



Alyssa R. Watzman
1700 Lincoln Street, Suite 4000
Denver, Colorado 80203
Alyssa.Watzman@lewisbrisbois.com
Direct: 720.292.2052

May 10, 2022

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Email: ldtheft@oag.state.md.us

Re: Notice of Data Security Incident

Dear Attorney General Frosh:

Lewis Brisbois Bisgaard & Smith LLP (“Lewis Brisbois”) represents Genetics & IVF Institute (“GIVF”) in connection with a recent data security incident described in greater detail below.

1. Nature of the security incident.

On September 24, 2021, GIVF discovered that it had experienced an incident disrupting access to certain of its computer systems. In response, GIVF took immediate steps to secure its digital environment and promptly launched an investigation. In so doing, GIVF engaged independent digital forensics and incident response experts to determine what happened and to identify any information that may have been accessed or acquired without authorization as a result. On April 11, 2022, GIVF learned that certain personal information may have been impacted in connection with the incident. GIVF then worked diligently to identify address information required to effectuate notification. Notably, GIVF has no evidence of the misuse of any potentially impacted information.

The information belonging to Maryland residents that may have been accessible by the malicious actor(s) responsible for this incident includes Social Security Numbers, credit or debit card information, and/or medical information.

2. Number of Maryland residents affected.

GIVF notified 19 Maryland residents of this incident via first class U.S. mail on May 10, 2022. A sample copy of the notification letter is included with this correspondence.

3. Steps taken relating to the Incident.

As soon as GIVF discovered this incident, GIVF took steps to secure its systems and launched an investigation to determine what happened and whether personal information had been accessed or acquired without authorization. GIVF has also implemented additional safeguards to help ensure the security of its systems and to reduce the risk of a similar incident occurring in the future.

GIVF has established a toll-free call center through Kroll, a leader in risk mitigation and response, to answer any questions about the incident and address related concerns. The call center is available at (855) 788-1519 from 9:00 A.M. to 6:30 P.M. Eastern Time, Monday through Friday (excluding holidays). In addition, while GIVF is not aware of the misuse of any information as a result of this incident, out of an abundance of caution, GIVF is also providing complimentary identity protection services through Kroll to notified individuals.

4. Contact information.

GIVF remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact Lewis Brisbois.

Best regards,



Alyssa R. Watzman
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure: Sample Notification Letter

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_1 (“Subject:” and Variable Header)>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

I am writing to inform you of a recent data security incident experienced by Genetics & IVF Institute (“GIVF”) that may have affected your personally identifiable information. GIVF takes the privacy and security of all information within its possession very seriously. We want to emphasize that GIVF has no evidence of the misuse or attempted misuse of your personally identifiable information.

What Happened? On September 24, 2021, GIVF discovered that it had experienced an incident disrupting access to certain of its computer systems. In response, GIVF took immediate steps to secure its digital environment and promptly launched an investigation. In so doing, GIVF engaged independent digital forensics and incident response experts to determine what happened and to identify any information that may have been accessed or acquired without authorization as a result. On April 11, 2022, GIVF learned that your personally identifiable information may have been impacted in connection with the incident which is the reason for this notification. GIVF then worked diligently to identify address information required to effectuate notification. **Notably, GIVF has no evidence of the misuse or attempted misuse of any potentially impacted information.**

What Information Was Involved? The information potentially impacted in connection with this incident included your <<b2b_text_2 (“name” and Impacted Data)>>.

What Are We Doing? As soon as GIVF discovered this incident, GIVF took the steps described above. In addition, GIVF implemented measures to enhance the security of its digital environment in an effort to minimize the risk of a similar incident occurring in the future. GIVF also notified the Federal Bureau of Investigation of this incident and will provide whatever cooperation is necessary to hold the perpetrator(s) accountable.

Although GIVF has no evidence of the misuse or attempted misuse of any potentially impacted information, GIVF is providing you with information about steps that you can take to help protect your information and is offering you complimentary identity monitoring services through Kroll – a data breach and recovery services expert. These services include 12 months of Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (Date)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

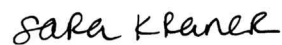
Additional information describing your services is included with this letter.

What You Can Do: You can follow the recommendations on the following page to help protect your information. GIVF also encourages you to activate the complimentary services being offered to you through Kroll.

For More Information: Further information about how to protect your information appears on the following page. If you have questions or need assistance, please call Kroll at (855) 788-1519 from 9:00 A.M. to 6:30 P.M. Eastern Time, Monday through Friday (excluding major U.S. holidays). Kroll call center representatives are fully versed on this incident and can answer any questions that you may have.

Please accept my sincere apologies and know that GIVF takes this matter very seriously and deeply regrets any worry or inconvenience that this may cause you.

Sincerely,



Sara Kraner

SVP Administration and General Counsel

Genetics & IVF Institute

STEPS YOU CAN TAKE TO HELP 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, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may 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 1-877-322-8228, 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. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: 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 one year. 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>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze 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 obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order 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.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

\$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Note: Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.



Alyssa R. Watzman
1700 Lincoln Street, Suite 4000
Denver, Colorado 80203
Alyssa.Watzman@lewisbrisbois.com
Direct: 720.292.2052

June 17, 2022

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Email: Idtheft@oag.state.md.us

Re: Supplement to Notification of Data Security Incident

Dear Attorney General Frosh:

Lewis Brisbois Bisgaard & Smith LLP (“Lewis Brisbois”) represents Genetics & IVF Institute (“GIVF”) in connection with the data security incident described below. This letter is being sent to supplement the notice relating to this incident submitted on behalf of GIVF on May 11, 2022 because, on May 25, 2022, GIVF identified an additional fifty (50) Maryland residents whose personal information may have been impacted in connection with the incident. GIVF provided notice of the incident to such individuals on June 16, 2022.

1. Nature of the security incident.

On September 24, 2021, GIVF discovered that it had experienced an incident disrupting access to certain of its computer systems. In response, GIVF took immediate steps to secure its digital environment and promptly launched an investigation. In so doing, GIVF engaged independent digital forensics and incident response experts to determine what happened and to identify any information that may have been accessed or acquired without authorization as a result. On April 11, 2022, GIVF learned that certain personal information may have been impacted in connection with the incident and then worked diligently to effectuate notification. On May 25, 2022, GIVF identified additional potentially impacted individuals, worked diligently to identify address information, and then promptly provided notification of this incident thereto. Notably, GIVF has no evidence of the misuse of any potentially impacted information.

The information belonging to the additional fifty (50) Maryland residents notified of this incident that may have been accessible by the malicious actor(s) responsible for this incident included the individuals’ names and Social Security numbers.

2. Number of Maryland residents affected.

GIVF notified a total of 69 Maryland residents of this incident by letters sent via first class U.S. mail on May 10, 2022 and June 16, 2022. A sample copy of the notification letter sent to the individuals notified on June 16, 2022 is included with this correspondence.

3. Steps taken relating to the Incident.

As soon as GIVF discovered this incident, GIVF took steps to secure its systems and launched an investigation to determine what happened and whether personal information had been accessed or acquired without authorization. GIVF has also implemented additional safeguards to help ensure the security of its systems and to reduce the risk of a similar incident occurring in the future.

GIVF has established a toll-free call center through Kroll, a leader in risk mitigation and response, to answer any questions about the incident and address related concerns. The call center is available at (855) 788-1519 from 9:00 A.M. to 6:30 P.M. Eastern Time, Monday through Friday (excluding holidays). In addition, while GIVF is not aware of the misuse of any information as a result of this incident, out of an abundance of caution, GIVF is also providing complimentary identity protection services through Kroll to notified individuals.

4. Contact information.

GIVF remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact Lewis Brisbois.

Best regards,



Alyssa R. Watzman

LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure: Sample Notification Letter

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Subject: Notice of Data Security Incident

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

I am writing to inform you of a data security incident that we – Genetics & IVF Institute (“GIVF”) – recently discovered may have affected your personally identifiable information. We take the privacy and security of all employee information within our possession very seriously. We want to emphasize that GIVF has no evidence of the misuse or attempted misuse of your personally identifiable information.

What Happened? On September 24, 2021, we discovered an incident that disrupted access to certain of our computer systems. In response, we took immediate steps to secure our digital environment and promptly launched an investigation. In so doing, we engaged independent digital forensics and incident response experts to determine what happened and to identify any information that may have been accessed or acquired without authorization as a result. On May 25, 2022, we learned that your personally identifiable information may have been impacted in connection with the incident which is the reason for this notification. We then worked diligently to identify address information required to effectuate notification. **Notably, GIVF has no evidence of the misuse or attempted misuse of any potentially impacted information.**

What Information Was Involved? The information potentially impacted in connection with this incident included your name and Social Security Number.

What Are We Doing? As soon as we discovered this incident, GIVF took the steps described above. In addition, we implemented measures to enhance the security of our digital environment in an effort to minimize the risk of a similar incident occurring in the future. We also notified the Federal Bureau of Investigation of this incident and will provide whatever cooperation is necessary to hold the perpetrator(s) accountable.

Although we have no evidence of the misuse or attempted misuse of any potentially impacted information, GIVF is providing you with information about steps that you can take to help protect your information and is offering you complimentary identity monitoring services through Kroll – a data breach and recovery services expert. These services include 12 months of Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

*You have until **September 7, 2022** to activate your identity monitoring services.*

Membership Number: <<Membership Number s_n>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

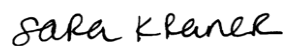
Additional information describing your services is included with this letter.

What You Can Do: You can follow the recommendations on the following page to help protect your information. We also encourage you to activate the complimentary services being offered to you through Kroll.

For More Information: Additional guidance on steps you can take to further protect your information, as well as information for enrolling in the complimentary identity monitoring services appears on the following pages. If you have questions or need assistance, please call Kroll at (855) 788-1519 from 9:00 A.M. to 6:30 P.M. Eastern Time, Monday through Friday (excluding major U.S. holidays). Kroll call center representatives are fully versed on this incident and can answer any questions that you may have.

Please accept our sincere apologies and know that we take this matter very seriously and deeply regret any worry or inconvenience that this may cause you.

Sincerely,



Sara Kraner

SVP Administration and General Counsel

Genetics & IVF Institute

STEPS YOU CAN TAKE TO HELP 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, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may 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 1-877-322-8228, 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. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: 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 one year. 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>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze 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 obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order 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.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

\$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

HOW TO ACTIVATE YOUR IDENTITY MONITORING SERVICES

1. You must activate your identity monitoring services by **September 7, 2022**. Your Activation Code will not work after this date.
2. Visit **[Enroll.krollmonitoring.com/redeem](https://enroll.krollmonitoring.com/redeem)** to activate your identity monitoring services.

Provide Your Activation Code: **<<Enter Activation Code>>** and Your Verification ID: **<<Enter Verification ID>>**

Note: Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

