



Aubrey L. Weaver
Constangy, Brooks, Smith & Prophete, LLP
Cybersecurity & Data Privacy Team
1650 Market Street, Suite 3600
Philadelphia, PA 19103
AWeaver@constangy.com
215-770-4234

March 3, 2025

VIA ELECTRONIC MAIL

Attorney General Anthony G. Brown
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 Security Incident

Dear Attorney General Brown:

Constangy, Brooks, Smith & Prophete, LLP, represents Racine Unified School District (“RUSD”), a school district in Wisconsin. RUSD takes the protection of all information within its possession very seriously and has taken measures to reduce the likelihood of a similar incident reoccurring. This notice is being sent on behalf of RUSD because personal information for 3 Maryland residents could have been involved in a recent data security incident.

1. Nature of the Security Incident

On December 13, 2024, RUSD became aware of potentially suspicious activity on its network. Upon discovery, it promptly took steps to terminate the activity and secure its environment. In addition, RUSD engaged cybersecurity experts to investigate. The investigation determined that certain data may have been accessed or downloaded without authorization. After a thorough review of the information, RUSD determined that certain personal information was contained in the potentially affected data and took steps to locate information needed to complete notification. These efforts concluded in February 2025, and notice was provided promptly thereafter.

The potentially affected information may have included individuals’ names and Social Security number.

2. Number of Maryland Residents Affected

RUSD notified 3 Maryland residents within the potentially affected population on February 28, 2025, via USPS First-Class Mail. A sample copy of the notification letter sent to individuals is included with this correspondence.

3. Steps Taken Relating to the Incident

As soon as RUSD discovered the unusual network activity, it took steps to secure its systems and launched an investigation to determine learn more about what happened and what information could have been involved. RUSD has implemented additional safeguards to help protect its systems and to reduce the risk of a similar incident occurring in the future.

RUSD has established a toll-free call center through Cyberscout, a TransUnion company specializing in fraud assistance and remediation services, to answer questions about the incident and address related concerns. Additionally, RUSD is providing notified individuals with identity protection services through TransUnion. These identity protection services include: 12 months of Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge.

4. Contact Information

If you have any questions or need additional information, please do not hesitate to contact me at 215-770-4234 or aweaver@constangy.com.

Sincerely,

A handwritten signature in black ink, appearing to read 'Aubrey L. Weaver', with a stylized, flowing script.

Aubrey L. Weaver
Partner, Constangy Cyber Team

Attachment: Sample Notification Letter

Racine Unified School District
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



February 28, 2025

Subject: **Notice of Data Data Security Incident**

Dear [REDACTED],

We are writing to inform you of a data security incident that may have involved your personal information. Racine Unified School District ("RUSD") is committed to maintaining our employees' trust and demonstrating our commitment to data privacy and security. This letter has information about the incident and steps you can take to protect your information, including enrolling in the complimentary credit monitoring and identity protection services we are making available to you.

What happened? On December 13, 2024, RUSD learned of unusual activity in our network. In response, we immediately took measures to terminate the activity and secure our systems. In addition, we engaged cybersecurity experts to investigate. Our investigation determined that certain data may have been accessed or downloaded without authorization. After a thorough review of the information, we determined that certain personal information was contained in the potentially affected data. We then took steps to locate the information needed to complete notification to the individuals involved. This process was completed on February 18, 2025.

What Information Was Involved? The information potentially impacted in connection with this incident varies for each individual, but may have included information such as your name and Social Security Number.

What We Are Doing: As soon as we discovered the incident, we took the steps described above. We also performed a thorough review of our systems to investigate the incident and ensure that our systems remain secure. We also implemented additional security measures to protect our digital environment and minimize the likelihood of future incidents.

In addition, to help protect your information, we are offering complimentary access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau 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.

What You Can Do: You can review the guidance included with this letter about how to protect your information. You can also contact our call center with any questions and to enroll in the free services please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted please provide the following multi code to receive services: [REDACTED]. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter.

000010102G0400

P

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.

For More Information: If you have any questions about this letter, please contact our dedicated call center for this incident at 1-833-799-3898 toll-free Monday through Friday from 8 am - 8 pm Eastern time (excluding major U.S. holidays).

Please accept our sincere apologies for any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read 'Tim Peltz', with a stylized flourish at the end.

Tim Peltz, Chief Information Officer
Racine Unified School District
3109 Mt. Pleasant St.
Racine, WI 53404

Additional Steps You Can Take to Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov
877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
www.marylandattorneygeneral.gov/Pages/
CPD
888-743-0023

Oregon Attorney General
1162 Court St., NE
Salem, OR 97301
www.doj.state.or.us/consumer-protect
ion
877-877-9392



California Attorney General

1300 I Street
Sacramento, CA 95814
www.oag.ca.gov/privacy
800-952-5225

New York Attorney General

The Capitol
Albany, NY 12224
800-771-7755
ag.ny.gov

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
www.riag.ri.gov
401-274-4400

Iowa Attorney General

1305 E. Walnut Street
Des Moines, Iowa 50319
www.iowaattorneygeneral.gov
888-777-4590

NY Bureau of Internet and Technology

28 Liberty Street
New York, NY 10005
www.dos.ny.gov/consumerprotection/
212.416.8433

Washington D.C. Attorney General

400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov/consumer-protection
202-442-9828

Kentucky Attorney General

700 Capitol Avenue, Suite 118
Frankfort, Kentucky 40601
www.ag.ky.gov
502-696-5300

NC Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov/protectingconsumers/
877-566-7226

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit

www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.