

Nicholas A. Kurk
Direct Dial: 312-642-6738
E-mail: nkurk@mcdonaldhopkins.com

July 13, 2023

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

Brian E. Frosh
Office of the Maryland Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: ChildNet Youth and Family Services, Inc. – Incident Notification

Dear Mr. Frosh:

McDonald Hopkins PLC represents ChildNet Youth and Family Services, Inc. (“ChildNet”). I am writing to provide notification of an incident at ChildNet that may affect the security of personal information of one (1) Maryland resident. ChildNet’s investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, ChildNet does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On or around April 24, 2023, an unauthorized individual obtained access to a third-party vendor used by ChildNet. Upon learning of the issue, ChildNet immediately launched an investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of situations. ChildNet devoted considerable time and effort to determine what information was potentially accessed or acquired by the unauthorized individual. Based on this comprehensive investigation and review, ChildNet determined on June 26, 2023 that the potentially impacted information included a limited amount of personal information, including the affected residents’ full names, addresses, and Social Security numbers. The forensic investigation concluded that there was no evidence that this incident impacted anything other than data stored at ChildNet’s vendor.

ChildNet has no indication that any information has been misused. Nevertheless, out of an abundance of caution, ChildNet wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected resident against identity fraud. ChildNet is providing the affected resident with notification of this incident commencing on or about July 14, 2023 in substantially the same form as the letter attached hereto. ChildNet is providing the affected residents with 12 months of complimentary credit monitoring services and is advising the affected residents to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. ChildNet is

July 13, 2023

Page 2

advising the affected residents about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. The affected residents are also being provided with the contact information for the consumer reporting agencies, the Maryland Attorney General, and the Federal Trade Commission.

At ChildNet, protecting the privacy of personal information is a top priority. ChildNet is committed to maintaining the privacy of personal information in its possession and with its vendors, and has taken many precautions to safeguard it. ChildNet continually evaluates and modifies its practices and internal controls to enhance the security and privacy of the personal information.

Should you have any questions concerning this notification, please contact me at (312) 642-6738 or nkurk@mcdonaldhopkins.com. Thank you for your cooperation.

Very truly yours,



Nicholas A. Kurk

Encl.



Redacted

July 14, 2023

NOTICE OF DATA BREACH

Dear **Redacted**

We are writing with important information regarding a recent security incident. The privacy and security of the personal information we maintain is of the utmost importance to ChildNet Youth and Family Services, Inc. ("ChildNet"). As such, we wanted to provide you with information about the incident, inform you about the services we are providing to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

We recently learned that, on or around April 24, 2023, an unauthorized individual obtained access to data maintained by our third-party vendor, **Redacted**. **We have no evidence that this incident impacted anything other than data stored at our vendor, Redacted**. For example, there has been no evidence to suggest any unauthorized access to our email systems, our network or shared drives, any health or medical information, or any other data stored at any of our other vendors or partners.

What We Are Doing.

Upon learning of the issue, we immediately commenced a prompt and thorough investigation. As part of our investigation, we have been working very closely with external cybersecurity professionals experienced in handling these types of incidents. After an extensive forensic investigation and manual document review, we discovered on June 26, 2023 that documents containing your information stored by ChildNet on Paycom's platform were potentially accessed or acquired by the unauthorized individual.

What Information Was Involved?

The potentially impacted documents contained some of your personal information, specifically your name, address, and Social Security number.

What You Can Do.

To protect you from potential misuse of your information, we are providing you with **complimentary** access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services. These services provide you with alerts for 12 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 that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company. For more information on identity theft

prevention and instructions on how to activate your complimentary membership, please see the additional information provided in this letter.

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.

We all share in the frustration that incidents such as this can occur. We remain fully 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 to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, representatives are available for 90 days from the date of this letter, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call the Help Line at **Redacted** and supply the fraud specialist with your unique code listed above.

Sincerely,

Kathy Hughes
President/CEO
ChildNet Youth and Family Services, Inc.

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary 12 Month Credit Monitoring.

In response to the incident, 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 12 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. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to **<https://secure.identityforce.com/benefit/childnet>** 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.

It is always advisable and good practice to review all of your personal account passwords and enable multifactor authentication wherever available.

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.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; <https://ag.ny.gov/consumer-frauds-bureau/identity-theft>; Telephone: 800-771-7755 (TDD/TYY Support: 800-788-9898); Medicare Fraud Control Unit Direct Line: 212-417-5397.

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.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.