

Buffalo
New York
Chicago
Washington D.C.



www.octillolaw.com

May 8, 2024

VIA EMAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Email: Idtheft@oag.state.md.us

Dear Sir or Madam:

On behalf of Marist College, and pursuant to the Personal Information Protection Act ("PIPA"), Md. CodeAnn. Comm. Law 14-3504, this letter provides notice of a recent data security incident. By providing this notice, Marist College does not waive any rights or defenses regarding the applicability of Maryland law, including the applicability of the Maryland data notification laws or personal jurisdiction.

On or about December 11, 2023, Marist College detected suspicious activity related to a phishing campaign. Marist College immediately began an investigation and took steps to contain and remediate the situation, including by changing passwords, implementing additional technical safeguards on top of existing protections, and engaging data security and privacy professionals to assist in the investigation and response. With further investigation, Marist College confirmed that unauthorized actors accessed a limited number of Marist College email accounts, which may have included personal information, from December 9, 2023 through December 11, 2023. At this time, Marist College has implemented measures to further secure its email environment, including blocking additional suspicious mail domains and associated websites and setting alerts to monitor potentially affected email accounts. There is currently no evidence that any information has been misused for identity theft or fraud in connection with the incident.

Marist College has identified one (1) Maryland resident who may have been affected by the security incident. The information identified as the subject of the incident includes: name, address, and health information. Attached for your convenience is a copy of the template notification that was sent to the impacted Maryland resident on May 8, 2024.

Office of the Attorney General

May 8, 2024

Page 2

Please feel free to contact me with any questions at 716-898-2102 or dgreene@octillolaw.com.

Sincerely,

OCTILLO

A handwritten signature in black ink, appearing to read 'D. Greene', with a stylized flourish extending to the right.

Daniel P. Greene, Esq.

Certified Information Privacy Professional, United States (CIPP/US)

Certified Information Privacy Professional, Europe (CIPP/E)

Encl.

MARIST

May 8, 2024

VIA U.S. MAIL

[NAME]
[ADDRESS]
[CITY, STATE, ZIP]

Dear [NAME],

We are writing to inform you that Marist College (“Marist College” or “we”) experienced a data incident detected on December 11, 2023 (the “Incident”) that potentially involved your personal information (“Information”). This letter provides you with information about this Incident, our response, steps you can take, and if necessary, information on where to direct your questions. Additionally, although we are unaware of any misuse of your Information or fraud in relation to the Incident, as a precaution we have also provided steps you can take to protect your Information.

What Happened?

On or about December 11, 2023, Marist College detected suspicious activity related to a phishing campaign. We immediately began an investigation and took steps to contain and remediate the situation, including by changing passwords, implementing additional technical safeguards on top of our existing protections, and engaging data security and privacy professionals to assist our investigation and response.

With further investigation, we confirmed that unauthorized actors accessed a limited number of Marist College email accounts, which may have included your Information, from December 9, 2023 through December 11, 2023. There is currently no evidence that any Information has been misused for identity theft or fraud in connection with the Incident.

What Information Was Involved?

We determined that the following types of Information may have been impacted as a result of this Incident: [VARIABLE TEXT].

What We Are Doing.

Upon discovering the Incident, we immediately implemented measures to improve the security of our systems, including blocking additional suspicious mail domains and associated websites as well as setting alerts to monitor potentially affected email accounts. We have been working diligently to continue our investigation, add further technical safeguards to our existing protections, and secure our email environment. We continue to work with leading privacy and security professionals to aid in our investigation and response, and we are reporting this Incident to relevant government agencies.

What Can You Do?

Out of an abundance of caution, Marist College encourages individuals to remain vigilant against incidents of identity theft and fraud, to review account statements and explanation of benefits forms, and to monitor free credit reports for suspicious activity and to detect errors. Under U.S. law, individuals are entitled to one (1) free credit report annually from each of the three (3) major credit reporting bureaus. Please also review the “Additional Resources” section included with this letter, which outlines other resources you can utilize to protect your Information.

For More Information.

We take this Incident and the security of information in our care seriously. If you have further questions or concerns or would like more insight into the data about you that was potentially impacted, please call (845) 575-3446 Monday through Friday from 9 am – 5 pm Eastern.

Sincerely,



Michael Caputo, MS
VP of Information Technology & CIO
Marist College

Encl.

ADDITIONAL RESOURCES

Contact information for the three (3) nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every twelve (12) months from each of the three (3) nationwide credit reporting agencies.

To order your annual free credit report please visit www.annualcreditreport.com or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Georgia, Maryland, Massachusetts, New Jersey, and Vermont residents: You may obtain one (1) or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by calling one (1) of the three (3) nationwide credit reporting agencies above. 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.

Security Freeze. You may obtain a security freeze on your credit report, free of charge, to protect your privacy and confirm that credit is not granted in your name without your knowledge. You may also submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report, free of charge, or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place.

To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three (3) credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for them as well): (1) full name, with middle initial, and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. 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 home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

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

For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For Maryland Residents: You may obtain information about steps you can take to avoid identity theft from the Federal Trade Commission (contact information above) and the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.marylandattorneygeneral.gov, 1-888-743-0023.

For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html.

For New York Residents: You may obtain information regarding security breach response and identity theft prevention and protection information from the Federal Trade Commission (contact information above) and the New York Office of the Attorney General, Office of the Attorney General, The Capitol, Albany, NY 12224-0341, <https://ag.ny.gov>, 1-800-771-7755.

For Pennsylvania Residents: You may contact the Pennsylvania Office of the Attorney General, Bureau of Consumer Protection, 15th Floor, Strawberry Square, Harrisburg, PA 17120, www.attorneygeneral.gov, 1-800-441-2555.

Reporting of identity theft and obtaining a police report. You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

For Massachusetts Residents: You have the right to obtain a police report if you are a victim of identity theft.