

BakerHostetler

Baker&Hostetler LLP

811 Main Street
Suite 1100
Houston, TX 77002-6111

T 713.751.1600
F 713.751.1717
www.bakerlaw.com

William R. Daugherty
direct dial: 713.646.1321
wdaugherty@bakerlaw.com

September 13, 2019

VIA EMAIL (NDAG@ND.GOV)

Office of the Attorney General
State Capitol
600 E. Boulevard Ave., Dept. 125
Bismarck, ND 58505

Re: Incident Notification

Dear Sir or Madam:

We are writing on behalf of our client, Fellowship of Catholic University Students (“FOCUS”), to notify you of a security incident.

On January 16, 2019, FOCUS learned that an unauthorized individual attempted to redirect payroll funds of three employees (none of whom were North Dakota residents) by changing the direct deposit information in FOCUS’s human resources platform, Ceridian Dayforce. Upon learning this, FOCUS took immediate action to secure the affected employees’ accounts, contacted the affected employees, and launched an investigation to determine the nature and scope of the incident. Findings from the investigation indicated that an unauthorized individual gained access to a payroll administrator’s Dayforce account on January 13, 2019 and January 16, 2019. Although the investigation found no evidence of unauthorized access to other employees’ Dayforce accounts or tax forms, on February 28, 2019, it was determined that such possibility could not be ruled out because Ceridian advised that it did not have any additional logs showing what the unauthorized person accessed while in Dayforce. The personal information that may have been accessible included the information contained in an employee’s Dayforce account, including name, address, date of birth, employment details, bank account number, and Social Security number. On March 29, 2019, FOCUS notified certain current and former employees of FOCUS, including 35 residents of North Dakota, about the incident.¹

¹ Notification to the North Dakota Office of Attorney General was not made at that time because the number of North Dakota residents being notified was less than 250.

While investigating that incident, FOCUS learned that the unauthorized individual also accessed the email accounts of the payroll administrator and two former employees at various times from December 15, 2018 through January 16, 2019. The investigation was not able to determine which emails and attachments were viewed by the unauthorized individual. Therefore, FOCUS conducted a thorough review of the contents of the accessed accounts and determined that an email or an attachment to an email contained some personal information, including names, Social Security numbers, and dates of birth of 10 additional North Dakota residents. On May 22, 2019, FOCUS mailed notification letters via First Class Mail to the 10 additional North Dakota residents whose personal information was contained in the email accounts involved.

FOCUS subsequently learned that there was unauthorized accessed to two additional employee email accounts. FOCUS launched an investigation and conducted analysis of those additional two accessed accounts and determined that an unauthorized individual had access to the employees' email accounts at various times between November 9, 2018 and December 20, 2018. The investigation was not able to determine which emails and attachments were viewed by the unauthorized individual. Therefore, FOCUS conducted a thorough review of the contents of the accessed accounts and on July 13, 2019, determined that an email or an attachment to an e-mail contained the name and dates of birth for 464 North Dakota residents.

Today, FOCUS is sending notification letters via First Class Mail to 464 additional North Dakota residents whose personal information was contained in the email accounts involved. The total number of North Dakota residents notified about this incident is 509. This notice is being provided in accordance with N.D. Cent. Code § 51-30-02. Enclosed is a sample copy of the notification letter for each round of notifications. FOCUS is offering one year of complimentary credit monitoring and identity theft protection service through Experian to the individuals whose Social Security numbers were contained in the accessed accounts. FOCUS is also providing a call center for the individuals to call with questions regarding the incident.

To help prevent a similar incident in the future, FOCUS has implemented enhanced security measures in Dayforce and Office 365, including multi-factor authentication, and FOCUS will be providing additional phishing awareness training to employees.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,



William R. Daugherty
Partner

Enclosure



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Name 1>>:

Protecting the privacy and security of our employees' personal information is a top priority for Fellowship of Catholic University Students (FOCUS). We are writing to provide you with additional information about the incident we previously reported to you involving Ceridian Dayforce, the measures we have taken, and some steps you can take in response.

As we communicated previously, we recently learned that an unauthorized individual accessed Dayforce and attempted to redirect payroll funds of three employees. Upon learning this, we took immediate action to secure the affected employees' accounts, contacted the affected employees, and launched an investigation to determine the nature and full scope of the incident. Findings from our investigation indicate that an unauthorized individual gained access to a payroll administrator's Dayforce account on January 13, 2019 and January 16, 2019 and changed the direct deposit information for three employees. The investigation confirmed that there were no other changes to direct deposit accounts and that tax forms, such as Forms W-2 and 1095, were not accessed. Although our investigation found no evidence of unauthorized access to other employees' Dayforce accounts or information, our investigation was unable to rule out that possibility. So, it is possible that the unauthorized individual could have accessed personal information contained in your Dayforce account, including your name, address, date of birth, employment details, bank account number, and Social Security number. In addition, the unauthorized person had access to the payroll administrator's email account, which contained emails and attachments that included employee personal information, including names, addresses, employment details, bank account numbers, and Social Security numbers.

We wanted to make you aware of our findings and assure you that we take this type of incident very seriously. Out of an abundance of caution, **we are offering you a complimentary one-year membership of Experian's® IdentityWorksSM Credit 3B.** This product provides you with identity detection and resolution of identity theft. IdentityWorks Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. **For more information on IdentityWorks Credit 3B, including instructions on how to activate your complimentary one-year membership, as well as some additional steps you can take in response, please see the additional information provided in the following pages.**

We apologize for any inconvenience or concern this incident may have caused. To help prevent a similar incident in the future, we have implemented enhanced security measures in Dayforce and Office 365, and we will be providing additional phishing awareness training to employees. If you have any questions, please call 888-287-9902, Monday through Friday, from 7 a.m. to 7 p.m. MST.

Sincerely,

Tonya L. Bukacek
Vice President, Information Technology, Security & Facilities

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: <<Enrollment Deadline>> (Your code will not work after this date.)
2. VISIT the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
3. PROVIDE the Activation Code: <<Activation Code>>

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **877-890-9332** by <<enrollment deadline>>. Be prepared to provide engagement number <<engagement #>> as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at **877-890-9332**. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). 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.

ADDITIONAL STEPS YOU CAN TAKE

Regardless of whether you choose to take advantage of this free credit monitoring, we remind you to remain vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. If you detect any unauthorized activity on financial accounts, you should immediately contact your financial institution. We also recommend that you make your financial institution aware of this matter and take their advice on steps to protect your bank account. 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

If you are a resident of Connecticut, Maryland, or North Carolina, you may contact and obtain information from your state attorney general at:

- *Connecticut Attorney General's Office*, 55 Elm Street, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag
- *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us
- *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6400 / 1-877-566-7226, www.ncdoj.gov

If you are a resident of West Virginia, you have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described below. You also have a right to place a security freeze on your credit report, as described below.

Fraud Alerts: There are two types of 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 at least 90 days. 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. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Credit Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

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

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five years, provide the addresses where you have lived over the prior five years
5. Proof of current address such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five 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, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity 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 one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus 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 one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.

Fair Credit Reporting Act: You also have rights under the federal Fair Credit Reporting Act, which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has published a list of the primary rights created by the FCRA (<https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>), and that article refers individuals seeking more information to visit www.ftc.gov/credit. The FTC's list of FCRA rights includes:

- You have the right to receive a copy of your credit report. The copy of your report must contain all the information in your file at the time of your request.
- Each of the nationwide credit reporting companies – Equifax, Experian, and TransUnion – is required to provide you with a free copy of your credit report, at your request, once every 12 months.
- You are also entitled to a free report if a company takes adverse action against you, like denying your application for credit, insurance, or employment, and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You are also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; if you are on welfare; or if your report is inaccurate because of fraud, including identity theft.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited. You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you receive based on information in your credit report.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.



Return Mail Processing Center
PO Box 9349
Dublin, Ohio 43017

<<Mail ID>>
<<Name 1>><<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

May 22, 2019

Dear <<Name 1>>:

Fellowship of Catholic University Students (FOCUS) takes data security very seriously, and we understand the importance of protecting the information we maintain. We are writing to inform you that we recently identified and addressed an incident that may have involved some of your personal information. This letter describes the incident, the measures we have taken, and some steps you can take in response.

We recently notified your family member who is a current or former employee of FOCUS about an incident in which an unauthorized individual accessed FOCUS’s human resources and payroll program, Ceridian Dayforce. While investigating that incident, we learned that the unauthorized individual also accessed the email accounts of the payroll administrator and two former employees. On May 9, 2019, we concluded an investigation and analysis of those accessed accounts to determine the nature and full scope of the incident. Findings from our investigation indicate that an unauthorized individual had access to the employees’ email accounts, at various times from December 15, 2018 through January 16, 2019. The investigation was not able to determine which emails and attachments were viewed by the unauthorized individual. Therefore, FOCUS conducted a thorough review of the contents of the accessed accounts and determined that an email or an attachment to an e-mail contained some of your personal information including your name, <<variable data elements>>.

We wanted to make you aware of our findings and assure you that we take this type of incident very seriously. Out of an abundance of caution, **we are offering you a complimentary one-year membership of Experian’s® IdentityWorksSM Credit 3B.** This product provides you with identity detection and resolution of identity theft. IdentityWorks Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. **For more information on IdentityWorks Credit 3B, including instructions on how to activate your complimentary one-year membership, as well as some additional steps you can take in response, please see the additional information provided in the following pages.**

We apologize for any inconvenience or concern this incident may have caused. To help prevent a similar incident in the future, we have implemented enhanced security measures in Dayforce and Office 365, and we will be providing additional phishing awareness training to employees. If you have any questions, please call 888-287-9902, Monday through Friday, from 7 a.m. to 7 p.m. MST.

Sincerely,

Tonya L. Bukacek
Vice President, Information Technology, Security & Facilities

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: **August 30, 2019** (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: <https://www.experianidworks.com/3bcredit>
3. PROVIDE the **Activation Code**: <<**Activation Code**>>

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **877-890-9332** by **August 30, 2019**. Be prepared to provide engagement number **DB12617** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at **877-890-9332**. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

* Offline members will be eligible to call for additional reports quarterly after enrolling

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). 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

ADDITIONAL STEPS YOU CAN TAKE

Regardless of whether you choose to take advantage of this free credit monitoring, we remind you to remain vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. If you detect any unauthorized activity on financial accounts, you should immediately contact your financial institution. We also recommend that you make your financial institution aware of this matter and take their advice on steps to protect your bank account. 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

If you are a resident of Maryland or North Carolina, you may contact and obtain information from your state attorney general at:

- *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us
- *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6400 / 1-877-566-7226, www.ncdoj.gov

Fraud Alerts: There are two types of 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 at least 90 days. 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. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Credit Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

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

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five years, provide the addresses where you have lived over the prior five years
5. Proof of current address such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five 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, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity 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 one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus 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 one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>> <<Date>>

Dear <<Name 1>>:

Fellowship of Catholic University Students (FOCUS) takes data security very seriously, and we understand the importance of protecting the information we maintain. We are writing to inform you that we recently identified and addressed an incident that may have involved some of your personal information. This letter describes the incident, the measures we have taken, and some steps you can take in response.

On July 13, 2019, we concluded an investigation and analysis of a data security incident involving unauthorized access to two employees' email accounts. Upon learning of the unauthorized access to these accounts, we launched an investigation with assistance from a cybersecurity firm to determine the nature and scope of the of the unauthorized access. Findings from our investigation indicate that an unauthorized individual gained access to the employees' email accounts at various times between November 9, 2018 and December 20, 2018. The investigation was not able to determine which emails and attachments were viewed by the unauthorized individual. Therefore, FOCUS conducted a thorough review of the contents of the accessed accounts and determined that an email or an attachment to an email contained some of your personal information including your name, <<variable data elements>>.

We wanted to make you aware of our findings and assure you that we take this type of incident very seriously. We remind you to remain vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity.

We apologize for any inconvenience or concern this incident may have caused. To help prevent a similar incident in the future, we have implemented enhanced security measures in Office 365, and we will be providing additional phishing awareness training to employees. If you have any questions, please call 888-287-9902, Monday through Friday, from 7:00 a.m. to 7:00 p.m. MST.

Sincerely,

Tonya L. Bukacek
Vice President, Information Technology, Security & Facilities

ADDITIONAL STEPS YOU CAN TAKE

We remind you to remain 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