EXHIBIT 1

The Roman Catholic Diocese of Syracuse ("The Diocese of Syracuse") is located at 240 E Onondaga Street, Syracuse, NY 13202, and is writing to notify your office of an incident that may affect the security of certain personal information relating to one (1) Maine resident. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, The Diocese of Syracuse does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

On June 2, 2021, the Diocese of Syracuse discovered suspicious activity on its computer network. The Diocese of Syracuse immediately took steps to secure the network, and with the assistance of third-party specialists, launched an investigation into the nature and scope of the event. The investigation determined that certain systems had been infected by malware which prevented access to some files on the network. The investigation also determined the unauthorized actor had gained access to certain systems within their network between May 24, 2021, and June 2, 2021. As a result, the unauthorized actor may have had access to certain files within these systems. The Diocese of Syracuse then took steps to conduct a thorough and time-intensive review of the potentially impacted data to identify all individuals whose information may have been impacted. Following that review, the Diocese then worked to identify contact information for all of those individuals. That work was completed on May 24, 2022.

The information that could have been subject to unauthorized access includes name, and Social Security number.

Notice to Maine Resident

On or about June 6, 2022, The Diocese of Syracuse provided written notice of this incident to one (1) Maine resident. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, The Diocese of Syracuse moved quickly to investigate and respond to the incident, assess the security of The Diocese of Syracuse systems, and identify potentially affected individuals. Further, The Diocese of Syracuse notified federal law enforcement regarding the event. The Diocese of Syracuse is also working to implement additional safeguards and training to its employees. The Diocese of Syracuse is providing access to credit monitoring services for one (1) year, through IDX, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, The Diocese of Syracuse is providing impacted individuals with guidance on how to better protect against identity theft and fraud. The Diocese of Syracuse is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, 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 encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. The Diocese of Syracuse is providing written notice of this incident to relevant state regulators, as necessary.

EXHIBIT A

P.O. Box 1907
Suwanee, GA 30024

To Enroll, Please Call:
1-833-909-4275
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: <<XXXXXXXX>>

<<Name 1>> <<Name 2>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>

June 6, 2022

NOTICE OF <<SECURITY INCIDENT>> / <<DATA BREACH>>

Dear <<Name 1>> <<Name 2>>:

The Roman Catholic Diocese of Syracuse ("Diocese") is writing to inform you of an event that may impact the privacy of some of your information. We are providing you this letter as a precaution to inform you of this event, our response, and steps you can take to further protect your information, should you feel it necessary to do so.

What Happened?

On June 2, 2021, the Diocese discovered suspicious activity on its computer network. The Diocese immediately took steps to secure the network, and with the assistance of third-party specialists, launched an investigation into the nature and scope of the event. The investigation determined that certain systems had been infected by malware which prevented access to some files on the network. The investigation also determined the unauthorized actor had gained access to certain systems on our network between May 24, 2021 and June 2, 2021. As a result, the unauthorized actor may have had access to certain files within these systems. The Diocese then took steps to conduct a thorough and time-intensive review of the potentially impacted data to identify all individuals whose information may have been impacted. Following that review, the Diocese then worked to identify contact information for all of those individuals. That work was completed on May 24, 2022.

What Information Was Involved?

The information that may have been impacted by this event includes your name, and <<DATA ELEMENTS>>. At this time, we are not aware of any evidence this information was subject to actual or attempted misuse.

What We Are Doing.

The Diocese takes this event and the security of your information seriously. Upon learning of the event, we moved quickly to investigate and respond with the assistance of third-party cybersecurity specialists. The investigation and response included confirming the security of our systems, reviewing the contents of the relevant data for sensitive information, and notifying impacted individuals associated with that sensitive information. As part of our ongoing commitment to the privacy of personal information in our care, we are reviewing our policies, procedures and processes related to the storage and access of personal information. We have notified law enforcement of this event and will also notify applicable regulatory authorities, as required by law.

As an added precaution, we are also offering one year of complimentary access to credit monitoring services through IDX. Individuals who wish to receive these services must enroll by following the attached enrollment instructions.

What You Can Do.

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing account statements and monitoring your free credit reports for suspicious activity and to detect errors. You can review the enclosed *Steps You Can Take to Help Protect Personal Information* to learn helpful tips on steps you can take to protect against possible misuse should you feel it appropriate to do so.

For More Information.

If you have questions about this incident that are not addressed in this letter, please contact our dedicated call center at 1-833-909-4275, Monday through Friday from 9 am to 9 pm Eastern Time.

Sincerely,

Brian McAuliffe
Risk Manager

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Identity Monitoring

1. Website and Enrollment. Go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll is September 6, 2022.

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 1-833-909-4275 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and 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. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. The Diocese of Syracuse is located at 240 E Onondaga Street, Syracuse, NY 13202.

For 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 bureaus 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 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.

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

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are [#] Rhode Island residents impacted by this incident.