

# Kennedys

---

1600 Market Street  
Suite 1410  
Philadelphia, PA 19103  
USA

---

t +1 267.479.6700  
f +1 215.665.8475

---

[kennedyslaw.com](http://kennedyslaw.com)

---

t +1 267 479 6706  
[joshua.mooney@kennedyslaw.com](mailto:joshua.mooney@kennedyslaw.com)  
September 13, 2023

---

## By Email

Attorney General Anthony G. Brown  
Office of the Attorney General  
Attn: Security Breach Notification  
200 St. Paul Place  
Baltimore, MD 21202  
Email: [idtheft@oag.state.md.us](mailto:idtheft@oag.state.md.us)

## Re: *Security Breach Notification*

Dear Attorney General Brown:

We write on behalf of Biocair Inc. (Biocair) regarding an IT security incident suffered by the company. Biocair is a global logistics specialist with over 35 years of experience in the pharmaceutical, biotechnology, and life sciences sectors. Its principal place of business is in Cary, North Carolina.

On April 16, 2023, Biocair became aware of an IT disruption. Biocair's IT team began an immediate investigation and determined that some of its servers had been encrypted. Following this discovery, Biocair took its IT systems offline to mitigate further spread, and engaged legal counsel and outside forensic specialists (via counsel) to help contain and investigate the incident. Biocair since has determined that an unauthorized third party gained access to a limited set of electronic personal information stored on Biocair's network. Biocair restored its system from backups. Certain personal information belonging to 7 Maryland residents involving one or more of the following data elements potentially was impacted: name; dates of birth; email address; phone number; passport scan, expiration and number; social security number; driver license scan and number; and private health details. These individuals are current and/or former employees of Biocair. Out of an abundance of caution, Biocair will offer complimentary credit monitoring services to all notified individuals.

Notifications to the impacted Maryland residents will be issued by mail on or about September 14, 2023. A sample copy of the resident notification letter is enclosed as **Exhibit A**.

Kennedys is a trading name of Kennedys CMK LLP, a limited liability partnership, in New Jersey, United States (with registered number 0450171416)

Kennedys Law LLP, a UK Limited Liability Partnership, is a partner of Kennedys CMK LLP

*Kennedys offices, associations and cooperations:* Argentina, Australia, Belgium, Bermuda, Bolivia, Brazil, Canada, Chile, China, Colombia, Denmark, Dominican Republic, Ecuador, England and Wales, France, Guatemala, Hong Kong, India, Ireland, Israel, Italy, Mexico, New Zealand, Northern Ireland, Norway, Oman, Pakistan, Panama, Peru, Poland, Portugal, Puerto Rico, Scotland, Singapore, Spain, Sweden, Turkey, United Arab Emirates, United States of America.

---

Attorney General Anthony G. Brown  
Office of the Attorney General

Please understand that Biocair takes the security of personal information seriously. If you have any questions or require further information, please feel free to contact me. Thank you.

Yours sincerely,

**Joshua Mooney**  
Partner  
for Kennedys

cc: Brienne Huntsman, Esquire

# EXHIBIT A

***SAMPLE US Consumer Notice [on Biocair letterhead]***

<<Name>>

<<Address 1>>

<<Address 2>>

<<City>><<State>><<Zip>>

<<Country>>

<<Date>>

**Notice of An IT Security Incident**

Dear <<Name>>:

Biocair Inc. (Biocair) writes to inform you of an IT security incident arising from a ransomware event that may have impacted some personal information that you provided to us. This correspondence provides you with information about the incident, our response, and additional steps you may take should you determine it is appropriate.

**What Happened?**

In mid-April 2023, Biocair became aware of a significant IT disruption. Our IT team immediately launched an internal investigation and determined that we had been impacted by an IT security incident. Our IT team's initial findings confirmed that some of our servers were encrypted at file level. Following discovery of the encryption activities, we immediately took our IT systems offline to prevent any potential further spread of malicious activity. We also engaged legal counsel and a specialist team of IT security specialists to help contain and assess the nature and scope of the incident. Our investigation has determined some data was exfiltrated from our computer network and we believe that this data included some personal information you provided to us.

**What Information Was Involved?**

Biocair's investigation has determined the following personal data you provided to us was potentially accessed and exfiltrated by the unauthorized individual including your <<DATA ELEMENTS>>.

**What We Are Doing:**

Following discovery of the incident, Biocair immediately took steps to address the incident, including taking our systems offline to mitigate potential spread of malicious activity, taking action to confirm the network was secured, engaging outside counsel and leading IT security specialists to assist with determining the nature and scope of the incident, conducting a thorough internal investigation to assess data impacted by the IT security incident and notifying law enforcement and regulators in compliance with applicable law. Additionally, we are offering you complimentary credit monitoring and identity protection services through TransUnion, in an abundance of caution. You can find enrollment instructions below.

**What You Can Do:**

Attorney General Anthony G. Brown  
Office of the Attorney General

We recommend that you remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements for suspicious activity and to detect errors. If you discover any suspicious or unusual activity on your accounts, please promptly contact the financial institution or company. We have provided additional information below, which contains more information about steps you can take to help protect yourself against fraud and identity theft, as well as credit monitoring enrollment instructions.

**For More Information:**

The security of your personal information is important to us. We thank you for your ongoing support during this time. Should you have any questions or concerns, you may contact us at [dataquestions@biocair.com](mailto:dataquestions@biocair.com) or by phone at +1 617-420-6058.

Sincerely,

[Signatory name, position]

## STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

### **Activate Identity Monitoring Services**

Biocair has set up a free credit monitoring service, which you can apply for by emailing [dataquestions@biocair.com](mailto:dataquestions@biocair.com) or call +1 617-420-6058.

## TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

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

### *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 will have the option to call a TransUnion fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

### *Fraud Consultation*

You have unlimited access to consultation with a TransUnion 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 TransUnion 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.

You can sign up for the credit monitoring service within 90 days of the date of this letter. Due to privacy laws, we cannot register you directly. Enrolling in this service will not affect your credit score.

## IMPORTANT ADDITIONAL INFORMATION

**Obtaining a Free Credit Report:** You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com), or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at [www.consumer.ftc.gov/articles/0155-free-credit-reports](http://www.consumer.ftc.gov/articles/0155-free-credit-reports)) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

**Fraud Alerts:** You can place fraud alerts with the three credit bureaus by phone and online with Equifax ([https://assets.equifax.com/assets/personal/Fraud\\_Alert\\_Request\\_Form.pdf](https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf)), Experian ([www.experian.com/fraud/center.html](http://www.experian.com/fraud/center.html)) or TransUnion ([www.transunion.com/fraud-victim-resource/place-fraud-alert](http://www.transunion.com/fraud-victim-resource/place-fraud-alert)). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

**Monitoring:** You should always remain vigilant for incidents of fraud and identity theft by reviewing payment card account statements and monitoring your credit reports for suspicious or unusual activity.

Attorney General Anthony G. Brown  
Office of the Attorney General

**Security Freeze:** You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency by visiting their websites below or by mail. In order to place the security freeze for yourself, your spouse, or a minor under the age of 16, you will need to provide your name, address for the past two years, date of birth, Social Security number, proof of identity and proof of address as requested by the credit reporting company. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password, which will be required to lift the freeze, which you can do either temporarily or permanently. It is free to place, lift, or remove a security freeze.

The contact information for the three credit reporting agencies are:

**Equifax Security Freeze**

P.O. Box 105788  
Atlanta, GA 30348-5788  
[www.equifax.com/personal/credit-report-services/credit-freeze/](http://www.equifax.com/personal/credit-report-services/credit-freeze/)  
1-866-478-0027

**Experian Security Freeze**

P.O. Box 9554  
Allen, TX 75013-9544  
<http://www.experian.com/freeze/center.html>  
1-888-397-3742

**TransUnion Security Freeze**

P.O. Box 160  
Woodlyn, PA 19094  
[www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)  
1-800-916-8800

In addition, you may further educate yourself regarding identity theft, fraud alerts, credit freezes, and steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission (“FTC”), or your state Attorney General. The contact information for the FTC is as follows:

**FTC:** ([www.identitytheft.gov](http://www.identitytheft.gov)), tel.: 1-877-ID-THEFT (1-877-438-4338)  
& TTY: 1-866-653-4261, address: 600 Pennsylvania Avenue NW,  
Washington, DC 20580.

The Federal Trade Commission 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.

If you believe you are the victim of identity theft or fraud, or have reason to believe your personal information has been misused, you should immediately:

1. **File a complaint with the police.** Ask for the case reference number and the officer's name and telephone number. If you choose, you may obtain a copy of the police report.
2. **Inform your bank and creditors** by phone and in writing about any irregularities.
3. **Report any irregularities in your mail delivery**, for example, opened envelopes, missing financial statements or documents.
4. **Alert the government tax agency**, where you may be able to place an alert.

Attorney General Anthony G. Brown  
Office of the Attorney General

5. **Take any other appropriate steps** to reduce or eliminate the impact of identity theft, fraud, or misuse.

This notice has not been delayed by law enforcement.

*For Maryland residents*, the Maryland Attorney General may be contacted at 200 St. Paul Place, 16<sup>th</sup> Floor, Baltimore, MD 21202; 1-888-743-0023; and [www.oag.state.md.us](http://www.oag.state.md.us). Biocair may be contacted at 209 James Jackson Ave., Cary, North Carolina 27513, United States, Attn: General Counsel.

*For New York residents*, the New York Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

*For North Carolina residents*, the North Carolina Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and [www.ncdoj.gov](http://www.ncdoj.gov).