100 International Drive
23rd Floor
Baltimore, MD 21202

P 1.248.646.5070
F 1.248.646.5075

McDonald Hopkins
A business advisory and advocacy law firm®

Spencer S. Pollock, CIPP/US, CIPM
Direct Dial: (410) 456-2741
Cell: (410) 917-5189
E-mail: spollock@mcdonaldhopkins.com

June 13, 2023

VIA EMAIL (Idtheft@oag.state.md.us)

Anthony G. Brown
Office of the Attorney General
St. Paul Plaza
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Central Services of the Roman Catholic Archbishop of Baltimore - Security Breach Notification

Dear Mr. Brown:

We are writing on behalf of our client, Central Services of the Roman Catholic Archbishop of Baltimore ("Archdiocese of Baltimore") (located at 320 Cathedral Street, Baltimore, MD 21201) to notify you of a data security incident involving thirty-six (36) Maryland residents.

Nature

On or about July 13, 2022, Archdiocese of Baltimore learned that one of its facilities department employees received an email request for vendor payment including fraudulent ACH payment instructions. The payment was made by Archdiocese of Baltimore and it was later determined that this email was a spoof email by a threat actor posing as an Archdiocese of Baltimore vendor. In response, Archdiocese of Baltimore immediately implemented password resets and reset multi-factor authentication tokens. Archdiocese of Baltimore also engaged third-party independent cybersecurity experts to conduct an investigation into the incident to determine whether any email account in question was subject to unauthorized access.

At the conclusion of the investigation, in October 2022, Archdiocese of Baltimore determined that, while the email accounts in question belonging to facilities staff were not subject to unauthorized access, evidence was uncovered that ten other Archdiocese of Baltimore email accounts had been subject to unauthorized access beginning on or around January 2022 to August 9, 2022. At that time, Archdiocese of Baltimore immediately implemented additional password resets and ensured multi-factor authentication was enforced.

Given the results of the investigation, Archdiocese of Baltimore also began a comprehensive and thorough review of the affected email accounts. Archdiocese of Baltimore recently completed its review to identify the individuals whose personal information was included in the impacted data. On May 19, 2023, Archdiocese of Baltimore concluded its review and located the most recent contact information for these individuals. Archdiocese of Baltimore determined that the incident potentially involved thirty-six (36) Maryland residents.

The personal information obtained potentially included first and last name in addition to one or more of the following data elements: driver's license or state identification number, medical information, clinical or treatment information, prescription information, Social Security number, and financial account and routing number. Not all data elements were impacted for all potentially affected individuals. Through the investigation and review, Archdiocese of Baltimore discovered no evidence that personal information was used for identity theft or financial fraud.

Notice and Archdiocese of Baltimore's Response to the Event

On June 14, 2023, Archdiocese of Baltimore will mail written notification to the potentially affected Maryland residents for whom a mailing address is available or, alternatively, will contact the individuals by phone, pursuant to Md. Code Ann., Com. Law § 14-3501-3508, conveying the information in a substantially similar form as outlined in the enclosed letter (attached as Exhibit A).

Additionally, Archdiocese of Baltimore is providing the potentially impacted individuals the following:

- Free access to credit monitoring services for one year through TransUnion;
- Guidance on ways to protect against identity theft and fraud, including steps to report any suspected activities or events of identity theft or fraud to their credit card company and/or bank;
- The appropriate contact information for the consumer reporting agencies along with information on how to obtain a free credit report and place a fraud alert and security freeze on their credit file;
- A reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports; and
- Encouragement to contact the Federal Trade Commission and law enforcement to report attempted or actual identity theft and fraud.

Finally, in response to this incident, Archdiocese of Baltimore implemented multi-factor authentication on all user accounts within its Microsoft tenant. Further, Archdiocese of Baltimore is continuing to monitor its environment, perform annual technical security assessments, and Archdiocese of Baltimore is implementing additional cybersecurity safeguards, as needed. Archdiocese of Baltimore is also continuing to train employees and Archdiocese of Baltimore is increasing the complexity requirements for employee passwords to help minimize the likelihood of this type of incident occurring again.

Contact Information

If you have any questions or wish to discuss this event further, please do not hesitate to call me on my direct dial (410) 456-2741 or email me at spollock@mcdonaldhopkins.com.

Sincerely Yours,

Spencer S. Pollock, Esq., CIPP/US, CIPM

EXHIBIT A

[redacted]

ARCHDIOCESE of BALTIMORE
320 Cathedral Street
Baltimore, MD 21201

[redacted]

June 14, 2023

Re: Notice of Data Security Incident

Dear [redacted]

At Central Services of the Roman Catholic Archbishop of Baltimore ("Archdiocese of Baltimore"), we value transparency and respect the privacy of your information, which is why, as a precautionary measure, we are writing to let you know about a data security incident that may involve your protected personal information, what we did in response, and steps you can take to protect yourself against possible misuse of the information.

What Happened

On or about July 13, 2022, we learned that one of our facilities department employees received fraudulent ACH payment instructions via email requesting that Archdiocese of Baltimore pay one of our vendors. It was later determined that this email was a spoof email by a threat actor posing as our vendor. In response, we immediately implemented password resets and reset multi-factor authentication tokens. We also engaged third-party independent cybersecurity experts to conduct an investigation into the incident to determine whether any email account in question was subject to unauthorized access.

At the conclusion of the investigation, in October 2022, we determined that, while the email accounts in question belonging to our facilities staff were not subject to unauthorized access, evidence was uncovered that ten of our other email accounts had been subject to unauthorized access beginning on or around January 2022 to August 9, 2022. At that time, we immediately implemented additional password resets and we ensured multi-factor authentication was enforced.

Given the results of the investigation, we also began a comprehensive and thorough review of the affected email accounts. Our review recently concluded and determined that your protected personal information was included within the email accounts subject to unauthorized access and, as a result, your information may have been viewed or acquired by an unauthorized individual. Based on our investigation and review, we have no evidence that your information has been used for identity theft or financial fraud. However, we wanted to notify you of the incident out of an abundance of caution and provide you information on how to best protect your identity.

What Information Was Involved

The types of information included your [redacted]

To reiterate, we have no evidence indicating that any information has been used for identity theft or financial fraud.

What We Are Doing

The security and privacy of the information contained within our systems is a top priority for us. In response to this incident, we took immediate steps to secure our systems and engaged third-party forensic experts to assist in the investigation. We promptly terminated unauthorized access to the email accounts following the preliminary investigation into the suspicious activity. We conducted a forensic investigation and subsequent

review to identify the individuals potentially affected and the nature of information that may have been compromised to notify the appropriate individuals accordingly.

We have implemented multi-factor authentication on all user accounts within our Microsoft tenant. Further, we are continuing to monitor our environment, perform annual technical security assessments, and we are implementing additional cybersecurity safeguards, as needed. We are also continuing to train our employees and we are increasing the complexity requirements for our employee passwords to help minimize the likelihood of this type of incident occurring again.

What You Can Do

While we have no evidence that your personal information has been used for identity theft or fraud, out of an abundance of caution, 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. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event you become a victim of identity theft. These services will be provided by Cyberscout through Identity Force, a TransUnion company, specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring services at no charge, please log on to [redacted] 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.

This letter also provides other precautionary measures you can take to protect your personal information, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information

Please accept our apologies that this event occurred. We understand that you may have questions about what happened beyond what is covered in this letter. If you have additional questions, please contact me at [redacted] or [redacted]

Sincerely,

Marcus Madsen
CIO and Technology Director
Archdiocese of Baltimore
320 Cathedral Street
Baltimore, MD 21201

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary 12-Month Credit Monitoring.

To enroll in Credit Monitoring services at no charge, please log on to [redacted] 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.

2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary 12-month credit monitoring services, we recommend that you place an initial one (1) year "fraud alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105069
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
(800) 525-6285

Experian
P.O. Box 9554
Allen, TX 75013
https://www.experian.com/fraud/center.html
(888) 397-3742

TransUnion LLC
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016-2000
https://www.transunion.com/fraud-alerts
(800) 680-7289

3. Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "security freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-freeze/
(888) 298-0045

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

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
https://www.transunion.com/credit-freeze
(888) 909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name, or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland**,** Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202**,** www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.