

WOODS ROGERS VANDEVENTER BLACK

ATTORNEYS AT LAW

F. ELIZABETH BURGIN WALLER
(540) 983-7625
Beth.Waller@wrvbllaw.com

April 17, 2023

Via E-mail (ldtheft@oag.state.md.us)

Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202

To Whom It May Concern:

In accordance with Md. Code Ann. § 14-3504(h)(1), I am writing on behalf of my client, Fairfax County Public Schools (“FCPS”), to notify you regarding the nature and circumstances of a recent data security incident. FCPS’s mailing address is 8115 Gatehouse Road, Falls Church, VA 22042.

On or about December 19, 2022, an unauthorized user accessed two FCPS business email accounts. The incident was discovered shortly thereafter. Upon discovering the incident, FCPS engaged leading outside cybersecurity experts who confirmed that the unauthorized user’s access was limited only to FCPS’s email platform and further secured FCPS systems against any other unauthorized access. However, the impacted email accounts contained certain personally identifiable information, primarily certain mental or physical health information that FCPS teachers use to provide certain educational services to students.

It is unknown whether the unauthorized user was able to discover or access the personal information present in these accounts. There is no evidence indicating that the unauthorized user was able to use any of the personal information the email accounts contained to cause any harm, or for any malicious purpose.

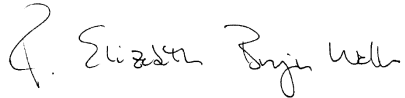
As described in detail in the attached notification letter, the student information involved may have included one or more of the following types of information: name, address, and/or certain mental or physical health history, condition, treatment, or diagnosis information that FCPS teachers use to provide educational services to students. Examples of this medical information include information about a child’s allergies or medically restricted diets, EpiPen ownership, disability or health condition (if applicable), and whether a student has a history of seizures. Please note that the impacted business email accounts did not contain Social Security numbers or any other information that could harm the financial identity of a Marylander.

[REDACTED]

Collectively, there are approximately eight (8) Maryland residents potentially impacted by this incident. We have worked expeditiously to identify each of these individuals. Attached for your reference is a copy of the notice we plan to mail out to impacted Maryland residents on February 10, 2023.

If you have any questions, please contact me via email at beth.waller@wrvblaw.com or via phone at 540.983.7625.

Very truly yours,

A handwritten signature in cursive script that reads "F. Elizabeth Burgin Waller". The signature is written in black ink and is positioned below the typed name.

F. Elizabeth Burgin Waller
Principal
Woods Rogers Vandeventer Black PLC

Enclosures



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

February 10, 2023

i9812-L02-0000002 T00001 P001 *****SCH 5-DIGIT 12345

PARENT OR GUARDIAN OF
SAMPLE A SAMPLE - L02 MINOR
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789



Dear Parents/Guardians of Sample A. Sample,

Fairfax County Public Schools (“FCPS”), like many school systems and organizations across the country, has unfortunately been the victim of an email compromise incident where an unauthorized user briefly gained access to two of FCPS’s business email accounts. We are writing to share with you how this incident may have affected health-related information related to your student and, as a precaution, to provide you with steps you can take to protect their information.

Although we have no evidence that the unauthorized user was successful in removing your student’s information from the two compromised FCPS email accounts or is using it for a malicious purpose, we wanted to alert you to this matter. As described below, the information contained in the account was health related information (such as a child’s allergies or Epi-Pen use) that would not permit access to a financial account or to create credit. However, out of an abundance of caution, we have arranged for your child to have free credit monitoring through our cyber insurance carrier if you choose it.

FCPS takes the privacy and security of your student’s personal information very seriously and we sincerely regret any concern this incident may cause you or your student.

What Happened and What Information Was Involved

The incident occurred on or about December 19, 2022, when an unauthorized user briefly gained access to two FCPS business email accounts by means of social engineering. We conducted an extensive review of the two email accounts to identify information contained in the emails and anyone who may have been impacted by this incident.

Based on this review, we have determined that the information in the email account may have included one or more of the following types of information: your student’s name coupled with certain mental or physical health history, condition, treatment, or diagnosis information that FCPS teachers use to provide educational services to your student. Examples of this include information about a student’s allergies or medically restricted diets, EpiPen ownership, disability or health condition (if applicable), and whether your student may have a history of seizures.

Please note that the impacted business email accounts did **not** contain information such as your student’s Social Security number. **However, even though we believe this incident did not place your student’s financial identity at risk, we have arranged for free credit monitoring to your student**

0000002



out of an abundance of caution. More information about the free credit monitoring services we are providing through Experian can be found in the attached Identity Theft and Protection Guide.

What We Are Doing

Upon discovering the incident, we began an investigation and engaged leading outside cybersecurity experts who confirmed that the unauthorized user's access was limited only to these two business email accounts on FCPS's web-based email platform.

We have no evidence to determine whether the unauthorized user was able to discover or access your student's information within these email accounts. We also have no evidence that the unauthorized user used any of the information in the email accounts to cause any harm, or that your student's information was used for any malicious purpose. However, out of an abundance of caution, we are notifying you of this event and are asking you to stay vigilant regarding your student's personal information.

We have notified the Virginia State Police's Fusion Intelligence Center, the national Cybersecurity and Infrastructure Security Agency (CISA), and the FBI Cyber Crimes Division of this incident. We intend to support any law enforcement investigation into this incident. We take our obligation to safeguard personal information very seriously and we are continuing to evaluate additional actions to strengthen our network security in the face of an ever-evolving cyber threat landscape.

What You Can Do

Please review the enclosed Identity Theft and Protection Guide for additional information on how to protect against identity theft and fraud. You may also take advantage of the complimentary credit monitoring services being offered for your student through Experian *IdentityWorks*. Information regarding the credit monitoring enrollment is included in the attached Identity Theft and Protection Guide.

For More Information

If you have any further questions regarding this matter or the credit monitoring services provided, please call **(888) 397-0104** toll-free Monday through Friday 9 a.m. to 11 p.m. EST., or Saturday and Sunday from 11 a.m. to 8 p.m. EST (excluding major U.S. holidays). Please be prepared to provide your engagement number **B084963**. Please also note that FCPS is utilizing Experian's return mail service, so the return address on this letter is to their mailing center.

We deeply regret that this incident occurred and are committed to supporting you.

Sincerely,



Dr. Michelle Reid
Superintendent
Fairfax County Public Schools

IDENTITY THEFT PROTECTION GUIDE AND INFORMATION

The following guide contains information regarding how to enroll your child in the free credit monitoring provided as well as additional resources on identity theft protection.

Details Regarding Enrollment with Experian

To help protect your minor dependent's identity, we are offering complimentary access to Experian IdentityWorksSM for twelve months.

If you believe there was fraudulent use of your minor dependent's 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 twelve 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 twelve-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your minor dependent's personal information, please follow the steps below:

- Ensure that you **enroll by** May 31, 2023 (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/minorplus>
- Provide your **activation code: ABCDEFGHI**
- Provide your minor's information when prompted

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 **(888) 397-0104** by May 31, 2023. Be prepared to provide engagement number **B084963** as proof of eligibility for the Identity Restoration services by Experian.

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:

- **Social Security Number Trace:** Monitoring to determine whether enrolled minors in your household have an Experian credit report. Alerts of all names, aliases and addresses that become associated with your minor's Social Security number (SSN) on the Experian credit report.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **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.

** 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.

Additional Information About Identity Theft Protection

Monitor Your Accounts

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax®
P.O. Box 740241
Atlanta, GA 30374-0241
1-800-685-1111
www.equifax.com

Experian
P.O. Box 9701
Allen, TX 75013-9701
1-888-397-3742
www.experian.com

TransUnion®
P.O. Box 1000
Chester, PA 19016-1000
1-800-888-4213
www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Credit Freeze

You have the right to put a security freeze, also known as a credit freeze, on your credit file, so that no new credit can be opened in your name without the use of a Personal Identification Number (PIN) that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. Should you wish to place a credit freeze, please contact all three major consumer reporting agencies listed below.

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/credit-report-services

Experian
P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016-2000
1-888-909-8872
www.transunion.com/credit-freeze

You must separately place a credit freeze on your credit file at each credit reporting agency. The following information should be included when requesting a credit freeze:

- 1) Full name, with middle initial and any suffixes;
- 2) Social Security number;
- 3) Date of birth (month, day, and year);
- 4) Current address and previous addresses for the past five (5) years;
- 5) Proof of current address, such as a current utility bill or telephone bill; and
- 6) Other personal information as required by the applicable credit reporting agency.

If you request a credit freeze online or by phone, then the credit reporting agencies have one (1) business day after receiving your request to place a credit freeze on your credit file report. If you request a lift of the credit freeze online or by phone, then the credit reporting agency must lift the freeze within one (1) hour. If you request a credit freeze or lift of a credit freeze by mail, then the credit agency must place or lift the credit freeze no later than three (3) business days after getting your request.

Fraud Alerts

You also have the right to place an initial or extended fraud alert on your file at no cost. An initial fraud alert lasts 1-year and 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 7 years. Should you wish to place a fraud alert, please contact any one of the agencies listed below. The agency you contact will then contact the other two credit agencies.

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-766-0008
[www.equifax.com/personal/
credit-report-services](http://www.equifax.com/personal/credit-report-services)

Experian
P.O. Box 9554
Allen, TX 75013-
9554
1-888-397-3742
[www.experian.com/
fraud/center.html](http://www.experian.com/fraud/center.html)

TransUnion
P.O. Box 2000
Chester, PA 19016-2000
1-800-680-7289
[www.transunion.com/fraud-
victim-resource/place-
fraud-alert](http://www.transunion.com/fraud-victim-resource/place-fraud-alert)

Monitor Your Personal Health Information

If applicable to your situation, we recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive the regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the website of the California Office of Privacy Protection at www.privacy.ca.gov to find more information about your medical privacy.



Additional Information

You can further educate yourself regarding identity theft and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC.

The Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.ftc.gov/idtheft

For Virginia residents: You may contact the Virginia Attorney General's Office, 202 North Ninth Street, Richmond, Virginia 23219, <https://www.oag.state.va.us/contact-us/contact-info>.

For North Carolina residents: The North Carolina Attorney General's Office may be contacted at 9001 Mail Service Center, Raleigh, NC 27699, (919) 716-6000, www.ncdoj.gov/contact-doj/.

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For New York residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov/>.

For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html.

For Rhode Island residents: You may contact the Rhode Island Office of the Attorney General at 150 South Main Street, Providence, RI 02903, 1-401-274-4400, <https://riag.ri.gov/>.

For District of Columbia residents: You may contact the Office of the Attorney General for the District of Columbia at 400 6th Street, NW, Washington, DC 20001, 1-202-442-9828, <https://oag.dc.gov/consumer-protection/consumer-alert-online-privacy>.

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.