

20621

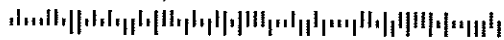
Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

June 15, 2021

G5356-L02-0000002 T00001 P001 *****AUTO**MIXED AADC 159



SAMPLE A. SAMPLE - L02 2YEAR
APT ABC
123 ANY ST
ANYTOWN, ST 12345-6789



Notice of Data Breach

Dear Sample A. Sample:

What happened: We are writing to inform you of a potential data breach event we experienced that may involve your personal information that was located on Reproductive Biology Associates and My Egg Bank North America's (1100 Johnson Ferry Rd NE #200 and #460, Atlanta, GA 30342, respectively) computer networks. Although we are unaware of any actual access or misuse of your information, we are providing notice to you and other potentially affected individuals about the incident and about the tools we are offering or that are otherwise available to protect you.

We first became aware of a potential data incident on April 16, 2021 when we discovered that a file server containing embryology data was encrypted and therefore inaccessible. We quickly determined that this was the result of a ransomware attack and shut down the affected server, thus terminating the actor's access, within the same business day. Based on our investigation, we believe the actor gained access on April 7, 2021. In the course of our ongoing investigation of the incident, on June 7, 2021 we discovered that your personal information was affected. We obtained confirmation from the actor that all exposed data was deleted and is no longer in its possession. In an abundance of caution, we conducted supplemental web searches for the potential presence of the exposed information, and at this time are not aware of any resultant exposure.

What information was involved: We are conducting a thorough investigation to determine what personal information might have been impacted. Impacted personal information may include the following:

- Full Name
- Address
- Social Security Number
- Laboratory Results
- Information relating to the handling of human tissue.
- Date of Birth



We are continuing to conduct appropriate monitoring to detect and respond to any misuse or misappropriation of the potentially exposed data.

What we are doing: We regret that this incident occurred and take the security of our information very seriously. As a result of this incident, we have initiated an investigation through a leading professional IT services firm to conduct interviews and analyze forensic data related to the incident. Specifically, we have deployed device tracking and monitoring to help contain and investigate the scope of the incident, as well as performed forensic analyses to understand the scope of the incident.

We have also applied additional internal controls and have provided additional cybersecurity training to our staff to prevent this type of incident from occurring in the future. These controls include working with a cybersecurity service provider to remediate actions taken by the actor and restore our systems, updating, patching, and in some cases replacing infrastructure to the latest versions, deploying password resets to appropriate users, rebuilding impacted systems, and deploying advanced antivirus and malware protection.

We are also very aware of the concern an incident such as this can create. Accordingly, we are offering you monitoring service for two years from the date of this letter. It may also be prudent to notify your bank in the event that anyone tries to access your accounts fraudulently.

In order to activate the credit monitoring service, please navigate to the following link: <https://www.experianidworks.com/credit>

The engagement number for this service is B014336. Enrollment ends on September 30, 2021.

Your activation code is: **ABCDEFGHI**

If you have any questions, or would prefer to enroll over the phone, you may contact Experian at (855) 919-2743. Please be prepared to provide engagement number B014336.

What can you do: Supplemental information is attached to this letter, including the Steps You Can Take to Protect Your Information as guidance on further protecting your personal data. You can also obtain information about fraud alerts and security freezes from the FTC and the credit reporting agencies listed below:

- Federal Trade Commission, <https://www.ftc.gov>, 600 Pennsylvania Avenue, NW, Washington, DC 20580 1-877-FTC-HELP
- Nationwide Consumer Reporting Companies:
 - Equifax, <https://www.equifax.com>, Equifax Credit Information Services, LLC, P.O. Box 740241, Atlanta, GA 30374, 1-800-525-6285
 - Experian <https://www.experian.com>, Experian National Consumer Assistance Center, P.O. Box 4500, Allen, TX 75013, 1-888-397-3742
 - TransUnion <https://www.transunion.com>, TransUnion Consumer Relations, P.O. Box 2000, Chester, PA 19016-2000, 1-800-680-7289

More information: Should you have further questions or concerns, we can be reached by mail at 1100 Johnson Ferry Rd NE #200, Atlanta, GA 30342, we also have a call center available at (855) 919-2743.

Respectfully,

Matthew K. Maruca
General Counsel
6750 West Loop South, Suite 395
Bellaire, Texas 77401

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.



Additional details regarding your EXPERIAN IDENTITYWORKS Membership:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- Experian credit report at signup: See what information is associated with your credit file. Daily credit reports are available for online members only.*
- Credit Monitoring: Actively monitors Experian file for indicators of fraud.
- Identity Restoration: Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- Experian IdentityWorks ExtendCARE™: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- Up to \$1 Million Identity Theft Insurance**: Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (844) 919-2743. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for two years from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Steps You Can Take to 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 closely reviewing your account statements and credit reports. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained.

Additionally, you should report any fraudulent activity or suspected incidence of identity theft to proper law enforcement authorities, including local law enforcement to file a police report, the Attorney General, or the FTC. To file a complaint with the FTC, go to www.ftc.gov/idtheft 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.

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> or calling 877-322-8228. 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 is provided below.

Fraud Alert

You may also consider placing a fraud alert on your credit report. An initial fraud alert is free and will remain 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 using the information below:

Equifax
1-800-525-6285
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

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

TransUnion
(800) 680-7289
www.transunion.com
P.O. Box 2000
Chester, PA 19022

Additional Free Resources on Identity Theft

- A copy of Take Charge: Fighting Back Against Identity Theft, 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 <http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.shtm>.

