Appendix

Spotswood Public Schools ("Spotswood") completed an investigation into unauthorized access to some of its computer systems. Spotswood is a pre-kindergarten through twelfth grade public school district in New Jersey. Upon discovering the incident, Spotswood immediately took steps to secure its network, contacted law enforcement, and began an investigation with the assistance of a cybersecurity firm. The investigation determined that an unauthorized person obtained access to some of Spotswood's systems on September 11, 2021, and took some files out of its network. Spotswood reviewed the files that were involved. On October 27, 2021, Spotswood determined that personal information for one Maine resident was contained in the files that were taken by the unauthorized person, including the individual's name and one or more of the following data elements: Social Security number, driver's license number, and/or financial account information.

On November 18, 2021, Spotswood will mail a notification letter to the Maine resident in accordance with Me. Rev. Stat. Tit. 10, §1348, via United States First-Class mail.[1] A sample copy of the notification letter is enclosed. Spotswood is offering the Maine resident access to a complimentary one-year subscription to credit monitoring, fraud consultation, and identity restoration services through Kroll. Spotswood is recommending that the individual remains vigilant to the possibility of fraud or identity theft by reviewing their account statements for unauthorized activity. Spotswood has also established a dedicated call center that individuals may call with related questions.

To further protect personal information, Spotswood will continue to review its systems and is taking steps to enhance its existing security protocols and implementing multifactor authentication for its users.

[1] This report is not, and does not constitute, a waiver of Spotswood's objection that Maine lacks personal jurisdiction over the company related to this matter.

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

Spotswood Public Schools understands the importance of protecting the information we maintain. I am writing to inform you of an incident that may have involved some of your personal information. This notice explains the incident, measures we have taken, and some steps that you may consider taking in response.

We completed an investigation into unauthorized access to some of our computer systems. Upon discovering the incident, we immediately took steps to secure our network, contacted law enforcement, and began an investigation with the assistance of a cybersecurity firm. We determined through the investigation that an unauthorized person obtained access to some of our systems on September 11, 2021, and took some files out of our network. We reviewed the files that were involved and, on October 27, 2021, determined that some of your information was contained in the files that were taken by the unauthorized person, including your <<b2b_text_1(Name, Data Elements)>>.

We encourage you to remain vigilant by reviewing your account statements and credit reports for any unauthorized activity. If you see charges or activity you did not authorize, please contact your financial institution immediately. As an added precaution, we are offering identity monitoring services through Kroll at no cost to you for one year. Your identity monitoring services include credit monitoring, fraud consultation, and identity theft restoration services.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6(Activation Deadline)>> to activate your identity monitoring services.

Membership Number: **<<Membership Number s_n>>**

For additional steps you can take in response to the incident, please see the pages that follow this letter.

Your confidence and trust are important to us, and we regret any inconvenience or concern this incident may cause. To further protect personal information, we continue to review our systems and are taking steps to enhance our existing security protocols. If you have any questions, please call (855) 912-1511 from 9:00 am to 6:30 pm Eastern time, Monday through Friday, excluding major U.S. holidays.

Sincerely,

Vita Marino

Vita Marino
Spotswood Board of Education
Business Administrator

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Triple Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax,* PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

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

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Additional Information for residents of North Carolina:

North Carolina residents may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov