Notice of Data Incident

[https://www.easterseals.com/in-sw/] Easterseals Rehabilitation Center Evansville ("ESRC") is writing to inform you of a recent data security incident that may have resulted in unauthorized access to some individuals' sensitive personal information. This notice is intended to provide details about the incident, steps we are taking in response, and resources available to help protect against the potential misuse of sensitive personal information.

What Happened?

On August 28, 2024, ESRC experienced a network disruption that impacted the functionality and access of certain systems. Upon discovery of this incident, ESRC immediately disconnected all access to the network and promptly engaged a specialized third-party cybersecurity firm and IT personnel to assist with securing the environment, as well as, to conduct a comprehensive forensic investigation to determine the nature and scope of the incident. The forensic investigation was completed on October 14, 2024. ESRC is completing its review of the compromised data and identifying individuals whose personal information may have been potentially compromised for the purposes of mailing out notice letters. A formal notice letter is currently being prepared and will be sent to those who have had their sensitive information impacted.

<u>What Information was Involved?</u> Based on the investigation, the following information related to you may have been subject to unauthorized access: social security number, health insurance information, medical information, and for some, financial information.

What We Are Doing: Data privacy and security is among ESRC's highest priorities, and we are committed to doing everything we can to protect the privacy and security of the personal information in our care. Upon discovery of the Incident, ESRC moved quickly to investigate and respond to the Incident and assessed the security of its systems. Specifically, ESRC engaged a specialized cybersecurity firm and IT personnel to conduct a forensic investigation to determine the nature and scope of the Incident. Additionally, ESRC took the following steps, including, but not limited to deploying an industry leading endpoint security software and enhancing our privacy and cybersecurity posture.

ESRC will be offering complimentary credit monitoring and identity theft protection services to those impacted individuals. Notification letters will be sent to those impacted individuals with the information to enroll in the credit monitoring services. ESRC strongly encourages all identified individuals to register for this free service.

What You Can Do: We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file. Please review the enclosed Steps You Can Take to Help Protect Your Information, to learn more about how to protect against the possibility of information misuse.

Substitute Notice

For More Information:

If you have any questions or concerns not addressed in this letter, please call 1-800-405-6108 (toll free) Monday through Friday, during the hours of 8:00 a.m. and 8:00 p.m. Eastern Standard Time (excluding U.S. national holidays).

ESRC sincerely regrets any concern or inconvenience this matter may cause and remains dedicated to ensuring the privacy and security of all information in our control.

Sincerely,

Kelly Schneider

Kelftet

President & CEO, Easterseals Rehabilitation Center Evansville

ADDITIONAL RESOURCES TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts

We recommend that you remain vigilant for incidents of fraud or identity theft by regularly reviewing your credit reports and financial accounts for any suspicious activity. You should contact the reporting agency using the phone number on the credit report if you find any inaccuracies with your information or if you do not recognize any of the account activity.

You may obtain a free copy of your credit report by visiting www.annualcreditreport.com, calling toll-free at 1-877-322-8228, or by mailing a completed Annual Credit Report Request Form (available at 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 for a fee by contacting one or more of the three national credit reporting agencies.

You have rights under the federal Fair Credit Reporting Act (FCRA). The FCRA governs the collection and use of information about you that is reported by consumer reporting agencies. You can obtain additional information about your rights under the FCRA by visiting https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act.

Credit Freeze

You have the right to add, temporarily lift and remove a credit freeze, also known as a security freeze, on your credit report at no cost. A credit freeze prevents all third parties, such as credit lenders or other companies, whose use is not exempt under law, from accessing your credit file without your consent. If you have a freeze, you must remove or temporarily lift it to apply for credit. Spouses can request freezes for each other as long as they pass authentication. You can also request a freeze for someone if you have a valid Power of Attorney. If you are a parent/guardian/representative you can request a freeze for a minor 15 and younger. To add a security freeze on your credit report you must make a separate request to each of the three national consumer reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The following information must be included when requesting a security freeze: (i) full name, with middle initial and any suffixes; (ii) Social Security number; (iii) date of birth (month, day, and year); (iv) current address and any previous addresses for the past five (5) years; (v) proof of current address (such as a copy of a government-issued identification card, a recent utility or telephone bill, or bank or insurance statement); and (vi) other personal information as required by the applicable credit reporting agency.

Fraud Alert

You have the right to add, extend, or remove a fraud alert on your credit file at no cost. A fraud alert is a statement that is added to your credit file that will notify potential credit grantors that you may be or have been a victim of identity theft. Before they extend credit, they should use reasonable procedures to verify your identity. Please note that, unlike a credit freeze, a fraud alert only notifies lenders to verify your identity before extending new credit, but it does not block access to your credit report. Fraud alerts are free to add and are valid for one year. Victims of identity theft can obtain an extended fraud alert for seven years. You can add a fraud alert by sending your request to any one of the three national reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The agency you contact will then contact the other credit agencies.

Federal Trade Commission

For more information about credit freezes and fraud alerts and other steps you can take to protect yourself against identity theft, you can contact the Federal Trade Commission (FTC) at 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), 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.

Substitute Notice

You should also report instances of known or suspected identity theft to local law enforcement and the Attorney General's office in your home state and you have the right to file a police report and obtain a copy of your police report.

Contact Information

Below is the contact information for the three national credit reporting agencies (Experian, Equifax, and TranUnion) if you would like to add a fraud alert or credit freeze to your credit report.

Credit	Access Your	Add a Fraud Alert	Add a Security Freeze
Reporting	Credit Report		
Agency			
Experian	P.O. Box 2002	P.O. Box 9554	P.O. Box 9554
	Allen, TX 75013-9701	Allen, TX 75013-9554	Allen, TX 75013-9554
	1-866-200-6020	1-888-397-3742	1-888-397-3742
	www.experian.com	https://www.experian.com/fraud/ce	www.experian.com/freeze/center.ht
		nter.html	ml
Equifax	P.O. Box 740241	P.O. Box 105069	P.O. Box 105788
	Atlanta, GA 30374-0241	Atlanta, GA 30348-5069	Atlanta, GA 30348-5788
	1-866-349-5191	1-800-525-6285	1-888-298-0045
	www.equifax.com	www.equifax.com/personal/credit-	www.equifax.com/personal/credit
	_	report-services/credit-fraud-alerts	report-services
TransUnion	P.O. Box 1000	P.O. Box 2000	P.O. Box 160
	Chester, PA 19016-1000	Chester, PA 19016	Woodlyn, PA 19094
	1-800-888-4213	1-800-680-7289	1-800-916-8800
	www.transunion.com	www.transunion.com/fraud-alerts	www.transunion.com/credit-freeze

Iowa and Oregon residents are advised to report suspected incidents of identity theft to local law enforcement, to their respective Attorney General, and the FTC.

Massachusetts residents are advised of their right to obtain a police report in connection with this incident.

District of Columbia residents are advised of their right to obtain a security freeze free of charge and can obtain information about steps to take to avoid identity theft by contacting the FTC (contact information provided above) and the Office of the Attorney General for the District of Columbia, Office of Consumer Protection, at 400 6th St. NW, Washington, D.C. 20001, by calling the Consumer Protection Hotline at (202) 442-9828, by visiting https://oag.dc.gov, or emailing at consumer.protection@dc.gov.

Maryland residents can obtain information about steps they can take to avoid identity theft by contacting the FTC (contact information provided above) or the Maryland Office of the Attorney General, Consumer Protection Division Office at 44 North Potomac Street, Suite 104, Hagerstown, MD 21740, by phone at 1-888-743-0023 or 410-528-8662, or by visiting http://www.marylandattorneygeneral.gov/Pages/contactus.aspx.

New York residents are advised that in response to this incident they can place a fraud alert or security freeze on their credit reports and may report any incidents of suspected identity theft to law enforcement, the FTC, the New York Attorney General, or local law enforcement. Additional information is available at the website of the New York Department of State Division of Consumer Protection at https://dos.nysits.acsitefactory.com/consumerprotection; by visiting the New York Attorney General at https://ag/ny.gov or by phone at 1-800-771-7755; or by contacting the FTC at www.ftc.gov/bcp/edu/microsites/idtheft/ or https://www.identitytheft.gov/#/.

North Carolina residents are advised to remain vigilant by reviewing account statements and monitoring free credit reports and may obtain information about preventing identity theft by contacting the FTC (contact information

Substitute Notice

provided above) or the North Carolina Office of the Attorney General, Consumer Protection Division at 9001 Mail Service Center, Raleigh, NC 27699-9001, or visiting www.ncdoj.gov, or by phone at 1-877-5-NO-SCAM (1-877-566-7226) or (919) 716-6000.

Rhode Island residents are advised that they may file or obtain a police report in connection with this incident and place a security freeze on their credit file and that fees may be required to be paid to the consumer reporting agencies.