Starling Physicians Provides Notice of a Data Incident

Starling Physicians is providing notice of a recent incident that may affect the security of certain information relating to current and former patients.

On March 9, 2021, Staring Physicians became aware of suspicious activity related to an employee's email account. Starling Physicians conducted an investigation and, on May 11, 2021, subsequently determined that an unauthorized actor gained access to an employee's email account between February 20 and March 9, 2021.

Starling Physicians then worked diligently to identify the scope of the impact, the type of information stored in the impacted email account and to whom the information relates. As part of the investigation, Starling Physicians was unable to rule out which specific emails and information stored within the account at the time of the event were accessed. Therefore, Starling Physicians is notifying individuals in an abundance of caution because certain information was present in the impacted email account at the time of the unauthorized access.

While the information involved varies by individual, Starling Physician's investigation determined that the following types of information were potentially present in the email account at the time of the incident: name, date of birth, medical information, health insurance information, financial account information, routing number, and Social Security number.

Starling Physicians takes this incident and the security of personal information in our care seriously. Upon discovering this incident, Starling Physicians took steps to investigate and respond to this incident, assess the security of relevant systems, and notify potentially affected individuals. In response to this event, Starling Physicians is reviewing and enhancing existing policies and procedures. Starling Physicians notified the Department of Health and Human Services of this incident. Starling Physicians is notifying potentially impacted individuals so that they may take further steps to protect their information should they feel it appropriate to do so.

While Starling has no evidence of attempted or actual misuse of anyone's information as a consequence of this incident, please review the below "Steps You Can Take to Help Protect Your Information," which contains information on what individuals can do to safeguard against possible misuse of information.

Starling Physicians understands individuals may have questions about this incident that are not addressed in this notice. Individuals seeking additional information may call our customer service line at (866) 988-3910. Individuals may also write to Starling Physicians at 2110 Silas Deane Highway, Rocky Hill, Connecticut 06067.

Steps You Can Take To Protect Your Personal Information

Starling Physicians encourages individuals to remain vigilant against incidents of identity theft and fraud by reviewing account statements and monitoring free credit reports for suspicious activity and to detect error. Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Individuals may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that 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 an individual is the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should they wish to place a fraud alert, they may contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in an individual's name without their consent. However, individuals should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, an individual cannot be charged to place or lift a credit freeze on their credit report. To request a security freeze, individuals will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should individuals wish to place a fraud alert or credit freeze, they may contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Individuals may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect their personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General.

The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; 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. Individuals can obtain further information on how to file such a complaint by way of the contact information listed above. Individuals have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity

theft, individuals will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and their state Attorney General. This notice has not been delayed by law enforcement.