April 16, 2024

Via Electronic Mail: DOJ-CPB@doj.nh.gov

Attorney General John M. Formella
33 Capitol St.
Concord, NH 03301

Re: Our Client : Roman Catholic Diocese of Phoenix
Wilson Elser File # : 16516.02218

Dear Attorney General Formella:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents The Roman Catholic Diocese of Phoenix (the "Diocese") with respect to a data privacy incident (hereinafter, the "Incident"). The Diocese 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 New Hampshire residents being notified, and the steps that the Diocese 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. 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.

1. Nature of Security Incident

On January 17, 2024, the Diocese discovered suspicious activity in its network environment. Upon discovery of this incident, the Diocese promptly took steps to secure its network and engaged a specialized cybersecurity firm to investigate the nature and scope of the incident. As a result of the investigation, the Diocese learned that an unauthorized actor accessed certain files and data stored within our network, including pension data for the Diocese.

Upon learning this, the Diocese began a time-consuming and detailed reconstruction and review of the data stored on the server at the time of this incident to understand whose information was

affected. On March 23, 2024, the Diocese identified persons whose sensitive data was included within the impacted data. At this time, we have no evidence any of the information has been misused by a third party.

1. Number of New Hampshire Residents Affected

A total of forty-six (46) New Hampshire residents were potentially affected by this incident. The investigation determined that the potentially impacted personal information included:

.

Notification letters to the potentially impacted individuals were mailed on , by first class mail. A sample copy of the notification letter is included with this letter under **Exhibit A.**

2. Steps taken in response to the Incident

Data security is one of the Diocese's highest priorities. Upon detecting this incident, the Diocese moved quickly to initiate an investigation to identify potentially affected individuals. The Diocese retained a leading data privacy and cybersecurity firm who assisted in the investigation. The Diocese also deployed additional monitoring tools and will continue to enhance the security of its systems. The Diocese take the protection and proper use of personal information very seriously.

The Diocese is also offering of complimentary credit monitoring and identity theft restoration services through Identity Force, a TransUnion company, to affected Massachusetts individuals to help protect their identity. Additionally, the Diocese 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.

3. Contact Information

The Diocese 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

.

Sincerely,

Wilson Elser Moskowitz Edelman & Dicker LLP

EXHIBIT A

THE ROMAN CATHOLIC
DIOCESE OF PHOENIX

PO Box 480149
Niles, IL 60714

<<FirstName>> <<LastName>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

Via First-Class Mail

April 15, 2024

<<Variable Header>>

Dear <<FirstName>> <<LastName>>:

The Roman Catholic Diocese of Phoenix (the "Diocese") is writing to inform you of a recent data security incident that has resulted in unauthorized access to your data. While we are unaware of any fraudulent misuse of the accessed data at this time, we are providing you with details about the incident, steps we are taking in response, and resources available to help you protect against the potential misuse of your data. Please be assured the Diocese takes the protection and proper use of your data very seriously.

What Happened?

On January 17, 2024, the Diocese discovered suspicious activity in its network environment. Upon discovery of this incident, the Diocese promptly took steps to secure its network and engaged a specialized cybersecurity firm to investigate the nature and scope of the incident. As a result of the investigation, the Diocese learned that an unauthorized actor accessed certain files and data stored within our network, including data for many participants in Diocese-sponsored employee benefits programs.

Upon learning this, the Diocese began a time-consuming and detailed reconstruction and review of the data stored on the server at the time of this incident to understand whose information was affected. On March 23, 2024, the Diocese identified persons whose sensitive data was included within the impacted data. At this time, we have no evidence any of the information has been misused by a third party, but because information related to you was disclosed, we are notifying you so you can take proactive steps to provide your information.

What Information Was Involved?

The following data was potentially accessed and acquired by a person not authorized to view them: . The Diocese is not aware of any sensitive financial account or payment card information being impacted in this matter.

What Are We Doing?

Data security is one of our highest priorities. Upon detecting this incident, we moved quickly to initiate an investigation, which included retaining a leading forensic investigation firm who assisted in conducting an investigation and confirming

the security of our network environment. We also deployed additional monitoring tools and will continue to enhance the security of our systems. We take the protection and proper use of personal information very seriously.

As part of our ongoing commitment to information privacy and the security of information, we are offering identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include: <<Membership Length>> of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do

We 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 *Recommended Steps to Help Protect Your Information*, to learn more about how to protect against the possibility of information misuse.

To enroll in Credit Monitoring services at no charge, please log on to https://response.idx.us/dphx, or scan the QR image and use the Enrollment Code provided above. IDX representatives are available Monday through Friday from 7 am - 7 pm Mountain Daylight Time. Please note the deadline to enroll is .

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information

IDX has set up a call center with representatives to assist you with questions regarding this incident. You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call 1-888-863-4962 or go to https://response.idx.us/dphx for assistance or for any additional questions you may have.

At the Roman Catholic Diocese of Phoenix, we take our responsibility to protect your personal information very seriously. We are deeply disturbed by this situation and apologize for any inconvenience.

Sincerely,

Very Rev. John R. Muir, V.G.
Moderator of the Curia

Recommended Steps to Help Protect Your Information

1. **Website and Enrollment.** Scan the QR image or go to https://response.idx.us/dphx and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-888-863-4962 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever 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 some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: 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.

New Mexico Residents: 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 a violator. 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. You can review your rights pursuant to the Fair Credit Reporting Act by visiting 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.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, https://consumer.ftc.gov, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.