

May 16, 2019

Anjali C Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

Via email

Attorney General Gordon MacDonald
Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, New Hampshire 03302
DOJ-CPB@doj.nh.gov

Re: Data Security Incident

Dear Attorney General MacDonald:

We represent St. Francis College ("SFC"), located at 180 Remsen Street, Brooklyn Heights, New York, 11201 with respect to a potential data security incident described in more detail below. SFC takes the security and privacy of the information in its control very seriously, and has taken steps to prevent a similar incident from occurring in the future.

1. Nature of the security incident.

Between November 28, 2018 and December 11, 2018, SFC learned that two employees were victims of payroll fraud. SFC conducted an internal investigation and discovered evidence to suggest a small number of employees' email accounts were potentially accessed by an unauthorized individual. SFC immediately took action to secure the email accounts and conducted an investigation with the assistance of computer forensic professionals to identify any personal information that may have been accessed as a result of the incident. On April 23, 2019, the investigation concluded and the computer forensic professionals were able to identify specific current and former employees' and students' personal information that was potentially accessible to the unauthorized individual(s). The email accounts contained information including names, Social Security numbers, financial account numbers, passport numbers, driver's license numbers and/or health information.

2. Number of New Hampshire residents affected.

Six (6) New Hampshire residents are known to have been potentially affected by this incident. Notification letters to these individuals were mailed on May 16, 2019, by first class mail. A sample copy of the notification letter is included with this letter.

3. Steps taken.

SFC has taken steps to prevent a similar event from occurring in the future, and to protect the privacy and security of potentially affected individuals' information. This includes changing passwords, providing

55 West Monroe Street, Suite 3800 • Chicago, IL 60603 • p 312.704.0550 • f 312.704.1522

Albany • Atlanta • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston • Indiana • Kentucky
Las Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • New Jersey • New Orleans • New York • Orlando • Philadelphia • Phoenix • San Diego
San Francisco • Sarasota • Stamford • Virginia • Washington, DC • West Palm Beach • White Plains

wilsonelser.com

users with additional training on network security, and implementing multifactor authentication. SFC will also provide potentially affected individuals with identity theft restoration and credit monitoring services for a period of twelve (12) months at no cost to the individuals.

4. Contact information.

SFC remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Anjali.Das@wilsonelser.com or (312) 821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP


Anjali C. Das

Enclosure.



ST. FRANCIS COLLEGE

C/O ID Experts
PO Box 4219
Everett WA 98204

ENDORSE



2Decode
SEQ

NAME
ADDRESS1
ADDRESS2
CSZ
COUNTRY

BREAK

To Enroll, Please Call:

(800) 405-9710

Or Visit:

<https://ide.myidcare.com/stfrancis>

Enrollment Code: <<XXXXXXX>>

<<Date>>

Dear <<First Name>> <<Last Name>>:

We are writing to inform you of a data security incident involving St. Francis College that may have resulted in unauthorized access to some of your personal information, including your name and Social Security number. We take the privacy and protection of your personal information very seriously. We apologize and regret any inconvenience this may cause. This letter contains information about what happened, steps we have taken and resources we are making available to you to help protect your identity.

Between November 28, 2018 and December 11, 2018, we learned that two employees were victims of payroll fraud. We immediately engaged with our Information Technology team to determine if any of our systems had been accessed without authorization. During an internal investigation, we found evidence suggesting that a small number of employees' email accounts were accessed by an unauthorized individual. We immediately took action to secure the email accounts and conducted an investigation with the assistance of computer forensic professionals to identify any personal information that may have been accessible as a result of the incident. On April 23, 2019, after a full and thorough search of all the material accessible within the affected email accounts, we discovered that information including your name and one or more of the following personal attributes: address, Social Security number, financial account number and/or health information were accessible in the affected email accounts. Apart from the limited number of employees affected by the payroll fraud, we have no evidence of misuse of anyone's information as a consequence of this incident.

In an abundance of caution, we are offering identity theft protection services through ID Experts®, the data breach and recovery services expert, to provide you with MyIDCare™. MyIDCare services include: 12 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by going to <https://ide.myidcare.com/stfrancis> and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 8:00 a.m. – 8:00 p.m. Eastern Time. Please note that the deadline to enroll is August 16, 2019.

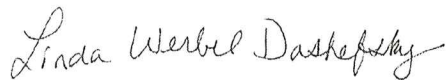
Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. MyIDCare representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

To receive credit services by mail instead of online, please call (800) 405-9710. Additional information describing your services is included with this letter.

We take the security of all information in our systems very seriously and want to assure you that we are taking steps to prevent a similar event from occurring in the future. Those steps include changing passwords, providing users with increased training on network security, implementing multi-factor authentication, and reporting the incident to government regulators.

We sincerely regret any inconvenience that this matter may cause you, and remain dedicated to protecting your information. Please see the addendum for additional steps you can take to protect your personal information. If you have any questions, please call (800) 405-9710 Monday through Friday, 8:00 a.m. to 8:00 p.m., Eastern Time.

Sincerely,

A handwritten signature in cursive script that reads "Linda Werbel Daskefsky".

Linda Werbel
Vice President of Government and Community Relations
St. Francis College



Recommended Steps to help Protect your Information

1. Website and Enrollment. Go to <https://ide.myidcare.com/stfrancis> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your MyIDCare membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.

3. Telephone. Contact MyIDCare at (800) 405-9710 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

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.

If you discover any suspicious items and have enrolled in MyIDCare, notify them immediately by calling or by logging into the MyIDCare website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

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.

Additional Important Information

For residents of Hawaii, Michigan, Missouri, Virginia, Vermont, and North Carolina: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia:

It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your 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 at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of Iowa:

State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon:

State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, and North Carolina:

You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

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

**Rhode Island Office of the
Attorney General**
Consumer Protection
150 South Main Street
Providence RI 02903
1-401-274-4400
www.riag.ri.gov

**North Carolina Office of the
Attorney General**
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.com

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Ave, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft

For residents of Massachusetts: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf), Experian (<https://www.experian.com/fraud/center.html>) or TransUnion (<https://www.transunion.com/fraud-victim-resource/place-fraud-alert>). 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. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, telephone or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, 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, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting each of the following national consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
www.freeze.equifax.com
800-525-6285

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze
888-397-3742

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022
freeze.transunion.com
800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.