



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

Vincent F. Regan
Office: (267) 930-4842
Fax: (267) 930-4771
Email: vregan@mullen.law

309 Fellowship Road, Suite 200
Mt. Laurel, NJ 08054

April 25, 2024

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 Francis Howell School District (“FHSD”) located at 801 Corporate Centre Drive O’Fallon, Missouri 63368, and are writing to notify your office of an incident that may affect the security of certain personal information relating to three (3) Maryland residents. By providing this notice, FHSD 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 or about February 15, 2024, Francis Howell School District identified unusual activity on certain network systems and determined that it was experiencing a cyber incident. FHSD promptly began an investigation to determine the full nature and scope of the event. Based on the investigation, FHSD determined that certain information was copied from the system on or about February 8, 2024, without authorization as part of the cyber incident.

The information that could have been subject to unauthorized access includes name, and Social Security number.

Notice to Maryland Residents

On or about April 25, 2024, FHSD provided written notice of this incident to three (3) 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, FHSD moved quickly to investigate and respond to the incident, assess the security of FHSD systems, and identify potentially affected individuals. Further, FHSD notified federal law enforcement regarding the event. FHSD is also working to implement additional safeguards and training to its employees. FHSD is providing access to credit monitoring services for one (1) year, through TransUnion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, FHSD 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. FHSD 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.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4842.

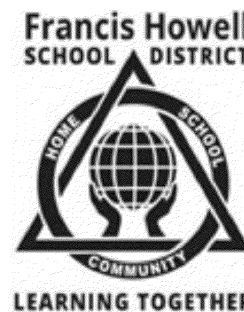
Very truly yours,

Vincent F. Regan of
MULLEN COUGHLIN LLC

VFR/cob
Enclosure

EXHIBIT A

Francis Howell School District
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



April 25, 2024

NOTICE OF DATA DATA BREACH

Dear [REDACTED]

We are writing to make you aware of a recent incident that affects your personal information. We take this incident very seriously and are providing details of the incident and information on the resources available to you to help protect your information from possible misuse, should you feel it is appropriate to do so.

What Happened? In mid-February 2024, Francis Howell School District identified unusual activity on certain network systems and determined that it was experiencing a cyber incident. We promptly began an investigation to determine the full nature and scope of the event. Based on the investigation, we determined that certain information was copied from the system on or about February 8, 2024 without authorization as part of the cyber incident. We continued reviewing this information and on March 15, 2024 confirmed that certain information relating to you was potentially affected.

What Information Was Involved? The type of information related to you potentially affected by this incident includes the following: your name and Social Security number, bank account number, account type, and routing number.

What We Are Doing. We take the confidentiality, privacy, and security of information in our care seriously. In response to this incident, we promptly took steps to secure our systems and conducted a detailed investigation to confirm the full nature and scope of the event. We also notified federal law enforcement of this incident.

As an added precaution, we are providing you with access to **Credit Monitoring/Credit Report/Credit Score** services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services. Please review the instructions in the attached *Steps You Can Take to Help Protect Your Information* for additional information on these services.

What You Can Do. We encourage you to remain vigilant against instances of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. We also encourage you to review the further information on steps you can take to protect personal information and to enroll in the identity protection services by following the instruction in the *Steps You Can Take to Help Protect Your Personal Information* section below. You may also write to us at 801 Corporate Centre Drive, O'Fallon, MO 63368.

000010102G0500

P

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call 1-833-543-2481. Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays.

Sincerely,

A handwritten signature in black ink, appearing to read "Kenneth Roumpos". The signature is fluid and cursive, with the first name "Kenneth" and last name "Roumpos" clearly distinguishable.

Dr. Kenneth Roumpos
Superintendent
www.fhdschools.org

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

To enroll in Credit Monitoring services at no charge, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted please provide the following unique code to receive services: **32738BBF726C**. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.



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.

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 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.