



DEF  
2020 NOV 1

John E. Foster, Division Counsel  
Office of Division Counsel  
8115 Gatehouse Road  
Falls Church, Virginia 22042  
Phone: 571-423-1250 E-mail jefoster@fcps.edu

**November 13, 2020**

Office of the New Hampshire Attorney General  
33 Capitol Street  
Concord, NH 03301

To Whom It May Concern:

In accordance with N.H. Rev. Stat. Ann. § 359-C:20, I am writing on behalf of Fairfax County Public Schools ("FCPS") to notify you regarding the nature and circumstances of a recent data security incident.

FCPS recently learned, during the first week of September 2020, that FCPS was the victim of a cyber attack involving ransomware. A sophisticated group of cyber criminals, known as the Maze group, is claiming responsibility for the attack. FCPS is just one of more than 1,000 educational systems to suffer a ransomware attack in the past year. Since September alone, multiple school districts have been reportedly victimized by these attacks.

Based on FCPS' investigation, we believe that the cyber criminals accessed and acquired sensitive personal information relating to students, employees and applicants stored on a very limited number of FCPS systems, and subsequently posted them on the dark web. As described in detail in the attached notification letters to affected individuals, the information acquired by the cyber criminals varied for different categories of individuals, and may have included names, dates of birth, ethnicity, addresses, social security numbers, health diagnoses, learning disabilities, health insurance account numbers, grades, disciplinary action, or other types of sensitive personal information.

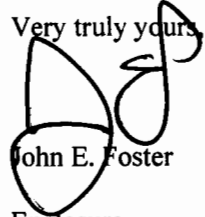
We discovered the attack on or about September 6, and promptly took steps to secure our systems and begin investigating the nature and scope of the incident. We have engaged leading outside security experts to assist with our investigation and are implementing various cyber security enhancements. We are working closely with the FBI and Virginia State Police, and supporting their criminal investigations to bring the attackers to justice. FCPS has arranged to provide potentially affected individuals with one year of identity/credit monitoring and identity restoration services through Experian at no cost to them.

Collectively, there are approximately 20 New Hampshire residents affected by this issue. Attached for your reference is a copy of the notice sent to former employees, applicants and other individuals on November 9, 2020.

November 13, 2020  
Page 2

Please do not hesitate to contact me if you have any questions.

Very truly yours,

A handwritten signature in black ink, appearing to read "John E. Foster". The signature is stylized and somewhat cursive, with a large initial "J" and "F".

John E. Foster

Enclosure



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

November 9, 2020

F9489-L03-0000003 T00001 P001 \*\*\*\*\*MIXED AADC



SAMPLE A SAMPLE  
APT 123  
123 ANY ST  
ANYTOWN, US 12345-6789



Dear Sample A Sample,

As you may know, during the first week of September 2020, Fairfax County Public Schools (“FCPS”) was the victim of a cyber attack involving ransomware. We are writing to notify you that some of your personal information was affected by this incident.

Ransomware is a form of malware that is used by hackers to prevent users from accessing files, and in some cases, extract and hold data hostage until a ransom is paid. In this case, a sophisticated group of cyber criminals, known as the Maze group, is claiming responsibility for the attack. In the midst of the challenges associated with virtual learning and the pandemic, cyber criminals have targeted educational systems around the country in an attempt to disrupt their operations. FCPS is just one of more than 1,000 educational systems to suffer a ransomware attack in the past year. Since September alone, multiple school districts have been reportedly victimized by these attacks.

**What We Are Doing**

We discovered the attack on or about September 6, and promptly took steps to secure our systems and begin investigating the nature and scope of the incident. We have engaged leading outside security experts to assist with our investigation, and implemented various cyber security enhancements. We are working closely with the FBI and Virginia State Police, and supporting their criminal investigations to bring the attackers to justice. We have also notified the Virginia Computer Crime Section of the Virginia Attorney General’s Office. FCPS takes our obligation to safeguard personal information very seriously and we are continuing to evaluate additional actions to further strengthen our network security.

**What Information Was Involved**

Based on our investigation, we believe that the cyber criminals accessed and acquired certain employment-related records stored on the affected FCPS HR systems, such as social security number, information related to the provision of health benefits such as health insurance account information, date of birth, and address. This information was subsequently posted on the dark web.



## What You Can Do

We are alerting you about this issue so you can take steps to help protect your identity and credit information. You are entitled to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll-free at 1-877-322-8228. We encourage you to remain vigilant by reviewing your account statements and monitoring your free credit reports.

**In addition, we have arranged to offer credit monitoring and identity restoration services from Experian at no cost to you.** The enclosed Reference Guide provides more information about the services and how to register for them, requesting credit reports, and additional recommendations on the protection of personal information.

## For More Information

We deeply regret that this incident occurred and are committed to supporting you. If you have any questions regarding this issue, please call (855) 347-6550 toll-free Monday through Friday from 9 am – 11 pm Eastern, or Saturday and Sunday from 11 am – 8 pm Eastern (excluding major U.S. holidays). Be prepared to provide your engagement number ENGAGE# included in the attached guide.

Sincerely,



Scott Brabrand, Superintendent  
Fairfax County Public Schools

## Reference Guide

We encourage affected individuals to take the following steps:

**Register for Credit Monitoring and Identity Restoration Services.** To help protect your identity, we are offering complimentary access to Experian IdentityWorks<sup>SM</sup> for ## months. You may activate the fraud detection tools available through Experian IdentityWorks as a complimentary ##-month membership. This product provides superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by February 28, 2021** (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**

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<sup>TM</sup>:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance<sup>\*\*</sup>:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you wish to enroll your spouse or minor dependents as well, contact FCPS Human Resources at [IDprotection@fcps.edu](mailto:IDprotection@fcps.edu) to obtain the Activation Codes necessary for enrollment and follow the same enrollment process described above. In your email to HR, please state the number of codes you are requesting broken down by spouse and number of minor dependent children.

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 ## 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](http://www.ExperianIDWorks.com/restoration).

\* 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.



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 (855) 347-6550. Be prepared to provide engagement number ENGAGE# as proof of eligibility for the Identity Restoration services by Experian.

**Order Your Free Credit Report.** To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com), call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at [www.consumer.ftc.gov](http://www.consumer.ftc.gov) and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three consumer reporting agencies provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store or commercial names. The consumer reporting agency will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the consumer reporting agencies of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate consumer reporting agency by telephone and in writing. Consumer reporting agency staff will review your report with you. If the information cannot be explained, then you will need to call the creditors involved. Information that cannot be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

**Report Incidents.** If you detect any unauthorized transactions in a financial account, promptly notify your payment card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General. If you believe your identity has been stolen, the FTC recommends that you take these steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. For streamlined checklists and sample letters to help guide you through the recovery process, please visit <https://www.identitytheft.gov/>.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft:

Federal Trade Commission  
Consumer Response Center  
600 Pennsylvania Avenue, NW  
Washington, DC 20580  
1-877-IDTHEFT (438-4338)  
[www.ftc.gov/idtheft/](http://www.ftc.gov/idtheft/)

**Consider Placing a Fraud Alert on Your Credit File.** To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three consumer reporting agencies. For more information on fraud alerts, you also may contact the FTC as described above.

Equifax	Equifax Information Services LLC P.O. Box 740241 Atlanta, GA 30374	1-800-525-6285	www.equifax.com
Experian	Experian Inc. P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19016	1-800-680-7289	www.transunion.com

**Consider Placing a Security Freeze on Your Credit File.** You may wish to place a “security freeze” (also known as a “credit freeze”) on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually. There is no charge to place or lift a security freeze. For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information.

The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver’s license or military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)

**For Iowa Residents.** You may contact law enforcement or the Iowa Attorney General’s Office to report suspected incidents of identity theft. This office can be reached at:

Office of the Attorney General of Iowa  
Hoover State Office Building  
1305 E. Walnut Street  
Des Moines, IA 50319  
(515) 281-5164  
[www.iowaattorneygeneral.gov](http://www.iowaattorneygeneral.gov)



**For Maryland Residents.** You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You may contact the Maryland Attorney General at:

Maryland Office of the Attorney General  
Consumer Protection Division  
200 St. Paul Place  
Baltimore, MD 21202  
(888) 743-0023 (toll-free in Maryland)  
(410) 576-6300  
[www.oag.state.md.us](http://www.oag.state.md.us)

**For Massachusetts Residents.** You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request to place a security freeze on your account.

**For New Mexico Residents.** You have rights under the federal Fair Credit Reporting Act (“FCRA”). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf> or [www.ftc.gov](http://www.ftc.gov).

**For New York Residents.** You can obtain information from the New York State Office of the Attorney General about how to protect yourself from identity theft and tips on how to protect your privacy online. You can contact the New York State Office of the Attorney General at:

Office of the Attorney General  
The Capitol  
Albany, NY 12224-0341  
1-800-771-7755 (toll-free)  
1-800-788-9898 (TDD/TTY toll-free line)  
<https://ag.ny.gov/>

Bureau of Internet and Technology (BIT)  
28 Liberty Street  
New York, NY 10005  
Phone: (212) 416-8433  
<https://ag.ny.gov/internet/resource-center>



**For North Carolina Residents.** You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at:

North Carolina Attorney General's Office  
9001 Mail Service Center  
Raleigh, NC 27699-9001  
(877) 566-7226 (toll-free in North Carolina)  
(919) 716-6400  
[www.ncdoj.gov](http://www.ncdoj.gov)

**For Oregon Residents.** We encourage you to report suspected identity theft to the Oregon Attorney General at:

Oregon Department of Justice  
1162 Court Street NE  
Salem, OR 97301-4096  
(877) 877-9392 (toll-free in Oregon)  
(503) 378-4400  
<http://www.doj.state.or.us>

**For Rhode Island Residents.** You may obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General at:

Rhode Island Office of the Attorney General  
Consumer Protection Unit  
150 South Main Street  
Providence, RI 02903  
(401)-274-4400  
<http://www.riag.ri.gov>

You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request for a security freeze on your account.

**For Washington, D.C. Residents.** You may obtain information about preventing and avoiding identity theft from the Office of the Attorney General for the District of Columbia at:

Office of the Attorney General for the District of Columbia  
441 4th Street NW  
Suite 1100 South  
Washington, D.C. 20001  
(202)-727-3400  
<https://oag.dc.gov/>

