Clark Hill

Melissa K. Ventrone
T (312) 360-2506
F (312) 517-7572
Email:mventrone@ClarkHill.com

Clark Hill
130 E. Randolph Street, Suite 3900
Chicago, Illinois 60601
T (312) 985-5900
F (312) 985-5999

August 31, 2026

VIA EMAIL

Office of the Attorney General
Hoover Building
1305 E Walnut St
Des Moines, IA 50319
databreach@ag.iowa.gov

Dear Attorney General Bird:

We represent Maryville Academy ("Maryville") with respect to a data security incident involving personal information described below. Maryville is a Covered Entity as defined under the Health Insurance Portability and Accountability Act ("HIPAA"). Maryville takes the security of the information in its control seriously and is committed to answering any questions you may have about the data security incident, its response, and steps taken to prevent a similar incident from occurring in the future.

1. Nature of security incident.

On July 15, 2024, Maryville discovered suspicious activity on their systems. Maryville implemented its incident response protocols and began an internal investigation. External cybersecurity specialists were engaged to help determine what occurred and whether any information was at risk. The investigation determined that some documents may have been impacted by the incident. While working to review the data, Maryville posted substitute notice on its website, and, to the extent possible, provided preliminary notice to certain potentially impacted individuals. Because it receives funding from government agencies, Maryville was required to manually review and segregate the data before further analysis could take place. This process could not be automated and took time to complete. Maryville then worked with a vendor to review the documents to identify and extract any personal information. This review concluded on June 29, 2026, at which point Maryville learned the following information may have been affected: date of birth, Social Security number, health and/or medical information, financial account number and routing number.

2. Number of residents affected.

Fifteen (15) Iowa residents were notified of the incident. A notification letter was sent to potentially affected individuals on August 31, 2026. A copy of the template notification letter is enclosed as Exhibit A.

3. Steps taken in response to the incident.

Since the incident, Maryville has deployed enhanced endpoint monitoring software, performed a global password reset, and implemented additional security controls. Maryville posted substitute notice of the data security incident on its website on September 13, 2024. In addition, potentially affected individuals were offered 12 months of credit monitoring and identity protection services through Cyberscout at no cost to them.

4. Contact Information

Maryville takes the security of the information in its control seriously and is committed to ensuring it is appropriately protected. If you have any questions or need additional information, please do not hesitate to contact me at mventrone@clarkhill.com or (312) 360-2506.

Sincerely,

CLARK HILL

Melissa K. Ventrone
Member

cc: Hannah Donahue – hdonahue@clarkhill.com

Maryville Academy
c/o Cyberscout
P.O. Box 3826
Suwanee, GA 30024

Maryville
Caring for Children. Strengthening Families.

38 1 7145 **********AUTO**5-DIGIT 60019
[redacted]

August 31, 2026

Dear [redacted]:

Maryville Academy ("Maryville") is writing to let you know about a data security incident that may have impacted your personal information. We take the privacy and security of your information seriously, and sincerely apologize for any concern or inconvenience this may cause you. This letter contains information about steps you can take to protect your information and resources we are making available to help you.

What happened?

On July 15, 2024, we discovered suspicious activity on our systems. As soon as we identified the suspicious activity, we implemented our incident response protocols and began an internal investigation. External cybersecurity specialists were hired to help us determine what had occurred, and whether any information was at risk. The investigation determined that some documents may have been impacted by the incident. Because we receive funding from government agencies, we were required to manually review and separate the data before further analysis could take place. This process could not be automated and took time to complete. We then worked with a vendor to review the documents, and on June 29, 2026, we learned your information may have been affected.

What information was impacted?

From our review, it appears your name and the following data elements may have been impacted: Social Security number.

What we are doing:

We want to assure you that we have taken steps to prevent this kind of event from happening in the future. Since the incident, we deployed enhanced endpoint monitoring software, changed passwords, and implemented additional security controls.

We are also providing you with 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. 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:

It is always a good idea to remain vigilant for incidents of identity theft or fraud, and to regularly review your bank account and other financial statements as well as your credit reports for suspicious activity. We also encourage you to contact Cyberscout with any questions and to take full advantage of the Cyberscout service being offered. Additional information about protecting your identity is included in this letter, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

How do I enroll for the free 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.

For more information:

If you have any questions or concerns, please email myquestions@maryvilleacademy.org or call 1-877-291-7597 Monday through Friday from 8:00 am to 8:00 pm Eastern Standard time. Your trust is our top priority, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,

Sister Catherine M. Ryan
Executive Director
Maryville Academy

RECOMMENDED STEPS TO HELP PROTECT YOUR INFORMATION

You've been provided with access to the following services from Cyberscout:

1. Single Bureau Credit Monitoring. You will receive alerts when there are changes to your credit data-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 Cyberscout fraud specialist, who can help you determine if it's an indicator of identity theft.

2. Fraud Consultation. You have unlimited access to consultation with a Cyberscout 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.

3. Identity Theft Restoration. If you become a victim of identity theft, an experienced Cyberscout 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 can dig deep to uncover the scope of the identity theft, and then work to resolve it.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-800-680-7289
P.O. Box 105069	P.O. Box 2000
Atlanta, GA 30348-5069	Chester, PA 19022-2000
www.equifax.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

District of Columbia: Office of the Attorney General, 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov.

Maryland Residents: Office of the Attorney General of Maryland**,** Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202**,** www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the 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 credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201904_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. 0 Rhode Island residents were notified of this incident. You have the right to obtain any police report filed in regard to this incident.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft