

September 15, 2023

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 Skidmore College (“Skidmore”), 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, Skidmore 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 February 17, 2023, Skidmore received an alert of suspicious activity in its systems and immediately began an investigation and took steps to contain and remediate the situation. This included changing passwords, implementing new threat detection and monitoring software, notifying law enforcement, and engaging outside cybersecurity professionals and data privacy counsel to assist.

The investigation found that an unauthorized actor gained access to the Skidmore network before deploying ransomware that encrypted a small percentage of its faculty and staff files sharing system. The investigation discovered that some business and finance files were at risk of exfiltration by the unauthorized actor. Accordingly, Skidmore engaged a third-party data mining team to perform a thorough review of the relevant data set for the presence of personal information. Skidmore then conducted a manual review of the data mining results to confirm identities of the individuals whose information was potentially involved and gather contact information, where available, in order to complete the review and notify individuals and appropriate regulators. There is currently no evidence that any information has been misused for identity theft or fraud in connection with this incident.

Skidmore determined that the incident involved the personal information of 177 Maryland residents. While specific personal information varies by individual the categories of information included for the individuals of Maryland are name, Social Security number, health insurance application and claims information and credit/debit card number without password or security code. Individual notice to these residents is being provided today, September 15, 2023, which

Office of the Attorney General

September 15, 2023

Page 2

includes an offer for twenty-four (24) months of cost-free credit monitoring. A copy of the letter being mailed to potentially affected residents is enclosed.

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

Sincerely,
OCTILLO

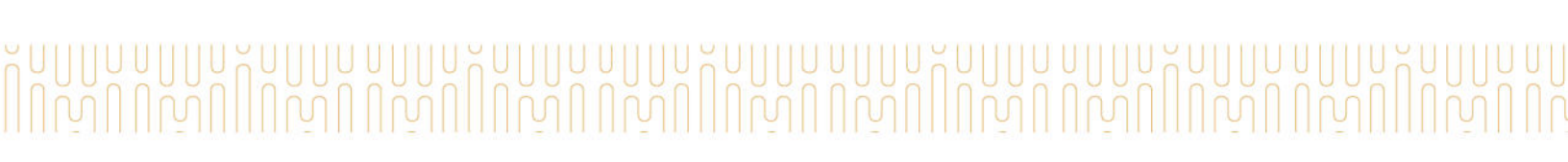
A handwritten signature in black ink, appearing to read 'D. Greene', with a stylized flourish extending to the right.

Daniel P. Greene, Esq.

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

Certified Information Privacy Professional, Europe (CIPP/E)

Encl.



SKIDMORE

C O L L E G E

Return mail will be processed by: IBC
PO Box 847 • Holbrook, NY 11741

September 15, 2023

Dear [REDACTED]:

I am writing to inform you that we, Skidmore College (“Skidmore” or “we”) recently experienced a data incident (“incident”) which potentially involved your personal information (“Information”). This letter provides you with information about this incident, what information was involved and what you can do, if you choose, in response. Additionally, although we are unaware of any misuse of your Information or fraud in relation to the incident, as a precaution we also provide steps you can take to protect your Information.

What Happened?

On February 17, 2023, Skidmore received an alert of suspicious activity in its systems and immediately began an investigation and took steps to contain and remediate the situation. This included changing passwords, implementing new threat detection and monitoring software, notifying law enforcement, and engaging outside cybersecurity professionals and data privacy counsel to assist.

The investigation found that an unauthorized actor gained access to the Skidmore network before deploying ransomware that encrypted a small percentage of its faculty and staff files sharing system. The investigation discovered that some business and finance files were at risk of exfiltration by the unauthorized actor. Accordingly, Skidmore engaged a third-party data mining team to perform a thorough review of the relevant data set for the presence of personal information. We then conducted a manual review of the data mining results to confirm the identities of the individuals whose information was potentially involved and gather contact information, where available, in order to send this notification. 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: [REDACTED]

What We Are Doing.

Upon becoming aware of the incident, we immediately implemented measures to further improve the security of our systems and practices. We worked with leading data privacy and security professionals to aid in our investigation and response and have reported this incident to relevant government agencies and federal law enforcement. We also implemented additional security protocols designed to protect our network, email environment, and systems.

What Can You Do?

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for twenty-four (24) months. While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary twenty-four (24) month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- You must **enroll by 12/7/2023** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>.
- Provide your **activation code**: [REDACTED]

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at [REDACTED] by 12/7/2023. Be prepared to provide engagement number B103893 as proof of eligibility for the Identity Restoration services by Experian.

While credit monitoring services are available to you at no cost for twenty-four (24) months, it is always recommended that you remain vigilant, regularly monitor free credit reports and review account statements, and that you report any suspicious activity to financial institutions. 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 any questions about the incident, please call [REDACTED], Monday through Friday, from 9:00 a.m. to 7:00 p.m. Eastern.

Sincerely,



Dwane Sterling
Chief Technology Officer
Skidmore College

ADDITIONAL RESOURCES

Contact information for the three 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 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 Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one 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 of the three 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 ensure 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 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 him/her 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.

For New Mexico Residents: You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may 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 or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

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 Alabama Residents: You may contact the Attorney General's Office for the State of Alabama, Consumer Protection Division, 501 Washington Avenue, Montgomery, AL 36104, www.oag.state.md.us, 1-800-392-5658.

For District of Columbia Residents: You may contact the District of Columbia Office of the Attorney General, 400 6th Street NW, Washington, D.C. 20001, consumer.protection@dc.gov, (202) 442-9828.

For Illinois Residents: You may contact the Illinois Office of the Attorney General, 100 West Randolph Street, Chicago, IL 60601, https://illinoisattorneygeneral.gov/about/email_ag.jsp, 1-800-964-3013.

For Iowa Residents: You may contact the Iowa Office of the Attorney General, 1305 E. Walnut Street, Des Moines IA 50319, consumer@ag.iowa.gov, 1-888-777-4590.

For Kansas Residents: You may contact the Kansas Office of the Attorney General, Consumer Protection Division, 120 SW 10th Ave, 2nd Floor, Topeka, KS 66612-1597, <https://ag.ks.gov/>, 1-800-432-2310.

For Kentucky Residents: You may contact the Kentucky Office of the Attorney General, Consumer Protection Division, 1024 Capital Center Drive, Suite 200, Frankfort, Kentucky 40601, www.ag.ky.gov, 1-800-804-7556.

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

For Minnesota Residents: You may contact the Minnesota Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For Missouri Residents: You may contact the Missouri Office of the Attorney General, Consumer Protection, 207 W. High St., P.O. Box 899, Jefferson City, MO 65102, www.ago.mo.gov, 1-800-392-8222.

For New Mexico Residents: You may contact the New Mexico Office of the Attorney General, Consumer Protection Division, 408 Galisteo Street, Villagra Building, Santa Fe, NM 87501, www.nmag.gov, 1-844-255-9210.

For New York Residents: You may contact 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 North Carolina Residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Main Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7266.

For Rhode Island Residents: You may contact the Rhode Island Office of the Attorney General, Consumer Protection Division, 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 1-401-274-4400.

For Texas Residents: You may contact the Texas Office of the Attorney General, Office of the Attorney General, PO Box 12548, Austin, TX 78711-2548, www.texasattorneygeneral.gov, 1-800-621-0508.

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 Iowa Residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

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

For North Carolina Residents: You are advised to report any suspected identity theft to law enforcement or to the North Carolina Attorney General.

For Oregon Residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

For Rhode Island Residents: Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.