JacksonLewis

Jackson Lewis P.C.
200 Connell Drive, Suite 2000
Berkeley Heights NJ 07922
(908) 795-5200 Main
(908) 464-2614 Fax
jacksonlewis.com

Via Data Breach Portal

April 17, 2023

Attorney General Aaron Frey
ME Office of Attorney General
6 State House Station
Augusta, ME 04333

Re: Fortra Data Incident – Addendum to Previous Notification

Dear Attorney General Frey:

On behalf of our client, CHSPSC, LLC ("CHSPSC"), we are writing to provide an addendum to the data incident notification we submitted to your office, on or about March 8, 2023, regarding the security incident experienced by Fortra, LLC ("Fortra") (the "Fortra Incident").[1]

CHSPSC has worked through approximately 99% of the files believed to have been compromised by the Fortra Incident. To date, CHSPSC has identified 1,173,555 individuals whose personal information may have been impacted by the Fortra Incident, of which 86 are believed to be Maine residents. We will continue working through the remainder of the files and will update you with any material changes to this information.

Furthermore, CHSPSC has commenced the notification process and begun mailing notices to affected individuals. Enclosed is the specimen letter being provided to affected individuals so they can take steps to minimize the risk that their information will be misused.

If you require any additional information on this matter, please do not hesitate to contact me.

Very truly yours,

JACKSON LEWIS PC

Joseph. J. Lazzarotti

Joseph J. Lazzarotti

Encl.

[1] CHSPSC is a professional services company that provides services to hospitals and clinics affiliated with Community Health Systems, Inc. ("CHSPSC Affiliates"). Please note that by providing this letter CHSPSC and CHSPSC Affiliates are not agreeing to the jurisdiction of the State of Maine, or waiving its right to challenge jurisdiction in any subsequent actions. We are providing this addendum as a courtesy.

CHSPSC, LLC
Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

March 24, 2023

J1980-L02-0000001 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L02 ADULT PATIENT
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

RE: Important Security Notification
Please read this entire letter.

Dear Sample A. Sample:

I'm writing to inform you of a security incident experienced by Fortra, LLC ("Fortra"), which Fortra reported occurred between January 28, 2023 and January 30, 2023 that resulted in the unauthorized disclosure of your personal information. Fortra is a cybersecurity firm that contracts with CHSPSC, LLC ("CHSPSC") to provide a secure file transfer software called GoAnywhere. CHSPSC is a professional services company that provides services to hospitals and clinics affiliated with Community Health Systems, Inc. ("CHSPSC Affiliates"). You are receiving this letter as either a current or former patient of one or more of CHSPSC Affiliates, whose personal information was affected as a result of Forta's incident. For a list of hospitals that are CHSPSC Affiliates and links to their websites to help you identify which CHSPSC Affiliates you may have received services from, please visit https://www.chs.net/serving-communities/locations/#USMap.

What Happened?
Fortra informed us it became aware of the incident the evening of January 30, 2023 and took impacted systems offline on January 31, 2023, stopping the unauthorized party's ability access the system. According to Fortra, the unauthorized party used a previously unknown vulnerability to gain access to Fortra's systems, specifically Fortra's GoAnywhere file transfer service platform, compromising sets of files throughout Fortra's platform.

CHSPSC received this information from Fortra on February 2, 2023, and immediately began its own investigation of potential impact of the Fortra incident on CHSPSC Affiliate personal information. CHSPSC has determined at this point in its investigation that your personal information was disclosed to the unauthorized party as a result of the Fortra incident.

What Information Was Involved?
The types of personal information may have included your full name, address, medical billing and insurance information, certain medical information such as diagnoses and medication, and demographic information such as date of birth and Social Security number.

What We Are Doing.
Both CHSPSC and Fortra have been in contact with law enforcement, including the Federal Bureau of Investigation ("FBI") and the Cybersecurity and Infrastructure Security Agency ("CISA"), and are supporting law enforcement's investigation.

To protect against an incident like this from reoccurring, Fortra informed us that it has deleted the unauthorized party's accounts, rebuilt the secure file transfer platform with system limitations and restrictions, and produced a patch for the software. CHSPSC has also implemented additional security measures, including immediate steps to implement measures to harden the security of CHSPSC's use of the GoAnywhere platform.

CHSPSC is making available ID restoration and credit monitoring services for 24 months, at no cost to you, through Experian to all potentially affected individuals who enroll. If you would like to enroll in these services or have questions related to this incident, CHSPSC has established a toll-free response line that can be reached at 800-906-7947, and is available Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays). If you are interested in enrolling in these services, the deadline to enroll is June 30, 2023. Be prepared to provide your engagement number B086999. You may also enroll online using the instructions provided further below.

This notice also provides other precautionary measures you can take to protect your personal information, including placing a fraud alert and security freeze on your credit files and 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. See "What else can you do to protect your personal information?" below.

What You Can Do.
The attached sheet describes steps you can take to protect your identity and personal information, such as checking your account statements and credit report. To help protect your identity, we are offering a complimentary 24-month membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: **June 30, 2023** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: **https://www.experianidworks.com/plus**
- Provide your **activation code**: **79GT7X5Q66**

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 **800-906-7947** by **June 30, 2023.** Be prepared to provide engagement number **B086999** as proof of eligibility for the identity restoration services by Experian.

For More Information.
Please be assured we are committed to protecting personal information. We share your frustration with this security incident, and we apologize for any inconvenience it this may cause you. We are working very hard to limit the impact of the Fortra incident on you. If you have further questions or concerns, please call 800-906-7947. Please refer to hours and engagement number above.

Sincerely,

Beth Witte

Beth Witte, SVP, Chief Compliance & Privacy Officer

ADDITIONAL RECOMMENDED STEPS

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:

- **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 file for indicators of fraud.
- **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™**: You receive the same high-level of Identity Restoration support even after your 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 information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at **800-906-7947**. 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 you for 24 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. You will also find self-help tips and information about identity protection at this site.

* 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.

What else can you do to protect your personal information?

We recommend you remain vigilant and consider taking the following steps to avoid identity theft, obtain additional information, and protect your personal information:

Order your free credit report at annualcreditreport.com, call toll-free at 877.322.8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's (FTC) website at www.ftc.gov. When you receive your credit report, review the entire report carefully. Look for any inaccuracies and/or accounts you don't recognize and notify the credit bureaus as soon as possible in the event there are any. You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information.

Place a fraud alert on your credit file. A fraud alert helps protect you against an identity thief opening new credit in your name. With this alert, when a merchant checks your credit history when you apply for credit, the merchant will receive a notice that you may be a victim of identity theft and to take steps to verify your identity. You also have the right to place a security freeze on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. You can place a fraud alert or request a security freeze by contacting the credit bureaus. The credit bureaus may require that you provide proper identification prior to honoring your request.

Equifax	Experian	TransUnion
P.O. Box 740256	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016-2000
800-525-6285	888-397-3742	1-800-916-8800
www.equifax.com	www.experian.com	www.transunion.com

Remove your name from mailing lists of pre-approved offers of credit for approximately six months.

If you aren't already doing so, please pay close attention to all bills and credit card charges you receive for items you did not contract for or purchase. Review all your bank account statements frequently for checks, purchases, or deductions not made by you. Note that even if you do not find suspicious activity initially, you should continue to check this information periodically since identity thieves sometimes hold on to stolen personal information before using it.

The FTC offers consumer assistance and educational materials relating to identity theft, privacy issues, and how to avoid identity theft. You may also obtain information about fraud alerts and security freezes from the consumer reporting agencies, your state Attorney General, and the FTC. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General, and/or the FTC. You can learn more about how to protect yourself from becoming an identity theft victim (including how to place a fraud alert or security freeze) by contacting the FTC at 877.IDTHEFT (1.877.438.4338), or www.ftc.gov/idtheft. The mailing address for the FTC is: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580.

For District of Columbia Residents: You can obtain additional information about steps to take to avoid identity theft from the Office of the Attorney General for the District of Columbia, 441 4th Street, NW, Washington, DC 200001, 202.727.3400, oag.dc.gov.

For Maryland Residents: You can obtain information about steps you can take to help prevent identity theft from the Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888.743.0023, oag.state.md.us.

For New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to

have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit see a summary of rights or visit or ftc.gov.

In addition, New Mexico consumers may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have the right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. For more information about obtaining a security freeze, go to https://consumer.ftc.gov/articles/what-know-about-credit-freezes-fraud-alerts.

For New York Residents: You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information: 1) New York Attorney General, 212.416.8433 or https://ag.ny.gov/internet/resource-center; or 2) NYS Department of State's Division of Consumer Protection, 800.697.1220 or https://dos.ny.gov/consumer-protection.

For North Carolina Residents: You can obtain information about steps you can take to help prevent identity theft from the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, 1.877.566.7226, ncdoj.gov.

For Rhode Island Residents: You may contact and obtain information from and/or report identity theft to your state attorney general at:

Rhode Island Attorney General's Office
150 South Main Street
Providence, RI 02903
Phone: 401.274.4400
Website: www.riag.ri.gov

You have the right to obtain a copy of the applicable police report, if any, relating to this incident.