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, Virginia IVF and Andrology Center, LLC, Arizona Reproductive Medicine Associates, Fertility Centers of Orange County, NYU Langone Reproductive Specialists of New York, Midwest Fertility Specialists, and Boston IVF.

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.

We recently received the completed results of the data review and determined on December 4, 2020 that information relating to additional individuals, as well as additional information types, were included in the impacted files when those files were accessed without authorization. The full scope of information types now known to potentially impacted by this Incident includes names, addresses, dates of birth, MPI numbers, Social Security numbers, driver's license / state ID numbers, passport numbers, medical treatment/diagnosis information, medical record information, health insurance/claims information, credit/debit card information, and financial account information. **The types of information impacted vary by individual.**

Please note that we continue to 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 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	**TransUnion**	**Equifax**
PO Box 9554	P.O. Box 160	PO Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	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, 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, 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	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	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, 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) for additional information on protection against identity theft. **Kentucky Residents:** Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300. **Maryland Residents:** Office of the Attorney General of Maryland**,** Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202**,** www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023. **New Mexico Residents**: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580. **New York Residents:** the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/. **North Carolina Residents:** Office of the Attorney General of North Carolina**,** Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400, 877-566-7226 (toll free within NC). **Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392. **Rhode Island Residents:** Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are two-hundred seventy (270) Rhode Island residents impacted by this incident. **Washington D.C. Residents:** the Office of Attorney General for the District of Columbia can be reached at: 441 4thStreet NW, Suite 1100 South, Washington, D.C. 20001; 1-202-442-9828; https://oag.dc.gov. **All US Residents:** Identity Theft Clearinghouse, Federal Trade

Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.