Notice of Data Security Event

Updated January 30, 2025

Catholic Charities West Michigan (CCWM) is dedicated to providing high-quality programs and services to families and individuals in West Michigan. We are writing to inform the community that we had a cyber incident in January 2025 that did not materially affect our programs and services. Please note that this matter does not affect our health record, donor, or payroll platforms.

What Happened? On January 13, 2025, an unknown cyber actor claimed to have accessed and copied files from our computer network. In response, we briefly took the computer network offline to investigate the claim and verify the security of the computer network. Through this investigation, we validated the claim that the computer network was accessed without permission and that files were likely copied between January 12 and 13.

What Information Was Involved? This matter did not affect our Electronic Health Record, donor, or payroll platforms. The majority of the files that were copied were unstructured non-profit operations and governance files. However, some files also contain information about clients of CCWM, including service details, scheduled sessions, progress notes and discharge summaries, treatment information, and adoption services. In other circumstances, the files may also include name and a unique identifier number, which can include an internally assigned identifier, a state assigned identifier, date of birth, or Social Security number. The files may also include historical volunteer background checks, which contain Social Security numbers. Files may also include certain human resources information, including current and former staff name, Social Security number, driver's license number, and direct deposit information.

Please note that we have no indication of an individual experiencing verified identity theft, fraud, or embarrassment as a result of this incident. Given the nature of the files involved with this matter, apart from staff and individuals with Social Security numbers affected, we will not be able to verify the identities and contact information to let individuals know about this matter directly, as much of the information is outdated. When the file review is complete, we will work to locate contact information and reach out to individuals with affected Social Security numbers if verifiable contact information is available. In the interim, whether individuals wish to take any steps in response to this matter is a personal decision. Individuals may utilize the free resources and guidance in the "Steps Individuals Can Take To Protect Personal Information" section below. If individuals have additional questions, they may refer to the "Frequently Asked Questions" section below or contact our toll-free dedicated assistance line.

What We Are Doing. While no safeguards can fully prevent all cybersecurity incidents, we are evaluating our technical measures and processes to further enhance our cyber security practices. We are also providing free resources and guidance in the "Steps Individuals Can Take To Protect Personal Information" section below.

What Individuals Can Do. As referenced above, any steps that individuals may wish to take are a personal decision. Should individuals feel steps need to be taken, they may review the "Steps Individuals Can Take To Protect Personal Information" and "Frequently Asked Questions" sections below.

For More Information. If individuals have questions about this matter, we have a dedicated assistance line with agents ready to answer their questions. Please contact our toll-free dedicated assistance line at 1-833-799-4081, Monday through Friday from 8:00 a.m. through 8:00 p.m. Eastern, excluding holidays. You may also write to us at Catholic Charities West Michigan, Attn: Director of Quality and Compliance, 40 Jefferson Ave. SE, Grand Rapids, MI 49503.

We are committed to maintaining the security of information in our care and confidence in our services. We thank you for your patience and understanding.

Sincerely,

Catholic Charities West Michigan

Frequently Asked Questions

What happened? In January 2025, an unknown cyber actor claimed to have accessed the computer network and copied certain files without permission. In response, the computer network was taken offline to verify its security and to determine what happened. Through this review, we validated the claim that the computer network was accessed without permission and that files were likely copied between January 12 and 13, 2025.

Was this a ransomware event? No. The investigation of this matter did not identify any files locked by a computer virus.

Did this affect CCWM's ability to provide services? No, we continue to provide high-quality services to its community.

What information was potentially affected? What Information Was Involved? This matter did not affect our Electronic Health Record, donor, or payroll platforms. The majority of the files that were copied were unstructured non-profit operations and governance files. However, some files also contain information about clients of CCWM, including service details, scheduled sessions, progress notes and discharge summaries, treatment information, and adoption services. In other circumstances, the files may also include name and a unique identifier number, which can include an internally assigned identifier, a state assigned identifier, date of birth, or Social Security number. The files may also include historical volunteer background checks, which contain Social Security numbers. Files may also include certain human resources information, including current and former staff name, Social Security number, driver's license number, and direct deposit information.

Will CCWM send notices directly to individuals to let them know about this matter? Given the nature of the files involved with this matter, apart from individuals with Social Security numbers affected, we will not be able to verify the identities and contact information to let individuals know about this matter directly. When the file review is complete, we will work to locate contact information and reach out to individuals with affected Social Security numbers if verifiable contact information is available. If individuals have concerns, they may use the free resources and guidance in the "Steps Individuals Can Take To Protect Personal Information" section below.

Has CCWM learned of any instances of identity theft, fraud, or embarrassment involving this matter? CCWM has no indication of an individual experiencing verified identity theft, fraud, or embarrassment as a result of this incident.

What is CCWM doing in response to this incident? We are evaluating our technical measures and processes to further enhance our cyber security practices. We are also notifying affected individuals and providing resources to help individuals protect information.

Why did it take so long to put out this notice? When incidents like this happen to organizations, they are required by federal and state regulations to complete an investigation. Technical investigations are very complex and take time to complete. After the technical investigation is complete, regulations require organizations to identify the specific types of information in the involved files. This type of review is a time and resource intensive process.

What is CCWM doing to protect my information? We take this event and the security of information in our care very seriously. We have security measures in place designed to protect the files on our systems. While no safeguards can fully prevent all cybersecurity incidents, we are evaluating our technical measures and processes to further enhance our cyber security practices. We will also continue to assess and update security measures and the training of team members to safeguard the privacy and security of information in our care.

Was law enforcement notified? Federal law enforcement was notified of this event.

Is the computer network safe? Yes, the computer network was reviewed and confirmed to be secure.

STEPS INDIVIDUALS CAN TAKE TO PROTECT PERSONAL INFORMATION

Monitor Relevant 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 a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their 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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any 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 a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of 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 they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax—www.equifax.com; 1-888-298-0045; and P.O. Box 105788 Atlanta, GA 30348-5788
Experian—www.experian.com; 1-888-397-3742; and P.O. Box 9554, Allen, TX 75013
TransUnion—www.transunion.com; 1-800-916-8800; and P.O. Box 160, Woodlyn, PA 19094

For loved ones that may have recently passed, individuals may also place a "deceased – do not issue credit" flag on the loved one's credit file. Only one consumer reporting bureau needs to be notified, and it will notify the other two major consumer reporting bureaus. Individuals may complete this process using the information provided by the credit bureaus at the below websites:

Equifax: https://www.equifax.com/personal/help/article-list/-/h/a/relative-death-contact-credit-bureaus
Experian: https://www.experian.com/blogs/ask-experian/reporting-death-of-relative/
TransUnion: https://www.transunion.com/blog/credit-advice/reporting-a-death-to-tu

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect their personal information by contacting the consumer reporting bureaus, the Federal Trade Commission,

or their 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement.

STEPS INDIVIDUALS CAN TAKE TO PROTECT THEIR MINOR DEPENDENTS' PERSONAL INFORMATION

Monitor Relevant Accounts

Typically, credit reporting agencies do not have a credit report in a minor's name. To find out if your minor dependent has a credit report or to request a manual search for your minor dependent's Social Security number, each credit bureau has its own process. To learn more about these processes or request these services, you may contact the credit bureaus by phone or in writing or you may visit or contact the below credit bureaus.

Equifax— https://www.equifax.com/personal/education/identity-theft/articles/-/learn/child-identity-theft/; 1-888-298-0045; and P.O. Box 105788 Atlanta, GA 30348-5788
Experian— https://www.experian.com/help/minor-request.html; 1-888-397-3742; and P.O. Box 9554, Allen, TX 75013
TransUnion— https://www.transunion.com/fraud-victim-resources; 1-800-916-8800; and P.O. Box 160, Woodlyn, PA 19094

To request information about the existence of a credit file in your minor dependent's name, search for your dependent's Social Security number, place a security freeze on your dependent's credit file, place a fraud alert on your dependent's credit report (if one exists), or request a copy of your dependent's credit report you may be required to provide some or all the following information:

- A copy of your driver's license or another government issued identification card, such as a state identification card, etc.;
- Proof of your address, such as a copy of a bank statement, utility bill, insurance statement, etc.;
- A copy of your minor dependent's birth certificate;
- A copy of your minor dependent's Social Security card;
- Your minor dependent's full name, including middle initial and generation, such as JR, SR, II, III, etc.;
- Your minor dependent's date of birth; and
- Your minor dependent's previous addresses for the past two years.

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps individuals can take to protect their 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. Individuals and/or their minor dependent have the right to file a police report if their minor dependent ever experiences identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, an individual or minor dependent will likely need to provide some proof that the minor dependent has been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and relevant state Attorney General.