JONES DAY

500 GRANT STREET, SUITE 4500 • PITTSBURGH, PENNSYLVANIA 15219.2514
TELEPHONE: +1.412.391.3939 • FACSIMILE: +1.412.394.7959

DIRECT NUMBER: (412) 394-7272
JKITCHEN@JONESDAY.COM

November 29, 2018

VIA U.S. MAIL

Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

To Whom It May Concern :

I am counsel for Franciscan University of Steubenville. I'm writing to provide notice of a data security incident, as described in the enclosed letter. Please contact me for any further information (412.394.7272, jkitchen@jonesday.com).

Sincerely,

James T. Kitchen

Enclosure

FRANCISCAN UNIVERSITY OF STEUBENVILLE

1235 University Boulevard
Steubenville, Ohio 43952-1763
www.franciscan.edu

Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

November 29, 2018

Notice of Data Security Incident

Office of the Attorney General:

I am writing to provide you notice of a data security incident at Franciscan University of Steubenville. The University discovered that an unauthorized third party compromised a limited number of University business email accounts in October 2018. In response, the University took immediate action to block further unauthorized access to University email accounts and determine what information may have been impacted with the assistance of outside experts. In addition, the University contacted the Federal Bureau of Investigation in order to provide notice of this incident and seek assistance.

Based on our investigation to date, we believe that there may have been unauthorized access to the names and Social Security numbers of nineteen residents in your state. We have seen no indication that any of the personal information was actually viewed by an unauthorized third party. Further, we have seen no indication that any of the personal information has been misused. However, out of an abundance of caution, we are notifying all of the potentially impacted residents in your state and providing each resident several resources, including 24 months of identity protection services. Those notices will be sent via U.S. mail on Friday, November 30, and an example of the notice is attached hereto.

We have already required our employees to change their passwords. Going forward, we will continue to make security enhancements to help prevent similar incidents from occurring in the future. Ongoing security analysis and testing of our network will be conducted, added levels of security will be configured within our software applications, and a thorough review of our ITS security policies and procedures will be conducted. A critical part of this plan will be the delivery of training programs for all of our faculty and staff to increase awareness.

The University takes information security very seriously and sincerely regrets any concern or inconvenience that this incident may have caused.

Sincerely,

Richard S. Rollino
Vice President of Finance

FRANCISCAN UNIVERSITY
OF STEUBENVILLE

1235 University Boulevard
Steubenville, Ohio 43952-1763
www.franciscan.edu

November 30, 2018

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Suffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

Notice of Data Security Incident

Dear <<MemberFirstName>> <<MemberLastName>>,

I am writing to make you aware of a data security incident at Franciscan University of Steubenville that may have involved your personal information, as described below. This letter explains the incident, measures the University has taken, and some actions you can take in response. The University takes information security very seriously and sincerely regrets any concern or inconvenience that this incident may cause you.

What Happened

The University discovered that an unauthorized third party compromised a limited number of University business email accounts in October, 2018. In response, the University took immediate action to block further unauthorized access to University email accounts and determine what information may have been impacted. In addition, the University contacted law enforcement in order to provide notice of this incident and seek assistance.

What Information Was Involved

Based on our investigation to date, we believe that there may have been unauthorized access to your <<ClientDef1 (name and [Personal Information])>>. We have seen no indication that any of your personal information was actually viewed by an unauthorized third party. Further, we have seen no indication that any of your personal information has been misused. However, out of an abundance of caution, we are notifying you of this incident and providing you resources (described below and in the attached "Additional Resources" page).

What We Are Doing

Upon learning of this incident, we took immediate action to secure any potentially impacted email accounts with the assistance of outside experts. We have required employees to change their passwords, and we will continue to make security enhancements to help prevent similar incidents from occurring in the future. Ongoing security analysis and testing of our network will be conducted, added levels of security will be configured within our software applications, and a thorough review of our ITS security policies and procedures will be conducted. A critical part of this plan will be the delivery of training programs for all of our faculty and staff to increase awareness. Law enforcement has also been notified. We are now notifying you so that you can take the steps recommended below.

What You Can Do

We recommend that you take steps to protect against identity theft or fraud. You can monitor your accounts and free credit reports for any signs of suspicious activity. You can also find information about how to obtain a free credit report, security freezes, and other guidance in the attached "Additional Resources" page, which we encourage you to review.

We are also offering you 24 months of identity monitoring services at no charge to you. The University has contracted a third-party service provider, Kroll, to provide these services to you, which include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. To take advantage of these services, you will need to activate them online at **<<IDMonitoringURL>>**. You have until <<Date>> to activate your identity monitoring services. Your Membership Number is: **<<Member ID>>**. If you have any questions about the services or would like to receive your credit

monitoring through the mail, please call Kroll at 1-???-???-????. Please note that to activate these services, you will need to provide your personal information to Kroll. Additional information about the services available from Kroll is enclosed.

As always, please be cautious of any unsolicited communications that ask you to provide your personal information electronically or over the telephone and avoid clicking on links or downloading attachments from suspicious emails.

If you have any questions or concerns, please call 1-???-???-????, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time.

Sincerely,

Richard S. Rollino
Vice President of Finance

ADDITIONAL RESOURCES

Credit Reports, Fraud Alerts, and Security Freezes

You may obtain a free copy of your credit report from each of the three credit reporting agencies by visiting www.annualcreditreport.com or by calling 1-877-322-8228. You can request information regarding fraud alerts, security freezes, and identity theft from the following credit reporting agencies:

- **Experian**, www.experian.com, 1-888-397-3742, P.O. Box 9554, Allen, TX 75013
- **TransUnion**, www.transunion.com, 1-888-909-8872, P.O. Box 2000, Chester, PA 19016-2000
- **Equifax**, www.equifax.com, 1-800-685-1111, P.O. Box 105788, Atlanta, GA 30348

You can contact these credit bureaus to place a "fraud alert" on your credit file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. When one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file.

A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies listed above. You will need to provide certain information:

- Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
- Social Security number
- Date of birth
- If you have moved in the past five years, provide the addresses where you have lived over the prior five years
- Proof of current address such as a current utility bill or telephone bill
- A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.)
- If you are a victim of identity theft, include a copy of either the police report, investigative report or complaint to a law enforcement agency concerning identity theft.
- If you are not a victim of identity theft, include payment by check, money order or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

You can also receive information from the Federal Trade Commission ("FTC") regarding fraud alerts, security freezes, your rights under the Fair Credit Reporting Act, and how to avoid and report identity theft:

FTC Identity Theft Clearinghouse, 600 Pennsylvania Avenue, NW, Washington, D.C. 20580, consumer.ftc.gov, 1-877-438-4338. Contact information for state Attorneys General is available at www.naag.org/current-attorneys-general.php.

Additional Information for Residents of Iowa, Maryland, North Carolina, Oregon, and Rhode Island

You can contact the FTC, local law enforcement, or your state attorney general to report suspected identity theft or request information on how to prevent it.

- **Iowa**: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, Iowa 50319-0106, www.iowaattorneygeneral.gov, 1-888-777-4590
- **Maryland**: Office of the Attorney General of Maryland, 200 St. Paul Place Baltimore, MD 21202, www.marylandattorneygeneral.gov, 1-888-743-0023
- **North Carolina**: Office of the Attorney General of North Carolina, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.com, 1-877-566-7226
- **Oregon**: Oregon Department of Justice, 1162 Court St. NE, Salem, OR 97301-4096, www.doj.state.or.us, 1-877-877-9392
- **Rhode Island**: Office of the Attorney General of Rhode Island, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, (401) 274-4400. In Rhode Island, you may file or obtain a police report.

Additional Information for Residents of Massachusetts

Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident.

If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. Massachusetts law also allows consumers to place a security freeze on their credit reports. If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift, or remove a security freeze. The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time. To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

INFORMATION ABOUT KROLL SERVICES

The University is offering you the following services[1] from Kroll at no charge to you:

Triple Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you can call a Kroll fraud specialist.

Fraud Consultation

You will have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.