Floyd County Public Schools ("FCPS"), like many school systems around the country, has unfortunately become the victim of a cybersecurity incident. We are posting to share what we know about the incident and how it may have potentially affected personal information. Please note that FCPS does not believe that this incident has resulted in the misuse of personal information for any malicious purpose.

What Happened?

On or around August 23, 2024, we received a tip from law enforcement suggesting suspicious activity on FCPS computer systems. FCPS immediately engaged some of the nation's leading outside cybersecurity experts to mitigate disruption to our systems and assist in a forensic investigation into the matter. School was closed on Friday August 23, 2024, while these experts analyzed the security of our technology environment. Fortunately, thanks to a timely tip from law enforcement and FCPS's rapid response, our systems were rapidly secured, and school resumed the following Monday.

Once FCPS systems were secured, we engaged an extensive investigation to determine the scope of information that could have been implicated. As is typical in these situations, it has taken some time to understand the scope of this matter.

FCPS has already notified our families and employees of this incident through informal updates. We recently mailed a formal notification letter to all students and all employees.

What Information Was Involved?

We have determined that some personal information might have been accessible to the cyber criminals. Accessible information related to school operations and did not contain student data. However, the school system recognizes that it has been from time-to-time entrusted with personal information pertaining to individuals beyond its current students and employees. The following types of personal information may have been subjected to unauthorized access or acquisition as a result of this incident: names, addresses, dates of birth, driver's license numbers, Social Security numbers, and medical information, such as an individual's medical or mental health history, mental or physical condition, treatment or diagnosis by a health care professional, or health insurance policy number.

What Is FCPS Doing In Response?

FCPS takes privacy and data security very seriously and we sincerely regret any concern this incident may cause you. We have contacted and are cooperating with law enforcement from the Virginia State Police's Virginia Fusion Center and the Cybersecurity and Infrastructure Security Agency of Homeland Security.

To relieve concerns and restore confidence following this incident, we have also arranged to offer credit monitoring and identity restoration services from Kroll at no cost to you. If you want credit monitoring, please email us at privacy@floyd.k12.va.us.

At the end of this notice, we have also included tips to protect your information further.

At this point in our investigation, we do not have any reason to believe that information is being used for harm. Still, out of an abundance of caution, we are offering these resources for your confidence.

For More Information

For more information about the incident or to request credit monitoring, please contact us at privacy@floyd.k12.va.us.

FCPS remains committed to the privacy and security of our schools and the personal information entrusted with us. We deeply regret the inconvenience or concern caused by this incident.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

1. **Monitor your accounts.** Regularly check your bank and credit card statements for unauthorized transactions or charges that could possibly occur during any security event.

2. **Sign up for a free credit report.** You may periodically obtain your free credit report from one or more national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com or 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	**Experian**	**TransUnion**
P.O. Box 105788 Atlanta, GA 30348-5788 1-800-685-1111 www.equifax.com/personal/ credit-report-services	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 www.experian.com/ freeze/center.html	P.O. Box 2000 Chester, PA 19016-2000 1-800-916-8800 www.transunion.com/ credit-freeze

3. **Review the report carefully.** Look for accounts or creditor inquiries you did not initiate or recognize. Check for inaccurate information, such as a home address or social security number. If you see anything you need help understanding, contact the credit reporting agency immediately.

4. **Consider freezing your credit.** You can put a free security freeze on your credit file so that new credit cannot be opened in your name without using a personal identification number (PIN) issued when you initiate the freeze. However, if you place a credit freeze, potential creditors and other third parties can only access your credit report if you temporarily lift the freeze. Therefore, using this tool could delay your ability to obtain credit. You must contact all three national consumer reporting agencies listed below to place a credit freeze:

Equifax	**Experian**	**TransUnion**
P.O. Box 105788 Atlanta, GA 30348-5788 1-800-685-1111 www.equifax.com/personal/ credit-report-services	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 www.experian.com/ freeze/center.html	P.O. Box 2000 Chester, PA 19016-2000 1-800-916-8800 www.transunion.com/ credit-freeze

5. **Create a fraud alert.** You can also place an initial or extended fraud alert on your file at no cost. An initial fraud alert will stay on your credit file for one year. The alert informs creditors of possible fraudulent activity within your report and requires the creditor to verify your identity before extending new credit. Should you wish to place a fraud alert, please contact any **one of the three** major consumer reporting agencies listed above. The agency you contact will then contact the other two.

6. **Change your passwords.** Update your passwords across all accounts, choosing strong, unique passwords. Excellent passwords are at least 12-16 characters and include a mix of uppercase and lowercase letters, numbers, and special characters. This is a regular best practice, regardless of this recent incident.

7. **Remain vigilant.** Be cautious of emails, phone calls, or messages asking for personal information. Scammers often use data breaches to launch phishing and other attacks. Verify the authenticity of any request before providing information.

8. **Learn more.** You can further educate yourself about identity theft and how to protect yourself at www.ftc.gov/idtheft.