

**Innovative Scientific Solutions, LLC (“Innovative Scientific Solutions”)
Notice Regarding Data Security Incident**

Innovative Scientific Solutions is committed to protecting the privacy and security of the personal information in our possession. On September 6, 2025, Innovative Scientific Solutions learned certain systems within our network environment were affected by a cybersecurity incident. Upon learning of the issue, we commenced an immediate and thorough investigation to determine the extent of the activity.

As part of the investigation, Innovative Scientific Solutions engaged third-party cybersecurity professionals experienced in handling these incidents. The investigation aimed to determine the extent of the activity and whether individual personal information, if any, was accessed or acquired by an unauthorized party. Following a thorough forensic investigation and extensive manual document review, on March 31, 2026, we determined that the files that were potentially accessed and/or acquired by an unauthorized third-party contained personal information.

While we have no indication that there has been any fraud as a result of this incident, out of an abundance of caution commencing on April 7, 2026, Innovative Scientific Solutions notified individuals whose information was included in the files that may have been accessed and/or acquired by the unauthorized party. Notified individuals have been provided with best practices to protect their information, and individuals whose Social Security numbers were contained in the impacted files have been offered complimentary credit monitoring.

Innovative Scientific Solutions understands the importance of safeguarding individual personal information. Innovative Scientific Solutions remains fully committed to maintaining the privacy of personal information in our possession, and upon learning of the event, Innovative Scientific Solutions took immediate action to protect the individual personal information it maintains. Innovative Scientific Solutions continually evaluates and modifies its practices to enhance the security and privacy of personal information and is taking measures to augment its existing cybersecurity.

For further questions or additional information regarding this incident, please contact the dedicated toll-free response line 1-877-421-8788. The response line is available Monday through Friday, 9:00 A.M. to 9:00 P.M. Eastern time.

– OTHER IMPORTANT INFORMATION –

1. Protecting Your Medical Information.

We have no evidence that your medical information involved in this incident was or will be used for any unintended purposes. However, the following practices can provide additional safeguards to protect against medical identity theft.

- 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.
- Review your “explanation of benefits statement” which you receive from your health insurance company. Follow up with your insurance company or 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 access (noted above) 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 the care provider for any items you do not recognize.

2. Placing a Fraud Alert on Your Credit File.

We recommend that you place an initial 1-year “fraud alert” on your credit files, at no charge. An initial fraud alert is free and will stay on your credit file for at least twelve months. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you before establishing any accounts in your name. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others. Additional information is available at <https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>.

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

3. Placing a Security Freeze on Your Credit File.

Following is general information about how to request a security freeze from the three credit reporting agencies at no charge. While we believe this information is accurate, you should contact each agency for the most accurate and up-to-date information. A security freeze prohibits a credit reporting agency from releasing any information from a consumer’s credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services. There might be additional information required, and as such, to find out more information, please contact the three nationwide credit reporting agencies (contact information provided below). 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.

4. Obtain and Monitor Your Credit Report

Under federal law, you are entitled to one free credit report every 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.

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.