

**Plastic Surgery Associates of South Dakota, Ltd.**  
Return Mail Processing Center  
P.O. Box 6336  
Portland, OR 97228-6336

<<Mail ID>>

<<Name 1>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<City>><<State>><<Zip>>

<<Country>>

<<Date>>

## **Re: Notice of Data Privacy Incident**

Dear <<Name 1>>:

Plastic Surgery Associates of South Dakota (“Plastic Surgery Associates”) is writing to inform you of an incident that may affect the security of your protected health information. While Plastic Surgery Associates is unaware of any actual or attempted misuse of your information, this letter contains details about the incident and our response, as well as steps you can take to protect your information, should you feel it appropriate to do so.

**What Happened?** On February 12, 2017, Plastic Surgery Associates discovered that some of our systems were infected with ransomware earlier that day. Plastic Surgery Associates immediately began efforts to remove the ransomware, decrypt the affected systems and hired third-party experts to determine what data, if any was subject to unauthorized access as part of the ransomware incident. While the investigation was able to rule out unauthorized access to the majority of our medical records, certain evidence became unavailable during our clean-up efforts. On or about April 24, 2017, we determined that without this evidence, we were unable to rule out unauthorized access to a limited number of patient records. Therefore, in an abundance of caution we are providing you with this notice.

**What Information Was Involved?** We currently have no evidence of any actual or attempted misuse of your information as a result of this incident. However, the files that may have been subject to unauthorized access contained information about you that may have included some combination of your name, Social Security number, driver’s license number/state identification number, credit card/debit card information, medical conditions, diagnosis information, lab results, address, date of birth and health insurance information.

**What We Are Doing.** The confidentiality, privacy, and security of our patient information is one of our highest priorities. We have stringent security measures in place to protect the security of information in our possession. In addition, as part of our ongoing commitment to the security of protected health information in our care, we are working to implement additional safeguards and security measures to enhance the privacy and security of information on our systems. We are also reporting this incident to the U.S. Department of Health and Human Services (HHS).

Securing your personal information is important to us. As a precautionary measure to help better protect your credit file from potential misuse, we have partnered with Equifax<sup>®</sup> to provide its Credit Watch<sup>™</sup> Silver credit monitoring and identity theft protection product for one year at no charge to you. A description of this product is provided in the attached material, which also contains instructions about how to enroll (including your personal activation code).

If you choose to take advantage of this product, it will provide you with a notification of key changes to your Equifax credit file, up to \$25,000 Identity Theft Insurance<sup>1</sup> Coverage, automatic fraud<sup>2</sup> alerts, access to your Equifax credit report and Identity Restoration. If you become a victim of identity theft, an Equifax identity restoration specialist will work on your behalf to help you restore your identity.

Even if you decide not to take advantage of the subscription offer, you may still receive Equifax Identity Restoration in the event that you become victim of identity theft by calling 877-368-4940, 9:00a.m. to 8:00p.m. Eastern, Monday through Friday, before July 20, 2018.

You must complete the enrollment process for Equifax Credit Watch™ Silver by October 25, 2017. We urge you to consider enrolling in this product, at our expense, and reviewing the Additional Resources enclosed with this letter.

***What You Can Do.*** You can review the enclosed *Steps You Can Take to Protect Your Information* for information you can use to better protect against the misuse of your information, should you feel it appropriate to do so. You can enroll in the free credit monitoring being offered by following the instructions provided in the enclosed *Steps You Can Take to Protect Your Information*.

***For More Information.*** We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 800-954-9263 (toll free), Monday through Friday, 8:00 a.m. to 8:00 p.m. CT.

We sincerely regret any inconvenience or concern this incident has caused you.

Sincerely,

A handwritten signature in cursive script that reads "Jodi Pierret". The signature is written in black ink and is positioned above the printed name and title.

Jodi Pierret  
Clinical Manager

## Steps You Can Take to Protect Your Information

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

At no charge, you can also have these credit bureaus place a “fraud alert” on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax  
P.O. Box 105069  
Atlanta, GA 30348  
800-525-6285  
[www.equifax.com](http://www.equifax.com)

Experian  
P.O. Box 2002  
Allen, TX 75013  
888-397-3742  
[www.experian.com](http://www.experian.com)

TransUnion  
P.O. Box 2000  
Chester, PA 19106  
800-680-7289  
[www.transunion.com](http://www.transunion.com)

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer’s credit report without the consumer’s written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. Fees vary based on where you live, but commonly range from \$3 to \$15. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. In order to request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of your state identification card or driver’s license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze  
P.O. Box 105788  
Atlanta, GA 30348  
1-800-685-1111  
[www.freeze.equifax.com](http://www.freeze.equifax.com)

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

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

You can further educate yourself regarding identity theft, security freezes, fraud alerts, and the steps you can take to protect yourself against identity theft and fraud by contacting the Federal Trade Commission or your state Attorney General. The Federal Trade Commission can 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 encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should be reported to law enforcement, the Federal Trade Commission, and your state Attorney General. This notice has not been delayed as the result of a law enforcement investigation.



Activation Code: <<Code>>

### About the Equifax Credit Watch™ Silver identity theft protection product

Equifax Credit Watch will provide you with an “early warning system” to changes to your credit file and help you to understand the content of your Equifax credit file. The key features and benefits are listed below.

Equifax Credit Watch provides you with the following benefits:

- Comprehensive credit file monitoring of your Equifax credit report with daily notification of key changes to your credit file.
- Wireless alerts and customizable alerts available
- One copy of your Equifax Credit Report™
- \$25,000 in identity theft insurance with \$0 deductible, at no additional cost to you †
- 24 by 7 live agent Customer Service to assist you in understanding the content of your Equifax credit information, to provide personalized identity theft victim assistance and in initiating an investigation of inaccurate information.
- 90 day Fraud Alert placement with automatic renewal functionality \*
- Identity Restoration If you become a victim of identity theft, an Equifax identity restoration specialist will work on your behalf to help you restore your identity. Call 877-368-4940, 9:00a.m. to 8:00p.m. Eastern, Monday through Friday, before July 20, 2018 for assistance.

### **How to Enroll: You can sign up online**

To sign up online for **online delivery** go to [www.myservices.equifax.com/silver](http://www.myservices.equifax.com/silver)

1. Welcome Page: Enter the Activation Code provided at the top of this page in the “Activation Code” box and click the “Submit” button.
2. Register: Complete the form with your contact information (name, gender, home address, date of birth, Social Security Number and telephone number) and click the “Continue” button.
3. Create Account: Complete the form with your email address, create a User Name and Password, check the box to accept the Terms of Use and click the “Continue” button.
4. Verify ID: The system will then ask you up to four security questions to verify your identity. Please answer the questions and click the “Submit Order” button.
5. Order Confirmation: This page shows you your completed enrollment. Please click the “View My Product” button to access the product features.

Even if you decide not to take advantage of the subscription offer, you may still receive Equifax Identity Restoration in the event that you become victim of identity theft by calling 877-368-4940, 9:00a.m. to 8:00p.m. Eastern, Monday through Friday, before July 20, 2018.

### Directions for placing a Fraud Alert

A fraud alert is a consumer statement added to your credit report. This statement alerts creditors of possible fraudulent activity within your report as well as requests that they contact you prior to establishing any accounts in your name. Once the fraud alert is added to your credit report, all creditors should contact you prior to establishing any account in your name. To place a fraud alert on your credit file, visit: [www.fraudalerts.equifax.com](http://www.fraudalerts.equifax.com) or you may contact the Equifax auto fraud line at 1-877-478-7625, and follow the simple prompts. Once the fraud alert has been placed with Equifax, a notification will be sent to the other two credit reporting agencies, Experian and Trans Union, on your behalf.