

## US Fertility Provides Notice of Data Security Incident

Reproductive Partners Medical Group (“RPMG”) was recently told by our software provider U.S. Fertility (“USF”) that they had a data security incident. USF software helps us provide patient services.

USF told us that If your personal information was accessed, you will be receiving an official notice, by mail, from USF. Depending on the information accessed, USF may offer you free credit monitoring or the contact information for their call center, where you will be able to ask any further questions.

Here is what we have been told by USF: On September 14th, 2020, USF experienced a security incident (“Incident”). USF engaged forensics specialists to determine what information may have been affected. Both the FBI and the U.S. Department of Health and Human Services were notified. In December USF advised us that the information of some RPMG patients may have been affected. The personal information affected varies by patient and may include a social security number, names, date of birth, driver’s license, or passport number. RPMG engaged its own outside counsel to determine how we can best help our patients and ascertain who was affected and what data was accessed. To date, there is no evidence that any personal information was misused or made public.

The below notice is provided by USF which provides information regarding the mitigation actions taken by USF, credit monitoring services, call center services, and account monitoring tips. If your personal information was affected, you will receive a notification letter in the mail directly from USF in the coming weeks.

### **US Fertility Provides Notice of Data Security Incident**

US Fertility (“USF”) is providing notice of a recent incident that may affect the security of certain individuals’ protected health information. USF provides IT platforms and services to several infertility clinics, including Georgia Reproductive Specialists, LLC d/b/a SGF Atlanta, Center for Reproductive Endocrinology, Center for Reproductive Medicine & Advanced Reproductive Technologies, Center for Reproductive Medicine Alabama, Center for Reproductive Medicine Orlando, Coastal Fertility Specialists, Fertility Centers of Illinois, LLC, Fertility Partners of Pennsylvania Surgery Center, LLC, Idaho Center for Reproductive Medicine, Nevada Center for Reproductive Medicine, Nevada Fertility Center, New York Fertility Medical Practice, PLLC d/b/a SGF New York, Northwest Center for Infertility and Reproductive Endocrinology, LLP d/b/a IVF Florida Reproductive Associates, Reproductive Endocrinology Associates of Charlotte, Reproductive Partners Fertility Center - San Diego, Reproductive Partners Medical Group, Inc., Reproductive Science Center of the San Francisco Bay Area, Seattle Reproductive Medicine, SGF Tampa Bay, LLC, Shady Grove Fertility Center of Pennsylvania, PLLC, Shady Grove Reproductive Science Center, P.C., Sher Institute of Reproductive Medicine New York, Sher Institute of Reproductive Medicine St. Louis, UNC Fertility, Utah Fertility Center, Virginia Fertility Associates, LLC d/b/a SGF Richmond, and Virginia IVF and Andrology Center, LLC.

On September 14, 2020, USF experienced an IT security event (the “Incident”) that involved the inaccessibility of certain computer systems on our network as a result of a malware infection. We responded to the Incident immediately and retained third-party computer forensic specialists to assist in our investigation. Through our immediate investigation and response, we determined that data on a number of servers and workstations connected to our domain had been encrypted by ransomware. We proactively removed a number of systems from our network upon discovering the Incident. With the assistance of our third-party computer forensic specialists, we remediated the malware identified, ensured the security of our environment, and reconnected systems on September 20, 2020. We also notified federal law enforcement authorities of the Incident and continue to cooperate with their investigation. The forensic investigation is now concluded and confirmed that the unauthorized actor acquired a limited number of files during the period of unauthorized access, which occurred between August 12, 2020 and September 14, 2020, when the ransomware was executed.

We have been working diligently with a specialized team of third-party data auditors to perform a comprehensive review of all information contained in the files accessed without authorization as a result of the Incident. The purpose of this review was to accurately identify any individuals whose personal information may have been present within the impacted files and therefore accessible to the unauthorized actor.

On November 13, 2020, we began receiving the results of this review and determined that the following information relating to certain individuals was included in the impacted files when they were accessed without authorization: names, addresses, dates of birth, MPI numbers, and Social Security numbers. The types of information impacted vary by individual, and we determined that for many individuals, Social Security numbers were not impacted. Please also note that we have no evidence of actual misuse of any individual’s information as a result of the Incident.

In response to the Incident, USF has taken the following actions to mitigate any risk of compromise to information involved and to better prevent a similar event from recurring: (1) fortified the security of our firewall; (2) utilized the forensic specialists engaged to monitor network activity and remediate any suspicious activity; (3) provided notification to potentially impacted individuals as quickly as possible. We are also adapting our existing employee training protocols relating to data protection and security, including training targeted at recognizing phishing emails. We believe these steps will be effective in mitigating any potential harm to individuals. As always, we encourage individuals to review account statements, explanations of benefits, and credit reports carefully for unexpected activity and to report any questionable activity to the associated institutions immediately.

We sincerely apologize that this Incident occurred and remain committed to safeguarding the privacy and security of the information entrusted to us. We have established a dedicated call center for individuals to contact with questions or concerns. If you have any questions regarding this Incident that are not addressed in this notice, please contact our assistance line, which can be reached at 855-914-4699 (toll free), Monday through Friday from 9:00 am to 9:00 pm EST, excluding U.S. holidays.

As indicated above, we have no evidence of actual misuse of any individual's information as a result of this Incident. Included are proactive steps that can be taken to safeguard one's personal information in response to any data security event:

### **Monitor Accounts**

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.

You also have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian: PO Box 9554 Allen, TX 75013 1-888-397-3742 [www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html)

TransUnion: P.O. Box 160 Woodlyn, PA 19094 1-888-909-8872 [www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

Equifax: PO Box 105788 Atlanta, GA 30348-5788 1-800-685-1111  
[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior 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. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your 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 you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:  
Experian: P.O. Box 9554 Allen, TX 75013 1-888-397-3742 [www.experian.com/fraud/center.html](http://www.experian.com/fraud/center.html)

TransUnion: P.O. Box 2000 Chester, PA 19016 1-800-680-7289 [www.transunion.com/fraud-victimresource/place-fraudalert](http://www.transunion.com/fraud-victimresource/place-fraudalert)

Equifax: P.O. Box 105069 Atlanta, GA 30348 1-888-766-0008  
[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

### **Additional Information**

You can further educate yourself regarding fraud alerts, security freezes, and the steps you can take to protect yourself and prevent identity theft by contacting the consumer reporting agencies, 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); 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.

California Residents: Visit the California Office of Privacy Protection ([www.oag.ca.gov/privacy](http://www.oag.ca.gov/privacy)) for additional information on protection against identity theft.