NOTICE OF DATA BREACH

April 9, 2026

Lehi Legacy Center Patrons,

The purpose of this letter is to notify you about the unauthorized access, acquisition, disclosure, loss of access, or destruction of your personal data held by the Lehi Legacy Center. This notice has been provided to you without unreasonable delay as described in Utah Code § 63A-19-406. At this time, the scope of the data breach has been substantially determined, and the integrity of the affected system has been restored, though the investigation remains ongoing to confirm the full extent of the incident

What Happened?

On February 26, 2026, the Lehi Legacy Center's sports registration software, Sportsman Software, experienced a system outage caused by a cybersecurity incident. An unauthorized party gained access to certain systems and disrupted their functionality, temporarily making services unavailable. The Sportsman Software operator, Peak Software Systems, immediately initiated its incident response protocols, engaged external cybersecurity experts, and worked to restore services. Systems have since been restored and the incident has been contained, though the investigation remains ongoing.

What Personal Data Was Involved?

Based on the investigation to date, certain files uploaded to the Sportsman system may have been accessed or acquired by an unauthorized party. For the Legacy Center's use of the system, this information may have included names, dates of birth, phone numbers, gender, email addresses, emergency contact information, school, grade, shirt size, parents' names, and home addresses. Peak Software Systems has indicated that the affected files appear to be routine in nature and there is no current indication that highly sensitive personal information, such as Social Security numbers or financial account information, was involved.

What We Are Doing.

Upon learning of the incident, Peak Software Systems took immediate steps to contain the issue, restore system functionality, and engage third-party cybersecurity specialists to investigate. The Lehi Legacy Center is working closely with the vendor to understand the scope of the incident and the data involved. Additional security measures and monitoring enhancements are being implemented by the vendor to help prevent similar incidents in the future.

What You Can Do.

Although Peak Software Systems has indicated that no highly sensitive personal information was involved, you may protect yourself from identity theft or other financial losses by

monitoring your financial accounts. You may contact the three credit bureaus to place a fraud alert or freeze on your accounts. Their contact information is:

EQUIFAX	EXPERIAN	TRANSUNION
P.O. Box 740241	P.O. Box 2104	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
1-888-766-0008	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

You may also receive a free credit report each year from each of these agencies at by visiting: www.annualcreditreport.com.

The following resources provide information about fraud schemes and how you can protect yourself:

- The Utah Attorney General's STOP FRAUD UTAH website provides information about fraud and the White-Collar Crime Offender Registry at:
  https://www.utfraud.com/

- The Utah Division of Consumer Protection provides information about a variety of common fraud schemes at:
  https://dcp.utah.gov/education/

- The Utah Department of Public Safety and the Statewide Information and Analysis Center provides resources to protect yourself from cybercrimes at:
  https://siac.utah.gov/resources/

- The Federal Bureau of Investigations provides information about ways to avoid being a victim of fraud at:
  https://www.fbi.gov/how-we-can-help-you/scams-and-safety

- The Federal Trade Commission provides consumer advice about protecting yourself from identity theft and ways to recover if you have been a victim of a crime at:
  https://consumer.ftc.gov/features/identity-theft
  https://www.identitytheft.gov/#/

- The Securities and Exchange Commission provides information about protecting your money at:
  https://www.sec.gov/