

February 15, 2024

**Jennifer S. Stegmaier**  
312.704.0550 (direct)  
jennifer.stegmaier@wilsonelser.com

**Via Email:**

**Attorney General Anthony G. Brown**

Office of the Attorney General

Attn: Security Breach Notification

200 St. Paul Place

Baltimore, MD 21202

[IDTheft@oag.state.md.us](mailto:IDTheft@oag.state.md.us)

**Re: Data Security Incident Involving St. Mary's Seminary and University**

Dear Attorney General Brown:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents St. Mary's Seminary and University ("St. Mary's"), a seminary located at 5400 Roland Ave., Baltimore, MD 21210, with respect to a recent data privacy incident that was first discovered by St. Mary's on December 31, 2023 (hereinafter, the "Incident"). St. Mary's 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.

This letter will serve to inform you of the nature of the Incident, what information may have been compromised, the number of Maryland residents being notified, and the steps that St. Mary's has taken in response to the Incident. We have also enclosed hereto a sample of the notification made to the potentially impacted individuals, which includes an offer of free credit monitoring services.

**1. Nature of the Incident**

On December 31, 2023, St. Mary's became aware of a suspicious activity on its network. Upon discovery of this incident, St. Mary's immediately disconnected all access to the network and promptly engaged a specialized third-party cybersecurity firm and IT personnel to assist with securing the environment, as well as, to conduct a comprehensive forensic investigation to determine the nature and scope of the incident. While the forensic investigation remains ongoing, St. Mary's found evidence to suggest some files were accessed by an unauthorized actor.

Based on these findings, St. Mary's began reviewing the affected systems to identify the specific individuals and the types of information that may have been compromised. While this process remains ongoing, St. Mary's will notify affected individuals by mail as the information becomes available.

Although St. Mary's is unaware of any fraudulent misuse of information, it is possible that the following information may have been subject to unauthorized access: name; address; Social

Security Number, financial account information; and date of birth. In addition, student identification number may have been accessed for those students who were potentially impacted.

As of this writing, St. Mary's has not received any reports of related identity theft since the date of the incident (December 31st to present).

## **2. Number of Maryland residents affected.**

St. Mary's is working on determining the number of Maryland residents affected. The conclusion of the forensic investigation will provide additional insight as to the number of individuals impacted. St. Mary's shall provide the total number of MD residents affected and a copy of the notification letter to the Attorney General office as it becomes available. St. Mary's did post substitute notice on its website on February 15, 2024. The notice can be found at <https://stmarys.edu/>.

## **3. Steps taken in response to the Incident.**

St. Mary's is committed to ensuring the security and privacy of all personal information in its control and is taking steps to prevent a similar incident from occurring in the future. Upon discovery of the Incident, St. Mary's moved quickly to investigate and respond to the Incident and assessed the security of its systems. Specifically, St. Mary's engaged a specialized cybersecurity firm and IT personnel to conduct a forensic investigation to determine the nature and scope of the Incident. Additionally, St. Mary's took the following steps, including, but not limited to: disconnecting all access to the network; changing administrative credentials; restoring operations in a safe and secure mode; enhancing security measures; and took steps and will continue to take steps to mitigate the risk of future harm.

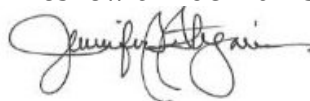
St. Mary's will notify individuals and provide Credit monitoring as appropriate. Additionally, St. Mary's shall provide guidance on how to better protect against identity theft and fraud, including providing information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and the contact details for the Federal Trade Commission.

## **4. Contact information**

St. Mary's 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 [Jennifer.stegmaier@wilsonelser.com](mailto:Jennifer.stegmaier@wilsonelser.com) or 312-704-0550.

Very truly yours,

**Wilson Elser Moskowitz Edelman & Dicker LLP**



Jennifer S. Stegmaier

July 22, 2024

**Jennifer S. Stegmaier**  
312.704.0550 (direct)  
jennifer.stegmaier@wilsonelser.com

**Via Email**

**Attorney General Anthony G. Brown**

Office of the Attorney General

Attn: Security Breach Notification

200 St. Paul Place

Baltimore, MD 21202

[IDTheft@oag.state.md.us](mailto:IDTheft@oag.state.md.us)

**Re: Supplemental Data Security Incident Involving St. Mary's Seminary and University**

Dear Attorney General Brown:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents St. Mary's Seminary and University ("St. Mary's"), a seminary located at 5400 Roland Ave., Baltimore, MD 21210, with respect to a recent data privacy incident that was first discovered by St. Mary's on December 31, 2023 (hereinafter, the "Incident"). This is a supplement to the preliminary notice that was previously submitted to your office on February 15, 2024. St. Mary's 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.

This letter will serve to inform you of the nature of the Incident, what information may have been compromised, the number of Maryland residents being notified, and the steps that St. Mary's has taken in response to the Incident. We have also enclosed hereto a sample of the notification made to the potentially impacted individuals, which includes an offer of free credit monitoring services.

**1. Nature of the Incident**

On December 31, 2023, St. Mary's became aware of a suspicious activity on its network. Upon discovery of this incident, St. Mary's immediately disconnected all access to the network and promptly engaged a specialized third-party cybersecurity firm and IT personnel to assist with securing the environment, as well as, to conduct a comprehensive forensic investigation to determine the nature and scope of the incident. The forensic investigation was concluded on or about February 14, 2024 and determined that certain files were accessed by an unauthorized actor and the date range of the breach was from December 29, 2023 through December 31, 2024.

Based on these findings, St. Mary's began reviewing the impacted files to identify the specific individuals and the types of information that may have been compromised. On June 17, 2024, St. Mary's finalized the list of individuals to notify, followed by organizing the mailing, call center, and credit monitoring services for the impacted population. This process was necessary to provide

accurate information and notice to the potentially impacted individuals. St. Mary's began mailing notice letters to potentially impacted individuals on July 8, 2024 through July 22, 2024.

Based on its investigation, the following information may have been subject to unauthorized access: name; address; and Social Security Number. As of this writing, St. Mary's has not received any reports of related identity theft since the date of the incident (December 31st to present).

## **2. Number of Residents affected.**

St. Mary's determined that information pertaining to 201 Maryland residents was impacted as a result of the Incident. Notification letters to these individuals were mailed on July 8, 2024 to July 22, 2024, by first class mail. A sample copy of the notification letter is attached hereto as **Exhibit A**.

## **3. Steps taken in response to the Incident.**

Data privacy and security is among St. Mary's highest priorities, and it is committed to doing everything they can to protect the privacy and security of the personal information in their care. Upon discovery of the Incident, St. Mary's moved quickly to investigate and respond to the Incident and assessed the security of its systems. Specifically, St. Mary's engaged a specialized cybersecurity firm and IT personnel to conduct a forensic investigation to determine the nature and scope of the Incident. Additionally, St. Mary's took the following steps, including, but not limited to: disconnecting all access to the network; reset credentials; installed SentinelOne and Huntress on all end points.

In response to the incident, St. Mary's also provided impacted individuals with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for 12 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, St. Mary's also provided proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services are provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

Additionally, St. Mary's provided guidance on how to better protect against identity theft and fraud, including providing information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and the contact details for the Federal Trade Commission.

## **4. Contact information**

St. Mary's 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 [Jennifer.stegmaier@wilsonelser.com](mailto:Jennifer.stegmaier@wilsonelser.com) or 312-704-0550.

Very truly yours,

**Wilson Elser Moskowitz Edelman & Dicker LLP**

A handwritten signature in black ink, appearing to read "Jennifer S. Stegmaier". The signature is fluid and cursive, with the first name "Jennifer" being more legible than the last name "Stegmaier".

Jennifer S. Stegmaier

# **Exhibit A**

St. Mary's Seminary and University  
c/o Cyberscout  
PO Box 1286  
Dearborn, MI 48120-9998

***Via First-Class Mail***



July 22, 2024

**Re: Notice of Data Breach**

Dear [REDACTED],

St. Mary's Seminary and University ("St. Mary's"), located at 5400 Roland Ave, Baltimore, MD 21210, is supplementing its prior letter that was mailed to you on July 8, 2024 regarding the recent data security incident that may have resulted in an unauthorized access to your personal information. This letter is to intended to provide you with a new unique enrollment code to receive complimentary credit monitoring services that St. Mary's is providing to you at no cost. **Please disregard the enrollment code in the prior letter.**

**What Happened?**

On December 31, 2023, St. Mary's became aware of a suspicious activity on its network. Upon discovery of this incident, St. Mary's immediately disconnected all access to the network and promptly engaged a specialized third-party cybersecurity firm and IT personnel to assist with securing the environment, as well as, to conduct a comprehensive forensic investigation to determine the nature and scope of the incident. The forensic investigation concluded on or about February 14, 2024, and determined that certain files were accessed by an unauthorized actor.

Based on these findings, St. Mary's began reviewing the affected files to identify the specific individuals and the types of information that may have been compromised. On June 17, 2024, St. Mary's finalized the list of individuals to notify, followed by organizing the mailing, call center, and credit monitoring services for the impacted population. This process was necessary to provide accurate information and notice to the potentially impacted individuals.

**What Information Was Involved?**

Although St. Mary's has no evidence that any sensitive information has been misused by third parties as a result of this incident, we are notifying you out of an abundance of caution and for purposes of full transparency. Based on the investigation, the following information related to you may have been subject to unauthorized access: name; address; and Social Security number.

**What We Are Doing**

Data privacy and security is among St. Mary's highest priorities, and we are committed to doing everything we can to protect the privacy and security of the personal information in our care. Upon discovery of the Incident, St. Mary's moved quickly to investigate and respond to the Incident and assessed the security of its systems. Specifically, St. Mary's engaged a specialized cybersecurity firm and IT personnel to conduct a forensic investigation to determine the nature and scope of the Incident. Additionally, St. Mary's took the following steps, including, but not limited to: disconnecting all access to the network; reset credentials; installed SentinelOne and Huntress on all end points.

000010103G0500

P

In response to the incident, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for twelve months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

### **How do I enroll for the free services?**

To enroll in Credit Monitoring services at no charge, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED]. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

### **What You Can Do**

We encourage you to enroll in the complimentary credit monitoring being offered to you by St. Mary's. We also encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file. Please review the enclosed *Steps You Can Take to Help Protect Your Information*, to learn more about how to protect against the possibility of information misuse.

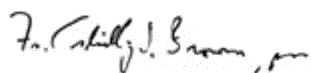
We would like to reiterate that, at this time, there is no evidence that your information was misused. However, we encourage you to take full advantage of the services offered.

### **For More Information**

Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call the help line at 1-800-405-6108 and supply the fraud specialist with your unique code listed above.

St. Mary's sincerely regrets any concern or inconvenience this matter may cause, and remains dedicated to ensuring the privacy and security of all information in our control.

Sincerely,



Fr. Phillip J. Brown, P.S.S.  
President Rector  
St. Mary's Seminary and University

## Steps You Can Take to Help Protect Your Information

**Credit Reports:** 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](http://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.

**Fraud Alerts:** You can place fraud alerts with the three credit bureaus by phone or online. 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.

### Experian

P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742

### TransUnion

P.O. Box 2000  
Chester, PA 19016  
1-800-680-7289

### Equifax

P.O. Box 105069  
Atlanta, GA 30348  
1-800-525-6285

[www.experian.com/fraud/center.html](http://www.experian.com/fraud/center.html) [www.transunion.com/fraud-alerts](http://www.transunion.com/fraud-alerts) <https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>

**Monitoring:** You should always remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and by monitoring your credit report for suspicious or unusual activity.

**Security Freeze:** You 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, 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 any one or more of the following national consumer reporting agencies:

### Experian

P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742

### TransUnion

P.O. Box 160  
Woodlyn, PA 19094  
1-888-909-8872

### Equifax

P.O. Box 105788  
Atlanta, GA 30348-5788  
1-888-298-0045

[www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html) [www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze) <https://www.equifax.com/personal/credit-report-services/credit-freeze/>

**File Police Report:** You have the right to file or obtain a police report if you 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 proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.



**FTC and Attorneys General:** You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, [www.identitytheft.gov](http://www.identitytheft.gov), 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. Instances of known or suspected identity theft should also be reported to law enforcement.

**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 Massachusetts:** It is required by state law that you are informed of your right to obtain a 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.

**For residents of New Mexico:** State law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the 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 credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act at [www.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf) or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

**For residents of Oregon:** State law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

**For residents of Rhode Island:** It is required by state law that you are informed of your right to file or obtain a police report in regard to this incident.

**For residents of Arizona, Colorado, District of Columbia, Illinois, Maryland, New York, North Carolina, and Rhode Island:** You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

**Federal Trade Commission - Consumer Response Center:** 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); [www.identitytheft.gov](http://www.identitytheft.gov)

**Arizona Office of the Attorney General** Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

**Colorado Office of the Attorney General** Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 [www.coag.gov](http://www.coag.gov)

**District of Columbia Office of the Attorney General - Office of Consumer Protection:** 400 6th Street, NW, Washington, DC 20001; 202-727-3400; [www.oag.dc.gov](http://www.oag.dc.gov)

**Illinois office of the Attorney General -** 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; [www.illinoisattorneygeneral.gov](http://www.illinoisattorneygeneral.gov)

**Maryland Office of the Attorney General** - Consumer Protection Division: 200 St. Paul Place, 16<sup>th</sup> floor, Baltimore, MD 21202; 1-888-743-0023; [www.oag.state.md.us](http://www.oag.state.md.us)

**New York Office of Attorney General** - Consumer Frauds & Protection: The Capitol, Albany, NY 12224; 1-800-771-7755; <https://ag.ny.gov/consumer-frauds/identity-theft>

**North Carolina Office of the Attorney General** - Consumer Protection Division: 9001 Mail Service Center, Raleigh, NC 27699; 1-877-566-7226; [www.ncdoj.com](http://www.ncdoj.com)

**Rhode Island Office of the Attorney General** - Consumer Protection: 150 South Main St., Providence RI 02903; 1-401-274-4400; [www.riag.ri.gov](http://www.riag.ri.gov)



