THOMPSON HINE
ATLANTA CINCINNATI COLUMBUS LOS ANGELES NEW YORK
CHICAGO CLEVELAND DAYTON MINNEAPOLIS WASHINGTON, D.C.

September 3, 2025

VIA EMAIL

Department's Legal Division
P.O. Box 5757
Columbia, SC 29250
scdca@scconsumer.gov

Re: Cybersecurity Incident Notification

To whom it may concern:

This communication serves as notice, on behalf of our client, Cherokee County School District ("**CCSD**"), of a recent cybersecurity incident that affected South Carolina residents.

As background, CCSD is a public school district located at 141 Twin Lake Road Gaffney, South Carolina 29341, and CCSD provides pre-school, middle school, and high school educational services.

On or about March 13, 2025, CCSD discovered that a third party had gained unauthorized access to certain systems in its information technology environment. In response, CCSD immediately deployed security measures to contain and mitigate the issue, and retained a leading cybersecurity incident response team to accelerate its recovery efforts. Because of the security controls CCSD implemented prior to this incident, it was able to quickly resolve the issue and return to a normal state of operations without any significant disruptions. In addition, CCSD proactively notified the Federal Bureau of Investigation (FBI), and local law enforcement about this incident.

CCSD learned the unauthorized third party accessed portions of its environment that contained personal data concerning some students, staff, and parents/guardians of students. In turn, CCSD hired a third party to undertake an extensive and a comprehensive review of these files and records to identify whether they contained any personal data or other sensitive data. CCSD's third-party consultants recently completed its review, and identified that this information included the following categories of personal data: a person's name, Social Security number, driver's license number, passport number, financial account information, and certain health data.

On or about August 28, 2025, CCSD began notifying all individuals whose personal data may have been impacted by this incident, which included forty-six thousand, one hundred and nineteen 46,119 known South Carolina residents. The aforementioned notifications were in substantially the same form and manner as the attachment hereto (See Enclosure). CCSD has offered all individuals impacted by this incident **complimentary, multi-year credit monitoring services** through TransUnion, and has further established a dedicated call center to answer any questions that individuals may have about this incident.

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

Sincerely,

/s/ *Steven G. Stransky*, Partner
Thompson Hine LLP
127 Public Square # 3900
Cleveland, OH 44114

Enclosure: Data Incident Notice Template (Example)

Cherokee County School District
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

Cherokee County School District
141 Twin Lake Road
Gaffney, SC 29341

P
[redacted]

August 28, 2025

Re: Notification of Privacy Incident

Dear [redacted]

As you may recall, Cherokee County School District ("**CCSD**" or "**we**") reported that it faced a cybersecurity incident in the Spring of 2025. We provided information about this incident to students, parents, and local media, and discussed it at our School Board Meetings. CCSD understands the importance of data privacy and is committed to protecting the confidentiality of personal data within our custody and control. This letter is to inform you that this cybersecurity incident involved some of your personal data.

We recognize that cybersecurity is a significant concern in today's world, and we know that many individuals have been impacted by other cybersecurity incidents that are completely unrelated to CCSD, such as cyberattacks impacting hospitals, banks, and other businesses (e.g., 2024 National Public Data breach). Accordingly, to help alleviate any concerns that you may have with respect to this or other cybersecurity incidents, we are providing you with **complimentary credit monitoring and identity theft protection services** (see below for enrollment information).

Why Does CCSD Have My Personal information?

CCSD is a public school district located in South Carolina, and we provide pre-school, middle school, and high school educational services. Accordingly, we collect personal information on our students, parents, guardians, emergency contacts, teachers, staff, and other administrative officials for a variety of reasons, such as compliance with student recordkeeping laws, health and safety concerns, financial aid and enrollment purposes, and other business-related purposes.

What Happened?

In March 2025, CCSD discovered that a third party had gained unauthorized access to certain systems in our information technology ("**IT**") environment. In response, we immediately deployed security measures to contain and mitigate the issue, and we retained a leading cybersecurity incident response team to accelerate our recovery efforts. Because of the security controls we implemented prior to this incident, we were able to quickly resolve the issue and return to a normal state of operations without any significant disruptions. As part of our investigation into this cybersecurity incident, we discovered that an unauthorized third party accessed files and records in our custody and control. In turn, we hired a third party to undertake an extensive and a comprehensive review of these files and records to identify whether they contained any personal information or other sensitive data. Our third-party consultants recently finished this review, and we learned that your personal information was affected by this incident.

What Personal Information Was Involved?

As noted above, we retained outside consultants and advisors to undertake an extensive and comprehensive review of the CCSD files and records that were impacted by this cybersecurity incident and discovered they contained personal information.

The data accessed potentially contained the following personal information about you: name, Social Security number, driver's license number, passport number, financial account information, and certain health data. As noted above, CCSD was retaining a copy of this personal data for school administration and legal compliance purposes.

What We Are Doing / How We Responded

Please know that CCSD acted swiftly to address this data privacy incident. We take this event and our information security obligations seriously, and we have taken action to remediate this cybersecurity incident and help prevent future occurrences. Specifically, after discovering the unauthorized access to our IT environment, we immediately made technical configuration changes to all accounts to prevent any further unauthorized access. We are also implementing certain types of privacy and security training so that we are better positioned to address information security and privacy threats and issues. We also retained independent third-party IT security consultants to analyze the incident, including our information security tools and the status of our data security hygiene.

Credit Monitoring Services

To help alleviate any concerns that you may have with respect to this or other cybersecurity incidents, we are providing you with access to **Triple Bureau Credit Monitoring/Triple Bureau Credit Report/Triple Bureau Credit Score** services at no charge. These services provide you with alerts for **24 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 through Identity Force, a TransUnion company specializing in fraud assistance and remediation services. To enroll in Credit Monitoring services at no charge, please log on to https://bfs.cyberscout.com/activate and follow the instructions provided. When prompted please provide the following unique 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. 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.

What You Can Do

There are additional steps that you can take to better protect yourself and your personal data more generally. Please see the Data Security Information Attachment for information on some of the resources available to you that may help address any data security-related concerns you may have.

Point of Contact / Call Center

We have established a dedicated call center to answer questions you may have about this incident. Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call the help line at 1-**833-426-8113** and supply the fraud specialist with your unique code listed above.

* * *

Sincerely,

Dr. Thomas White
Superintendent, Cherokee County School District

Data Security Information

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, call toll free at 1-877-322-8228 or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. 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, https://www.transunion.com, 1-800-916-8800.

When you receive your credit report: (i) review it carefully, (ii) look for accounts you did not open, (iii) look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security Number). You should also look in the "inquiries" section for names of creditors from whom you have not requested credit. You should notify the consumer reporting agencies immediately of any inaccuracies in your report or if you see anything you do not understand. The consumer reporting agency and staff will review your report with you. 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), http://www.ftc.gov/idtheft.

If you are a resident of the following states, you may contact and obtain information from your state Attorney General at the following:

- California Department of Justice, Office of Privacy Protection, PO Box 944255, Sacramento, CA 94244-2550, 1-800-952-5225, www.oag.ca.gov/privacy.
- New York Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov/.
- Office of the Attorney General Colorado Department of Law, Ralph L. Carr Judicial Building 1300 Broadway, 10th Floor Denver, CO 80203, 1-720-508-6000, https://complaints.coag.gov/s/contact-us.
- Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut St., Des Moines, IA 50319, 1-515-281-5164, https://www.iowaattorneygeneral.gov/.
- Office of the Illinois Attorney General, 500 South Second Street, Springfield, IL 62701, 1-217-782-1090, https://illinoisattorneygeneral.gov/Contact/.
- Kansas Attorney General's Office, 120 SW 10th, 4th Floor, Topeka, KS 66612, 1-785-296-3751, 1-888-428-8436.
- Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202, www.marylandattorneygeneral.gov, 1-888-743-0023 or 1-410-576-6300.
- Office of the Texas Attorney General, PO Box 12548, Austin, TX 78711-2548, 1-512-463-2100, https://www.texasattorneygeneral.gov/contact-us.
- North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699, https://ncdoj.gov/,
- 1-919-716-6400 or 1-877-566-7226.
- Wisconsin Attorney General's Office, PO Box 7857, Madison, WI 53707-7857, 1-608-266-1221, https://www.doj.state.wi.us/ag/contact.

West Virginia. If you are a resident of West Virginia, you have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described below. You also have a right to place a security freeze on your credit report, as described below.

Fraud Alerts: There are two types of 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 at least 90 days. 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. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Credit Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, 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 security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit. 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 listed above.

To request a security freeze, you will need to provide the following information: (i) Your full name (including middle initial as well as Jr., Sr., II, III, etc.), (ii) Social Security number, (iii) Date of birth, (iv) If you have moved in the past five years, provide the addresses where you have lived over the prior five years, (v) Proof of current address such as a current utility bill or telephone bill, (vi) A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.), and (vii) If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze. To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time. To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze. The credit bureaus have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.

Fair Credit Reporting Act: You also have rights under the federal Fair Credit Reporting Act (the "FCRA"), which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The Federal Trade Commission has published a list of the primary rights created by the FCRA, and the article is available at (https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf), and that article refers individuals seeking more information to visit www.ftc.gov/credit. The Federal Trade Commission's list of FCRA rights includes the following:

You have the right to receive a copy of your credit report. The copy of your report must contain all the information in your file at the time of your request. Each of the nationwide credit reporting companies - Equifax, Experian, and TransUnion - is required to provide you with a free copy of your credit report, at your request, once every 12 months. You are also entitled to a free report if a company takes adverse action against you, like denying your application for credit, insurance, or employment, and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You are also entitled to one free report a year if you are unemployed and plan to look for a job within 60 days, if you are on welfare, or if your report is inaccurate because of fraud, including identity theft. You have the right to ask for a credit score. You have the right to dispute incomplete or inaccurate information. Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information. Consumer reporting agencies may not report outdated negative information. Access to your file is limited. You must give your consent for reports to be provided to employers. You may limit "prescreened" offers of credit and insurance you receive based on information in your credit report. You may seek damages from violators. Identity theft victims and active-duty military personnel have additional rights.

P 0000103030000