

Atara Biotherapeutics, Inc.
Substitute Notice – Website
Title: Notice of a Network Security Incident

Atara Biotherapeutics, Inc.
Notice Regarding a Data Security Incident

The privacy and security of the personal information we maintain is of the utmost importance to Atara Biotherapeutics, Inc. (“Atara”). On or about November 2, 2023, Atara experienced unauthorized access to our network.

Upon learning of this issue, Atara immediately commenced a prompt and thorough investigation. As part of our investigation, we have been working closely with external cybersecurity professionals experienced in handling these types of incidents.

After an extensive forensic investigation and document review, we determined on June 10, 2024 that certain impacted files containing personal information may have been accessed and acquired by the unauthorized individual(s). The information potentially impacted by this incident is full name, date of birth, digital signature, and medical information. Not all information was impacted for all individuals.

On August 16, 2024, Atara is sending notification letters to each potentially affected individual for whom it has a last known address. The notice contains information about the incident, as well as information and resources to help individuals protect their information.

Atara has no evidence that any data has been misused. Nevertheless, Atara encourages impacted individuals to take actions to help protect their personal information. These actions include placing a fraud alert and/or security freeze on their credit files, and/or obtaining a free credit report. Additionally, individuals should always remain vigilant in reviewing their financial account statements, explanation of benefits statements, and credit reports for fraudulent or irregular activity on a regular basis and report any suspicious activity to the proper authorities.

Atara remains committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it, including continually evaluating and modifying its practices and internal controls.

For individuals who have questions or need additional information regarding this incident, please contact Danielle M. Boram, Assistant General Counsel and Privacy Officer, at dboram@atarabio.com.

– OTHER IMPORTANT INFORMATION –

1. Placing a Fraud Alert on Your Credit File.

We recommend that you place an initial one (1) year “fraud alert” on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three (3) major credit bureaus at the numbers listed below. As soon as one (1) credit bureau confirms your fraud alert, they will notify the others.

Atara Biotherapeutics, Inc.
Substitute Notice – Website
Title: Notice of a Network Security Incident

Equifax

P.O. Box 105069
Atlanta, GA 30348-5069
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
(800) 525-6285

Experian

P.O. Box 9554
Allen, TX 75013
<https://www.experian.com/fraud/center.html>
(888) 397-3742

TransUnion

Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016-2000
<https://www.transunion.com/fraud-alerts>
(800) 680-7289

2. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a “Security Freeze” be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348-5788
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
(888) 298-0045

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
<http://experian.com/freeze>
(888) 397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
<https://www.transunion.com/credit-freeze>
(888) 909-8872

In order to place the security freeze, you will need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account, or to attempt to open an account in your name, or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

3. Obtaining a Free Credit Report.

Under federal law, you are entitled to one (1) free credit report every twelve (12) months from each of the above three major nationwide credit reporting companies. Call 1-877-322-8228 or request your free credit reports online at www.annualcreditreport.com. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

4. Protecting Your Health Information.

As a general matter, the following practices can help to protect you from medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.

Atara Biotherapeutics, Inc.

Substitute Notice – Website

Title: Notice of a Network Security Incident

- Review your “explanation of benefits” statement that you receive from your health insurance company. Follow up with your insurance company or the care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential disclosure to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or care provider for any items you do not recognize.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC’s Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General’s Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; <https://ag.ny.gov/consumer-frauds-bureau/identity-theft>; Telephone: 800-771-7755.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General’s Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226.