



IVF Michigan & Ohio Fertility Centers
37000 Woodward Ave., Suite 350
Bloomfield Hills, MI 48304

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Data Breach Notification

August 7, 2023

Dear Attorney General Brown,

I am writing to inform you of a data breach incident that occurred at IVF Michigan & Ohio Fertility Centers ("IVF Michigan"), affecting the personal information of Maryland residents. The purpose of this letter is to comply with the legal requirement to notify your office about the breach, as stipulated in the Maryland Personal Information Protection Act (Md. Code Ann., Comm. Law § 14-3504).

Affected Maryland Residents:

We have identified four Maryland residents whose personal information was compromised during the data breach.

Description of the Data Breach:

On February 25, 2023, IVF Michigan became the victim of a ransomware attack involving cyber criminals encrypting server data and demanding a ransom payment in exchange for decryption keys to recover the information. IVF Michigan's security systems automatically responded to the attack almost immediately. In accordance with the emergency protocol, IVF Michigan's systems were scanned, shut down, and disconnected from the internet.

On February 28, 2023, it was determined with reasonable certainty that certain files were accessed without authorization and likely exfiltrated. As of today, we are aware that some of the files involved in this incident may contain the following protected health and other information of the four Maryland residents:

- Clinical and health information: diagnosis/conditions, lab results, medications and other related treatment information
- Demographic and other personal information: Name, address/ZIP, and date of birth

Data Breach Response and Mitigation Efforts:

IVF Michigan became aware of the attack on February 28, 2023, and immediately launched an investigation into the nature and scope of the incident. Upon initial notice that systems were



compromised, our software services vendor immediately launched an incident response procedure to contain any existing threat and limit any potential harm.

We have taken several steps to mitigate the harm caused by this incident that include executing our emergency security system protocol, incident response procedures and hiring a forensics team that continues to assist and investigate. We have taken additional measures to prevent further breaches that include enhancing our security and risk management procedures, replacing our IT vendor and updating our encryption technologies.

Written Notification to Affected Individuals:

IVF Michigan will send written notification letters to the four impacted Maryland residents on August 9, 2023. A sample copy of this notification letter is enclosed.

IVF Michigan takes this cyber-attack very seriously, and we will continue to work with our experts to diligently respond to this situation. Please contact me at MBlau@ivf-mi.com or (248) 952-9600, if you require any further information or have additional questions regarding this data breach.

Sincerely,

A handwritten signature in blue ink, appearing to read 'MBLau'.

Michelle Blau
Human Resources and Business Development Director



IVF Michigan & Ohio Fertility Centers
37000 Woodward Ave., Suite 350
Bloomfield Hills, MI 48304

[Individual Name]

[Individual Address]

[City, State, Zip]

[DATE]

NOTICE OF DATA BREACH

Dear [Name]:

The safety and privacy of our patients' data is of paramount importance to us. For this reason, as a precautionary measure, we are writing to let you know about a data security incident that likely involved your personal information.

WHAT HAPPENED:

On February 25, 2023, IVF Michigan and Ohio Fertility Centers ("IVF Michigan") became the victim of a ransomware attack involving cyber criminals encrypting server data and demanding a ransom payment in exchange for decryption keys to recover the information. IVF Michigan's security systems automatically responded to the attack almost immediately. In accordance with the emergency protocol, IVF Michigan's systems were scanned, shut down, and disconnected from the internet.

IVF Michigan became aware of the attack on February 28, 2023, and immediately launched an investigation into the nature and scope of the incident. Steps have been, and are currently being, taken to contain and remediate any potential harm. Upon initial notice that systems were compromised, our software services vendor immediately launched an incident response procedure to contain any existing threat and limit any potential harm.

WHAT INFORMATION WAS INVOLVED:

On February 28, 2023, it was determined with reasonable certainty that certain files were accessed without authorization and likely exfiltrated. As of today, we are aware that some of the files involved in this incident may contain the following protected health and other information:

- **Clinical and health information:** diagnosis/conditions, lab results, medications and other related treatment information
- **Demographic and other personal information:** Name, address/ZIP, date of birth, driver's license and social security number
- **Financial information:** Credit card number with CVV code

We have not received any information indicating that the information described above has been disseminated to persons aside from the unauthorized actor who accessed and likely exfiltrated the data.

WHAT WE ARE DOING:

Upon becoming aware of the attack, IVF Michigan immediately launched an investigation and took action to assess and remedy the incident. We have taken several steps to mitigate the harm caused by this incident that include executing our emergency security system protocol, incident response procedures and hiring a forensics team that continues to assist and investigate. We have taken additional measures to prevent further breaches that include enhancing our security and risk management procedures, replacing our IT vendor and updating our encryption technologies.

IVF Michigan takes this cyber-attack very seriously. While this letter serves as notification of the cyber incident, we and our experts are continuing to diligently assess the situation and will provide an update should we obtain any additional information regarding the compromise of your personal information.

WHAT YOU CAN DO:

Given the nature of this incident we suggest that you take precautionary measures and remain vigilant by monitoring accounts and obtain free credit reports. For more information, please see the enclosure entitled "Steps You Can Take to Further Protect Your Information."

FOR MORE INFORMATION:

For further information and assistance, please contact IVF Michigan at 1-888-411-6462 or assistance@ivf-mi.com. We value your privacy and deeply regret that this incident occurred. Our investigation is continuing, and we will notify you if there are any significant developments.

Sincerely,



Michelle Blau

Human Resources and Business Development Director

Steps You Can Take to Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC).

To file a complaint with the FTC, go to IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

Obtain and Monitor Your Credit Report

We recommend that you obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348.

Access the form at <https://www.annualcreditreport.com/requestReport/requestForm.action>. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax
(866) 349-5191
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
(888) 397-3742
www.experian.com
P.O. Box 2002
Allen, TX 75013

TransUnion
(800) 888-4213
www.transunion.com
2 Baldwin Place, P.O. Box
1000
Chester, PA 19016

Consider Placing a Fraud Alert on Your Credit Report

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Take Advantage of Additional Free Resources on Identity Theft

We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at <https://www.consumer.ftc.gov/topics/privacy-identity-online-security>.

For more information, please visit [IdentityTheft.gov](https://www.identitytheft.gov) or call 1-877-ID-THEFT (877-438-4338). A copy of Identity Theft – A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf.

OTHER IMPORTANT INFORMATION

Security Freeze

In some US states, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to apply for a new credit card, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. To place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement, or insurance statement. There is no charge to request a security freeze or to remove a security freeze.