your rights pursuant to the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.



IDX Identity Protection Services

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.
2. **Activate the identity monitoring** provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. *You must have access to a computer and the internet to use this service.* If you need assistance, IDX will be able to assist you.
3. **Telephone.** Contact IDX at 1-833-896-9468 to speak with knowledgeable representatives about the appropriate steps to take to protect your identity.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help. If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

IDX Identity will include one-year enrollment into the following service components:

1. **CYBERSCAN** - Dark Web monitoring of underground websites, chat rooms, and malware, 24/7, to identify trading or selling of personal information like Social Security numbers, bank accounts, email addresses, medical ID numbers, driver's license numbers, passport numbers, credit and debit cards, phone numbers, and other unique identifiers.
2. **IDENTITY THEFT INSURANCE** - Identity theft insurance will reimburse members for expenses associated with restoring their identity should they become a victim of identity theft. If a member's identity is compromised, the policy provides coverage for up to \$1,000,000, with no deductible.
3. **FULLY-MANAGED IDENTITY RECOVERY** - IDX's fully-managed recovery service provides restoration for identity theft issues such as (but not limited to): account creation, criminal identity theft, medical identity theft, account takeover, rental application, tax fraud, benefits fraud, and utility creation. This service includes a complete triage process for affected individuals who report suspicious activity, a personally assigned ID Care Specialist to fully manage restoration of each case, and expert guidance for those with questions about identity theft and protective measures.