

## **NOTICE OF DATA BREACH**

**Updated: January 8, 2024**

Stresser and Associates, P.C. is committed to protecting the privacy and security of the personal information we maintain. We are making individuals aware of an incident that may affect the privacy of certain individuals' information. We are providing notice of the incident so that potentially affected individuals may take steps to protect their information, should they feel it appropriate to do so.

**What Happened?** On or about November 28, 2022, we detected suspicious activity on our network and servers. After discovering this, we quickly took steps to evaluate and ensure the security of our systems and operations. Further, we immediately engaged third-party independent cybersecurity experts to conduct an investigation into the incident.

Our investigation determined that an unauthorized actor accessed our systems from November 22, 2022 to November 28, 2022, and potentially obtained some information. We have been in the process of conducting an exhaustive review to identify the potentially impacted individuals whose personal information was included within the files that may have been accessed or removed from our network by an unauthorized actor as a result of the incident. To date, we are not aware of any reports of identity fraud or improper use of personal information as a direct result of this incident. Out of an abundance of caution, we are providing notice of the incident to individuals whose information was potentially impacted and explaining the services we are making available.

**What Information Was Involved?** The potentially impacted data included first and last name, taxpayer identification number, financial account information, including account number and routing number, Social Security number, driver's license number, date of birth, medical information, and/or health insurance information, if it was provided to us.

**What We Are Doing.** The security and privacy of the information contained within our systems is a top priority for us. In response to this incident, we took immediate steps to secure our systems and engaged third-party forensic experts to assist in the investigation. Further, we are implementing additional cybersecurity safeguards, as needed, enhancing our employee cybersecurity training, and improving our cybersecurity policies, procedures, and protocols to help minimize the likelihood of this type of incident occurring again.

**How Will Individuals Know If They Are Affected By This Incident?** Stresser and Associates, P.C. is providing notice to data owners and individuals whose information was determined to be in the affected files in accordance with our legal obligations, to the best of our ability and to the extent we have valid mailing addresses. If an individual does not receive a letter but would like to know if they are affected, they may call 1-833-960-4110.

**For More Information.** For individuals seeking more information or who have questions, please call 1-833-960-4110.

**What You Can Do.** We encourage individuals to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, explanation of benefits forms, and monitoring your free credit reports for suspicious activity and to detect errors. Under U.S. law individuals are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order a free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. Individuals may also contact the three

major credit bureaus directly to request a free copy of their credit report, place a fraud alert, or a security freeze. Contact information for the credit bureaus is below:

### **Placing a Fraud Alert on Your Credit File.**

You may place an initial one-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

### **Consider 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 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.

If you do place a security freeze *prior* to enrolling in any credit monitoring service, 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.

### **Additional Information**

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; [www.identitytheft.gov](http://www.identitytheft.gov); 1-877-ID-THEFT (1-877-438-

4338); and 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. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

### **Protecting Your Medical Information.**

The following practices can provide additional safeguards to protect against medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your “explanation of benefits statement” which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

**Iowa Residents:** You may contact law enforcement or the Iowa Attorney General’s Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, [www.iowaattorneygeneral.gov](http://www.iowaattorneygeneral.gov), Telephone: 515-281-5164.

**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, <https://www.marylandattorneygeneral.gov/>, Telephone: 888-743-0023.

**Massachusetts Residents:** Under Massachusetts law, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

**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.

**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/](http://www.ncdoj.gov/), Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

**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/](http://www.doj.state.or.us/), Telephone: 877-877-9392.

**Washington D.C. Residents:** You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, <https://oag.dc.gov/consumer-protection>, Telephone: 202-442-9828.

**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 [www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf](http://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf) or [www.ftc.gov](http://www.ftc.gov).

**Rhode Island Residents:** You may contact law enforcement, such as the Rhode Island Attorney General's Office, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. You can contact the Rhode Island Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, [www.riag.ri.gov](http://www.riag.ri.gov), 401-274-4400. There was 1 Rhode Island resident impacted by this incident.