COLLEGE OF THE Holy Cross | Information Technology Services

Attorney General Joseph Foster
Office of the Attorney General
33 Capitol Street
Concord, New Hampshire 03301

Dear Attorney General Foster:

We are writing to notify you of unauthorized access of personal information involving up to 1 New Hampshire resident.

NATURE OF THE SECURITY BREACH OR UNAUTHORIZED USE OR ACCESS

On September 22nd, 2017, a College employee accidentally cross-mailed promissory notes of at least 4, and as many as 28 College alumni via the United States Postal Service (1 of those being a resident of New Hampshire). The mistake was caused by the mis-stuffing of envelopes. Due to the age of the promissory notes, they contained the names and Social Security numbers, and in some cases, Drivers License numbers of the individuals. Given the nature of the incident, we are not certain if all 28 individuals are affected, or just the 4 that we have confirmed. As a result, we are mailing all 28 potentially affected individuals.

NUMBER OF NEW HAMPSHIRE RESIDENTS AFFECTED

1 New Hampshire residents is potentially affected, and a notification has been sent to them via the United States Postal Service (a copy of that notice is attached).

STEPS YOU HAVE TAKEN OR PLAN TO TAKE RELATING TO THE INCIDENT

We have sent notification letters to the potentially affected individuals including one year of complimentary identity theft protection services. Those who we know for certain were affected have been telephoned and/or emailed. We do not believe any sort of fraud will arise, given that the recipients are all College alumni, but to be cautious, we have obtained identity theft protection services to offer the individuals affected. Going forward, the College's Bursar's Office will no longer be mailing paid-in-full promissory notes to alumni, and will instead have a third party mail a paid-in-full notice to former students. We are also undergoing an evaluation of business processes to identify if any further changes are required in order to avoid similar, future incidents.

You may contact myself, David Shettler, Information Security Officer with any questions.

David Shettler
Information Security Officer
College of the Holy Cross
Information Technology Services
1 College Street
Worcester, MA 01610
508-793-3073
dshettle@holycross.edu

COLLEGE OF THE
Holy Cross | Office of the Bursar

«AddressBlock»

October 18th, 2017

«GreetingLine»

I am writing on behalf of the College of the Holy Cross to inform you of a recent privacy incident concerning your personal information. On September 22, 2017, a College employee may have accidentally cross-mailed your promissory note with that of another alumni. The promissory note would have contained your name, Social Security Number, and potentially your Driver's License number.

We have no reason to believe that your information will be misused as a result of this error. To be cautious, however, we have contracted with Identity Guard to offer you free identity theft protection services for a year. Details of how to sign-up for that service follow. Please see attachment B for additional steps you can take to protect your identity.

We take our stewardship over your personal information very seriously, and implement numerous technical safeguards and staff training programs to prevent these issues from happening. We are adjusting our processes and training to minimize the chances of this happening in the future.

If you have any questions, please don't hesitate to contact me.

Sheila Coakley
Bursar
College of the Holy Cross
1 College Street
Worcester, MA 01610
508-793-2521

COLLEGE OF THE Holy Cross | Office of the Bursar

IDENTITY GUARD.

Bursar's Office
College of the Holy Cross
1 College Street
Worcester, MA 01610

NAME/ADDRESS

Dear FIRSTNAME,

COMPLIMENTARY SERVICE OFFER: At our expense, the College of the Holy Cross would like to offer you a free 1 year subscription to Identity Guard® Essentials, an identity theft protection service. Identity Guard provides monitoring and protection and also alerts you of certain activities that could indicate potential identity theft. This program is provided by Intersections Inc. (NASDAQ: INTX), a leading provider of consumer and corporate identity risk management services.

Identity Guard® Essentials features include:

- Social Security Number Monitoring
- Online "Black Market" Monitoring
- Account Takeover Alerts
- $1 Million Identity Theft Insurance*
- Lost Wallet Protection
- ID Verification™ Alerts
- ID Theft Victim Assistance
- ID Vault® Password Protection

If you wish to take advantage of this monitoring service, you must enroll by January 15th, 2018.

ENROLLMENT PROCEDURE: To activate this coverage please visit the Web site listed below and enter the redemption code. The redemption code is required for enrollment, and can only be used one time by the individual addressed.

1. Website: www.identityguard.com/enroll
2. Redemption Code: CODE and click "Submit"
3. Complete the Identity Guard Essentials enrollment form. To see additional product features, click "Service Details."

In order to enroll, you will need to provide the following personal information:

- Mailing Address
- Phone Number
- Social Security Number
- Date of Birth
- E-mail Address
- Redemption Code

This service is complimentary; no method of payment will be collected during enrollment and there is no need to cancel. We apologize for any inconvenience and urge you to enroll today. If you have any further questions regarding this incident, please call Sheila Coakley, Bursar at 508-793-2521 Monday through Friday, 8am to 5pm EST.

Sincerely,

Sheila Coakley
Bursar
College of the Holy Cross
508-793-2521
scoakley@holycross.edu

*Identity Theft Insurance underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Attachment B

We want to advise you of several other resources that are available to help you protect your personal information and suggest you monitor your accounts for suspicious activity.

1. Free Credit Report

You are entitled to receive your credit report from each of the three national credit reporting agencies once per year, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain your free annual credit report from each of the national credit reporting agencies by visiting www.annualcreditreport.com, by calling 877-322-8228 or by mailing your request to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

When you receive your credit report(s), please review them carefully. Look for any accounts you did not open, requests for your credit report from anyone that you did not apply for credit with, or inaccuracies regarding your personal identifying information, such as your home address or social security number. If you see anything you do not understand or that is incorrect, contact the appropriate credit reporting agency using the contact information on the credit report or listed below and ask them to have information relating to fraudulent transactions deleted:

Equifax P.O. Box 740256 Atlanta, GA 30374 www.equifax.com 800-525-6285	Experian P.O. Box 9554 Allen, TX 75013 www.experian.com 888-397-3742	TransUnion P.O. Box 6790 Fullerton, CA 92834 www.transunion.com 800-680-7289

Additionally, you can obtain information from the Federal Trade Commission about taking steps to avoid identity theft at: www.ftc.gov/bcp/edulmicrosites/idtheft.

2. Flagging Your Credit Report

To further protect you from the possibility of identity theft, each of the national credit reporting agencies provides the ability to place a fraud alert or security freeze on your credit files. A fraud alert notifies any creditors that access your credit report that you may be the victim of fraud and encourages them to take additional steps to protect you from fraud. Placing a fraud alert is as simple as calling the numbers above for each or any of the credit reporting agencies and requesting that a fraud alert be placed on your credit file.

Whether or not you find any signs of fraud on your credit reports, we recommend that you closely monitor your banking and credit account statements for suspicious activity on your existing accounts. You should

also remain vigilant over the next two years by attentively monitoring your credit reports and account statements for indications of fraud and/or theft, including identity theft.

3. Security Freeze

You are also permitted to place a "security freeze" on your credit file. A security freeze is different from a fraud alert. When you place a security freeze on your credit file, third parties, such as lenders or other companies (unless exempt under law), will not be able to access your credit report without your express consent. A security freeze may delay, interfere with or prohibit the timely approval of any subsequent request or application you make that involves access to your credit report. This may include, but is not limited to, new loans, credit, mortgages, insurance, rental housing, employment, investments, licenses, mobile phone service, utility service, digital signature service, internet credit card transactions and extension of credit at a retail point of sale. Additionally, while your report is frozen, companies that provide consumer data to credit reporting agencies will not be allowed to update name, address, social security number and date of birth information on your credit report. If you wish to apply for a new credit account or other credit relationship, and the prospective lender or company needs to access your credit report, you will need to either remove or temporarily lift the security freeze unless the situation is one of those exempt from security freezes as defmed by law. To submit a security freeze, you must submit a written request to each of the credit reporting agencies, including your full name (with middle initial and generation, such as Jr., III, etc.), address, social security number, date of birth (month, day, year) any required fee and proof of your current residence, such as a state issued identification card or driver's license, to the addresses below:

Experian Security Freeze P.O. Box 9554 Allen, TX 75013 888-397-3742 www.experian.com/freeze	Equifax Security Freeze P.O. Box 105788 Atlanta, Georgia 30348 800-685-1111 www.freeze.equifax.com	TransUnion LLC P.O. Box 6790 Fullerton, CA 92834 888-909-8872 www.freeze.transunion.com

If, at any time, you fmd suspicious activity on your credit reports, please take these steps. First, call your local police department, sheriff s office or local attorney general's office and file a report. Be sure to obtain a copy of this report, as many creditors will require the information it contains to absolve you of any fraudulent debts and it also is helpful to the credit reporting agencies. Second, file a complaint with the FTC at www.ftccomplaintassist.gov or call 1-877-ID-THEFT (877-438-4338). Last, notify all of the national credit reporting agencies of the suspicious activity.