Christopher J. DiIenno
Office: (267) 930-4775
Fax: (267) 930-4771
Email: cdiienno@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

January 8, 2021

VIA E-MAIL

Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100
E-mail: securitybreach@atg.wa.gov

Re: Notice of Data Event

Dear Sir or Madam:

We represent US Fertility LLC ("USF") located at 9600 Blackwell Road, Suite 500, Rockville, MD 20850 and are writing to notify your office of an incident that may affect the security of some personal information relating to forty-seven thousand nine hundred fifty-two (47,952) Washington residents. The investigation into this matter is ongoing, and this notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, USF does not waive any rights or defenses regarding the applicability of Washington law, the applicability of the Washington data event notification statute, or personal jurisdiction.

Nature of the Data Event

On September 14, 2020, USF experienced an IT security event (the "Incident") that involved the inaccessibility of certain computer systems on its network as a result of a malware infection. USF responded to the Incident immediately and retained third-party computer forensic specialists to assist in its investigation. Through its immediate investigation and response, USF determined that data on a number of servers and workstations connected to its domain had been encrypted by ransomware. USF proactively removed a number of systems from its network upon discovering the Incident. With the assistance of its third-party computer forensic specialists, USF remediated

the malware identified, ensured the security of its environment, and reconnected systems on September 20, 2020. USF also notified federal law enforcement authorities of the Incident and continues 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.

USF has 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 is to accurately identify any individuals whose personal information may have been present within the impacted files and therefore accessible to the unauthorized actor. USF recently received the results of this review and determined on December 4, 2020 that the following information relating to Washington residents was included in the impacted files when they were accessed without authorization: names, addresses, 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 impacted files may have also contained certain individuals' dates of birth. Please note, however, that USF has no evidence of actual misuse of any Washington residents' information as a result of the Incident.

Notice to Washington Residents

On or about January 8, 2021, USF is providing written notice of this Incident to affected individuals, which includes forty-seven thousand nine hundred fifty-two (47,952) Washington residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

In response to the Incident, USF has taken the following actions to mitigate any risk of compromise to individuals' information and to better prevent a similar event from recurring: (1) fortified the security of its 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. USF is also adapting its existing employee training protocols relating to data protection and security, including training targeted at recognizing phishing emails. USF believes these steps will be effective in mitigating any potential harm to individuals.

Additionally, USF is providing impacted individuals with guidance on how to remain vigilant against instances of identity theft and fraud, including advising individuals to review their account statements, explanations of benefits, and credit reports carefully for unexpected activity and to

report any questionable activity to the associated institutions immediately. USF is also providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. USF is offering access to complimentary credit monitoring and identity restoration services through TransUnion to any individuals for whom Social Security numbers or the equivalent were determined to be potentially impacted.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4775.

Very truly yours,

Christopher J. DiIenno of
MULLEN COUGHLIN LLC

CJD:mf1

Exhibit A

USFertility

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Re: Notice of Data Incident

Dear <<Name 1>>,

US Fertility ("USF") provides IT platforms and services to several infertility clinics, including <<Variable Data 2 – Practice>>. USF is committed to protecting the security and confidentiality of health information we gather in providing services. We are writing to make you aware of a recent incident that may affect the privacy of some of your protected health information. Please read this letter carefully and be sure to contact us with any questions or concerns you may have.

What Happened? 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.

What Information Was Involved? 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. We recently received the results of this review and determined on December 4, 2020 that the following information relating to you was included in the impacted files when they were accessed without authorization: name and <<Breached Elements>>. The impacted files may have also contained your date of birth. Please note, however, that we have no evidence of actual misuse of your information as a result of the Incident.

What We Are Doing. In response to the Incident, USF has taken the following actions to mitigate any risk of compromise to your information 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 you. As always, we encourage you to review your account statements, explanations of benefits, and credit reports carefully for unexpected activity and to report any questionable activity to the associated institutions immediately.

Out of an abundance of caution, we are providing you with twelve (12) months of complimentary access to credit monitoring and identity restoration services through TransUnion, as well as guidance on how to better protect your information, should you feel it is appropriate to do so. While we are covering the cost of these services, due to privacy restrictions, you will need to complete the activation process yourself.

What You Can Do. You can find out more about how to safeguard your information in the enclosed *Steps You Can Take to Protect Personal Information.* There, you will find additional information about the complimentary credit monitoring and identity restoration services we are offering and how to enroll.

For More Information. If you have any questions regarding this Incident that are not addressed in this letter, please contact our dedicated 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.

We sincerely apologize that this Incident occurred and remain committed to safeguarding the privacy and security of the information entrusted to us.

Sincerely,

Carrie Roll

Carrie Roll
General Counsel

Steps You Can Take to Protect Personal Information

Enroll in Complimentary Credit Monitoring

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) provided by TransUnion Interactive, a subsidiary of TransUnion,® one of the three nationwide credit reporting companies.

How to Enroll: You can sign up online or via U.S. mail delivery

- To enroll in this service, go to the *my*TrueIdentity website at **www.MyTrueIdentity.com** and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code **<<Insert Unique 12-letter Activation Code>>** and follow the three steps to receive your credit monitoring service online within minutes.

- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode **<<Insert static 6-digit Telephone Pass Code>>**and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

  You can sign up for the online or offline credit monitoring service anytime between now and **<<Enrollment Deadline>>**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score.
- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

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 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, 7 00 Capitol Avenue, Suite 118, Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300. **Maryland R esidents:** Office of the Attorney General of Maryland**,** Consumer Protection Division, 200 St. Paul Place, Baltimore, M D 21202**,** www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023. **New Mexico Residents**: You have rights pu rsuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used agains t you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incompl ete 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 outdat ed negative information; access to your file is limited; you must give your consent for credit reports to be provided to e mployers; 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 su mmarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the F air Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consu merfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Roo m 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580. **New York Residents:** t he 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**,** Consu mer 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: 401-27 4-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are (#) 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.