

September 20, 2022

**VIA ONLINE SUBMISSION**

Attorney General Aaron Frey  
SECURITY BREACH NOTIFICATION  
6 State House Station  
Augusta, ME 04333

RE: Data Incident Notification

Dear Attorney General Frey:

Our firm represents Rock County Human Services Department (“Rock County HSD”). Rock County HSD hereby formally submits notification of a recent data incident pursuant to Maine Rev. Stat. Tit. 10, Section 210-B-1346 et seq. Rock County HSD reserves the right to supplement this notice with any significant details learned subsequent to this submission. By providing this notice, Rock County HSD does not waive any rights or defenses regarding the applicability of Maine law, including the applicability of Maine Rev. Stat. Tit. 10, Section 210-B-1346 et seq., the applicability of any other laws of this or any other state, or the existence of personal jurisdiction over Rock County HSD.

Around June 14, 2022, Rock County HSD discovered a business email compromise that was the result of a phishing email campaign dated around February 28, 2022, that targeted Rock County HSD employees (the “Incident”). After discovering the Incident, the Rock County HSD engaged a team of third-party cybersecurity experts to work alongside inhouse experts to launch an investigation and fortify Rock County HSD’s systems. After reviewing the results of its investigation and assessing what information could have potentially been affected by the business email compromise, Rock County HSD determine that personal information and personal health information in Rock County HSD’s email may have been accessed and/or acquired during the Incident. Additionally, Rock County HSD notified law enforcement and this notice was not delayed by law enforcement.

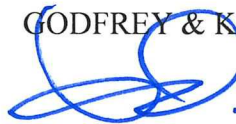
At this time, Rock County HSD does not have any evidence of the misuse of any personal information or personal health information. In light of the foregoing and out of an abundance of caution, Rock County HSD has decided to notify your office (via this letter) and the one (1) Maine resident potentially affected by this Incident via U.S. Mail on or about September 13, 2022. A sample notification letter to the affected resident is attached hereto as Exhibit A.

Attorney General Aaron Frey  
September 20, 2022  
Page 2

Rock County HSD takes the security of personal information seriously. Rock County HSD has taken further steps to bolster the security of its mail systems including a department-wide password reset, extension and deployment of additional sophisticated geo-fencing, and creation of a plan for bolstering monthly phishing and other cybersecurity training for employees, in addition to accelerating existing plans to implement network monitoring programs to further protect email. In addition, Rock County HSD has retained Kroll to provide notice to affected individuals and Experian to provide free identity theft and credit monitoring services.

Sincerely,

GODFREY & KAHN, S.C.



Lillie Conrad

LLC

**EXHIBIT A**

**Sample Notification Letter**



Rock County  
Human Services Department  
P.O. Box 1649  
Janesville, WI 53547-1649  
www.co.rock.wi.us/hsd



<<Date>> (Format: Month Day, Year)

Parent or Guardian of

<<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>

<<address\_1>>

<<address\_2>>

<<city>>, <<state\_province>> <<postal\_code>>

<<country>>

**RE: Notice of Data Breach. Please read this entire letter.**

Dear Parent or Guardian of <<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>,

Rock County Human Services Department recently discovered an incident that may affect the security of your minor's personal information and or personal health information. We want to provide you with information about the incident, steps we are taking in response, and steps you may take to guard against identity theft and fraud, should you feel it is appropriate to do so.

**What Happened?** Around June 14, 2022, Rock County Human Services Department ("Department") discovered a cybersecurity incident during which a bad actor accessed select data in our email. The cybersecurity incident involved what is known as a business email compromise, during which a bad actor deployed a phishing email campaign dated around February 28, 2022 that targeted the Department's employees. We believe that access to our email was limited, as was the impact to the Department's operations. Employees are working as normal and consumers can access care as they always have. After discovering the incident, the Department engaged a team of third-party cybersecurity experts to work alongside inhouse experts to launch an investigation and fortify our systems. Additionally, we notified law enforcement and this notice was not delayed by law enforcement.

While you might not be a client of the Department, you are receiving this notice because during the third-party expert review of this matter, we discovered the Department had one email with data about current and former participants in and applicants or requested enrollees to the Children's Long-Term Support ("CLTS") program that was improperly shared by the Wisconsin Department of Health Services with one of our employees and the employee's email was potentially accessed as noted above.

Importantly, the Rock County Human Services Department does not have evidence that any fraud or identity theft with regard to the persons receiving this letter has occurred. Because we value transparency and your security and privacy, we are providing this notification as your minor's personal information and or personal health information was affected.

**What Information Was Involved?** The personal information about your minor affected by this incident includes your minor's: <<b2b\_text\_1 (data elements)>><<b2b\_text\_2 (data elements cont.)>>.

**What Are We Doing?** We take the protection of personal information and personal health information seriously and are taking steps to prevent a similar occurrence. In addition to providing this notice, communicating with law enforcement and conducting a full investigation of the incident, we took a series of measures to further secure our email systems following the incident. These measures include a department-wide password reset, extension and deployment of additional sophisticated geo-fencing, and creation of a plan for bolstering our monthly phishing and other cybersecurity trainings for employees. Additionally, we accelerated existing plans to implement network monitoring programs that will further protect our email.

We understand that this is likely very concerning, particularly for our customers utilizing our programs and services. We're committed to supporting you and will be reaching out directly to all impacted individuals with guidance and complimentary credit monitoring, should it be of interest. Impacted individuals will receive a notice in the mail. Please note: we are sending this notice to the last address provided for your minor. If your have an updated address for your minor, please let us know and we will send another notice.

To help protect your minor's identity, we are offering a complimentary 12-month membership of Experian's® IdentityWorks<sup>SM</sup>. This product provides superior identity detection and resolution of identity theft. To activate this membership and start monitoring your minor's personal information please follow the steps below:

- Ensure that you **enroll by:** <<b2b\_text\_6 (date)>> **at 5:59pm CT** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/minorplus>
- Provide your **activation code:** <<Activation Code s\_n>>
- Provide your minor's information when prompted

If you have questions about the product, need assistance with identity restoration for your minor or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877.288.8057 by <<b2b\_text\_6 (date)>> **at 5:59pm CT**. Be prepared to provide engagement number <<b2b\_text\_3 (engagement #)>> as proof of eligibility for the identity restoration services by Experian.

#### **ADDITIONAL DETAILS REGARDING THE 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:**

A credit card is not required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks for your minor:

- **Social Security Number Trace:** Monitoring to determine whether enrolled minors in your household have an Experian credit report. Alerts of all names, aliases and addresses that become associated with your minor's Social Security Number (SSN) on the Experian credit report.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE<sup>TM</sup>:** Receive the same high-level of Identity Restoration support even after the Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance\*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your minor's information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 877-288-8057. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to your minor for 12 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at [www.ExperianIDWorks.com/restoration](http://www.ExperianIDWorks.com/restoration). You will also find self-help tips and information about identity protection at this site.

**What You Can Do.** Please review the enclosed *Information about Identity Theft Protection* for additional information on how to protect against identity theft and fraud. You may also take advantage of the complimentary identity protection services being offered for your minor.

**For More Information.** We sincerely regret any inconvenience or concern caused by this incident. If you have further questions or concerns, please call 855-544-2848, Monday through Friday from 8 am to 5:30 pm Central, excluding major US holidays.

Sincerely,



Lisa Moore-Kelty, Records Manager and HIPAA Privacy Officer  
Rock County – Human Services Department

\* 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.

## Information about Identity Theft Protection

### Monitor Your Accounts

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at [www.annualcreditreport.com](http://www.annualcreditreport.com), by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at [www.annualcreditreport.com](http://www.annualcreditreport.com)) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

#### **Equifax®**

P.O. Box 740241  
Atlanta, GA 30374-0241  
1-800-685-1111  
[www.equifax.com](http://www.equifax.com)

#### **Experian**

P.O. Box 9701  
Allen, TX 75013-9701  
1-888-397-3742  
[www.experian.com](http://www.experian.com)

#### **TransUnion®**

P.O. Box 1000  
Chester, PA 19016-1000  
1-800-888-4213  
[www.transunion.com](http://www.transunion.com)

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

### Credit Freeze

You have the right to put a security freeze, also known as a credit freeze, on your credit file, so that no new credit can be opened in your name without the use of a Personal Identification Number (PIN) that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. Should you wish to place a credit freeze, please contact all three major consumer reporting agencies listed below.

#### **Equifax**

P.O. Box 105788  
Atlanta, GA 30348-5788  
1-800-685-1111  
[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

#### **Experian**

P.O. Box 9554  
Allen, TX 75013-9554  
1-888-397-3742  
[www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html)

#### **TransUnion**

P.O. Box 2000  
Chester, PA 19016-2000  
1-888-909-8872  
[www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

You must separately place a credit freeze on your credit file at each credit reporting agency. The following information should be included when requesting a credit freeze:

1. Full name, with middle initial and any suffixes;
2. Social Security number;
3. Date of birth (month, day, and year);
4. Current address and previous addresses for the past five (5) years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. Other personal information as required by the applicable credit reporting agency;

If you request a credit freeze online or by phone, then the credit reporting agencies have one (1) business day after receiving your request to place a credit freeze on your credit file report. If you request a lift of the credit freeze online or by phone, then the credit reporting agency must lift the freeze within one (1) hour. If you request a credit freeze or lift of a credit freeze by mail, then the credit agency must place or lift the credit freeze no later than three (3) business days after getting your request.

### Fraud Alerts

You also have the right to place an initial or extended fraud alert on your file at no cost. An initial fraud alert lasts 1-year and 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 7 years. Should you wish to place a fraud alert, please contact any one of the agencies listed below. The agency you contact will then contact the other two credit agencies.

**Equifax**

P.O. Box 105788  
Atlanta, GA 30348-5788  
1-888-766-0008  
[www.equifax.com/personal/  
credit-report-services](http://www.equifax.com/personal/credit-report-services)

**Experian**

P.O. Box 9554  
Allen, TX 75013-9554  
1-888-397-3742  
[www.experian.com/  
fraud/center.html](http://www.experian.com/fraud/center.html)

**TransUnion**

P.O. Box 2000  
Chester, PA 19016-2000  
1-800-680-7289  
[www.transunion.com/fraud-  
victim-resource/place-fraud-alert](http://www.transunion.com/fraud-victim-resource/place-fraud-alert)

**Monitor Your Personal Health Information**

If applicable to your situation, we recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive the regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the website of the California Office of Privacy Protection at [www.privacy.ca.gov](http://www.privacy.ca.gov) to find more information about your medical privacy.

**Additional Information**

You can further educate yourself regarding identity theft and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC.

**The Federal Trade Commission**

600 Pennsylvania Avenue, NW  
Washington, DC 20580  
1-877-ID-THEFT (1-877-438-4338)  
TTY: 1-866-653-4261  
[www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)