Appendix

On September 10, 2021, Smith College ("Smith") concluded its investigation of a phishing email incident that resulted in unauthorized access to an email account used by the Smith College Office of Student Financial Services. Upon first suspecting unauthorized access to the email account, Smith immediately secured the account, launched an investigation, and notified law enforcement.

Through its investigation, Smith determined that an unauthorized party gained access to the email account between the dates of July 27, 2021 and August 4, 2021. Smith reviewed the emails and attachments contained in the email mailbox to identify individuals whose information may have been viewed by the unauthorized party. Through this review, Smith identified an email in the account containing the name and banking information (bank account and routing numbers) of one Maine resident.

On September 17, 2021, Smith is providing written notice via United States Postal Service First Class mail to the Maine resident whose personal information was potentially accessed by the unauthorized party.[1] Smith encouraged the individual to remain vigilant for fraud by monitoring her credit reports and financial account statements. Smith also provided the individual with a phone number that she can call to obtain more information regarding the incident.

To help prevent a similar incident from occurring in the future, Smith implemented multi-factor authentication for remote access to the email account involved in this incident and is providing additional training to its faculty and staff concerning cybersecurity best practices.

[1] This notice does not waive Smith's objection that Maine lacks personal jurisdiction over it regarding any claims related to this incident.

SMITH COLLEGE

Office of Enrollment
Smith College
Northampton, Massachusetts 01063
T (413) 585-4900
F (413) 585-4917

September 17, 2021

Eva Goldfinger
18 Howard Street
Portland, ME 04101

Dear Eva:

Smith College is committed to protecting the privacy and security of the information we maintain. We are writing to inform you about a data security incident that may have involved some of your information. This notice explains the incident, measures we have taken, and some steps you can take in response.

On September 10, 2021, Smith concluded its investigation of a phishing email incident that resulted in unauthorized access to an email account used by the Smith College Office of Student Financial Services. Upon first suspecting unauthorized access to the email account, we immediately secured the account, launched an investigation, and notified law enforcement.

Through our investigation, we determined that an unauthorized party gained access to the email account between the dates of July 27, 2021 and August 4, 2021. We then reviewed the emails and attachments contained in the email mailbox to identify individuals whose information may have been viewed by the unauthorized party. Through this review, we identified an email in the account containing your name and banking information (bank account and routing numbers).

We encourage you to remain vigilant by regularly reviewing your credit reports and financial account statements for any unauthorized activity. If you see charges or activity you did not authorize, please contact the relevant financial institution immediately.

We regret any concern this incident may cause you. To help prevent a similar incident from occurring in the future, we have implemented multi-factor authentication for remote access to the email account involved in this incident and are providing additional training to our faculty and staff on cybersecurity best practices. If you have any questions, please contact David Belanger, Director of Student Financial Services at 413-585-2530 or dbelange@smith.edu.

Sincerely,

Joanna May
Vice President for Enrollment

ADDITIONAL STEPS YOU CAN TAKE

We remind you 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 or call toll free at 1-877-322-8228. 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, www.transunion.com, 1-800-916-8800

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), www.ftc.gov/idtheft

Fraud Alerts: There are two types of general 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 one year. 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.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? 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 below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

You may contact Smith College via U.S. mail at 10 Elm Street, Northampton, Massachusetts 01063 or via telephone at 413-584-2700.