

NH DEPT OF JUSTICE
APR 26 24 PM 12:28

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®

April 23, 2024

VIA U.S. MAIL

John M. Formella
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301

Re: Catholic Diocese of Cleveland - Incident Notification

Dear Mr. Formella:

We are writing on behalf of our client, the Catholic Diocese of Cleveland (the "Diocese") (located at 1404 East 9th Street, Cleveland, OH 44114), to notify you of an information security incident involving one (1) New Hampshire resident. By providing this notice, the Diocese does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature

On January 12, 2024, the Diocese detected an information security incident involving unauthorized access to one (1) employee's business email account. Upon learning this, the Diocese engaged our firm and third-party forensic and incident response professionals to conduct a thorough investigation of the nature and scope of the incident.

Following the forensic investigation, the Diocese determined that the contents of the email account were subject to access and acquisition by an unauthorized individual between December 14, 2023 and January 12, 2024. The Diocese conducted an extensive manual review of the affected data and, on March 14, 2024, we discovered the potentially impacted data contained personal information. On April 8, 2024, the Diocese located the most recent contact information for the affected individuals and discovered the incident affected a New Hampshire resident. The personal information potentially obtained from the New Hampshire resident included

Notice and Response to the Event

Baltimore | Chicago | Cleveland | Columbus | Detroit | West Palm Beach
mcdonaldhopkins.com

Commencing on April 17, 2024, the Diocese will begin mailing written notifications to the potentially affected individuals in substantially similar form as the enclosed letter (attached as **Exhibit A**).

Additionally, the Diocese is providing the potentially impacted residents the following:

- Free access to credit monitoring services for _____ ;
- 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.

Further, the Diocese will provide notice to the applicable government regulators, officials, and state Attorneys General (as necessary).

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

Sincerely Yours,

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

Exhibit A

Baltimore | Chicago | Cleveland | Columbus | Detroit | West Palm Beach
mcdonaldhopkins.com



Catholic Diocese
of Cleveland

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

Property and Casualty Insurance

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Dear <<First_Name>>:

The privacy and security of the personal information entrusted to us is of the utmost importance to the Catholic Diocese of Cleveland (hereinafter, the "Diocese"). We are writing to provide you with information regarding an information incident which potentially affected the security of some of your personal information. As such, we wanted to provide you with information about the incident, explain the services we are making available to you and let you know that we continue to take significant measures to protect your information.

What Happened?

On January 12, 2024, the Diocese detected an information security incident involving unauthorized access to one (1) employee's business email account.

What We Are Doing.

Upon learning this, we contained the incident and commenced a prompt and thorough investigation. As part of the investigation, we engaged third-party cybersecurity professionals experienced in handling these type of incidents. The investigation aimed to determine the nature and scope of the incident and whether any personal information was accessed and/or acquired by an unauthorized party.

Following the forensic investigation, we determined that the contents of the email account were subject to access and acquisition by an unauthorized individual between December 14, 2023 and January 12, 2024. We conducted an extensive manual review of the affected data and, on March 14, 2024, we discovered the potentially impacted data contained your personal information. On April 5, 2024 we located your last known address to provide you with direct notice of this incident.

What Information Was Involved?

One or more of the files potentially acquired by the unauthorized party contained

What You Can Do.

We have no evidence that any of your information has been used to commit identity theft or financial fraud. Nevertheless, out of an abundance of caution, we are providing you with _____ of complimentary services through Experian IdentityWorksSM.

This letter also provides precautionary measures you can take to protect your personal information, including placing a Fraud Alert and Security Freeze on your credit files, and 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. The enclosed "Other Important Information" provides further details regarding what you can do and how you can enroll in your complimentary membership.

For More Information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at . This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, between 8:00 am and 5:30 pm Central Time, excluding major U.S. holidays.

Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information.

Sincerely,

Dave Gebacz

Assistance Finance Officer

The Catholic Diocese of Cleveland

- OTHER IMPORTANT INFORMATION -

1. Enrolling in Complimentary Credit Monitoring.

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. 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 from the date of the incident (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 Identity Restoration is available to you for _____ 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.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary _____ membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** <<b2b_text_6 (activation deadline)>> (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your **activation code:** <<Activation Code (S_N)>>

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at _____. Be prepared to provide engagement number <<b2b_text_2 (Engagement Number)>> as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR _____ 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.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

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

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

2. Placing a Fraud Alert.

We recommend that you place a one-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 30348-5069
www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
(888) 378-4329

Experian

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

TransUnion

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

3. Consider 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 cost. 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 sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348-5788
www.equifax.com/personal/credit-report-services/credit-freeze/
(800) 349-9960
(888) 298-0045

Experian Security Freeze

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

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
www.transunion.com/credit-freeze
(888) 916-8800

In order to place the security freeze, you will need to supply your name, address, date of birth, Social Security number and other personal information such as copy of a government issued identification. 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. 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.

You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

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 this notice letter states that your financial account information and/or credit or debit card information was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number.

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.

Consider keeping a record of your contacts. Start a file with copies of your credit reports, the police reports, any correspondence, and copies of disputed bills. It is helpful to log conversations with creditors, law enforcement officials, and other relevant parties.

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, <https://www.marylandattorneygeneral.gov/>, Telephone: 888-743-0023.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.