

Christine Czuprynski
Direct Dial: 248.220.1360
E-mail: cczuprynski@mcdonaldhopkins.com

August 30, 2022

VIA EMAIL (Idtheft@oag.state.md.us)
Office of the Maryland Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Family Resource Agency – Incident Notification

Dear Sir or Madam:

McDonald Hopkins PLC represents Family Resource Agency. I am writing to provide notification of an incident at Family Resource Agency (“FRA”) that may affect the security of personal information of approximately one (1) Maryland resident. FRA’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, FRA does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On July 30, 2022, FRA detected a ransomware infection on its network. Upon learning of the issue, FRA contained the threat by disabling all unauthorized access to its network, restored encrypted data, and immediately commenced a prompt and thorough investigation with the assistance of third-party cybersecurity professionals experienced in handling these types of incidents. Though the investigation is ongoing, FRA determined on August 5, 2022 that the perpetrator may have removed certain files and folders from its network. On August 22, 2022, after reviewing and updating the addresses in FRA’s records, FRA determined that the potentially acquired information included some personal information of one Maryland resident, including name, Social Security number, driver's license number, and medical information.

We have no evidence that any information has been misused. Nevertheless, out of an abundance of caution, we want to make this office and the impacted Maryland resident aware of the incident. FRA is providing notification of this incident on August 26, 2022, in substantially the same form as the notification letter attached hereto. FRA is advising the affected residents about the process for placing fraud alerts and/or security freezes on their credit files and obtaining free credit reports. FRA is also offering complimentary credit monitoring to the impacted residents. The residents are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At FRA, protecting the privacy of personal information is a top priority. FRA is committed to maintaining the privacy of personal information in its possession and has taken many

August 30, 2022

Page 2

precautions to safeguard it. FRA continually evaluates and modifies its practices and internal controls to enhance the security and privacy of personal information.

Should you have any questions regarding this notification, please contact me at (248) 220-1360 or cczuprynski@mcdonaldhopkins.com. Thank you for your cooperation.

Sincerely,

A handwritten signature in black ink, appearing to read "Christine N. Czuprynski", with a stylized, flowing script.

Christine N. Czuprynski

Encl.



IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

Dear [REDACTED],

The privacy and security of the personal information we maintain is of the utmost importance to Family Resource Agency. We're writing with important information regarding a recent data security incident that involved some of your information. We want to provide you with information about the incident, explain the services we are providing to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

On July 30, 2022, Family Resource Agency detected that a ransomware infection began encrypting files stored on our network.

What We Are Doing.

Upon learning of this issue, we contained the threat by disabling unauthorized access to our network and 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. Though the investigation is ongoing, we recently discovered that the incident likely resulted in the unauthorized acquisition of certain files and folders from our network. On August 5, 2022, we determined that the impacted files contain personal information belonging to current and former employees.

What Information Was Involved.

The impacted files likely contained some of your personal information, specifically your [REDACTED].

What You Can Do.

We have no evidence that any of your information has been misused. Nevertheless, out of an abundance of caution, we want to make you aware of the incident. To protect you from potential misuse of your information, we are offering a complimentary one-year membership of Experian IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your complimentary one-year 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.

Please accept our apologies that this incident occurred. 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, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [REDACTED]. 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, 9:00 a.m. to 6:30 p.m. Eastern time, excluding major U.S. holidays.

Sincerely,

Family Resource Agency

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary 12-Month Credit Monitoring.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: [REDACTED] (Your code will not work after this date.)
 - a. Enrollments must occur by no later than 5:59pm CT.
2. VISIT the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
3. PROVIDE the Activation Code: [REDACTED]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-288-8057. Be prepared to provide engagement number [REDACTED] as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **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.
- **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.

**Activate your membership today at <https://www.experianidworks.com/3bcredit>
or call 877-288-8057 to register with the activation code above.**

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8057.

* 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 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 30348-5069
<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

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 30348-5788

<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.

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.

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.