NOTICE OF DATA BREACH INCIDENT

UPDATED: 12/29/2021

ABOUT THE DATA PRIVACY INCIDENT

San Luis Obispo County YMCA ("the Y") is making individuals aware of an incident that may affect the privacy of certain information. Although the Y is unaware of any actual or attempted misuse of such information, we are providing notice of the event so potentially affected individuals may take steps to better protect their information from misuse, should they feel it appropriate to do so.

FREQUENTLY ASKED QUESTIONS

What Happened? On July 19, 2021, the Y became aware of suspicious activity relating to certain systems. Upon discovery, the Y immediately worked with third party forensic investigators to investigate the nature and scope of the activity and the Y's systems of interest, and immediately reported the incident to law enforcement. The investigation determined that the Y was a target of a cyber event that impacted our business operations. The Y determined that an unauthorized actor might have accessed certain information within our systems. Soon after, the Y conducted a diligent and thorough assessment of all the information potentially affected by this event to identify individuals whose information was present in the relevant data. Upon discovery of this incident, the Y immediately reported the incident to the Federal Bureau of Investigation and will continue to work with law enforcement in connection with any criminal investigation.

What Information Was Involved? While the investigation to determine the full scope of information affected is ongoing and may vary by individual, the involved systems may have contained the following types of information at the time of the incident: names, addresses, dates of birth, Social Security number, driver's license or state identification numbers, financial account numbers, payment card numbers, signatures, mother's maiden names, medical diagnosis/medical treatment information, and employer identification numbers/tax identification numbers. While we are unaware of any actual or attempted misuse of any personal information, in an abundance of caution, the Y is sending written notification to all potentially impacted individuals for whom we could obtain address information.

What is the Y Doing. The confidentiality, privacy, and security of information within the Y's care are among the Y's highest priorities. Upon learning of the event, the Y immediately took steps to secure the systems and investigate the full scope of the incident and is taking additional steps to further enhance the security of its systems. These steps include implementing additional technical safeguards and working on additional training and education for our staff on ways to guard against cyber-attacks. In an abundance of caution, the Y is also notifying potentially affected individuals and providing information on steps that may be taken to best protect personal information. Importantly, we have neither seen any evidence of any use (or misuse) of the information involved, nor was the investigation able to confirm that any specific information was actually accessed, copied, or transferred from our server.

What You Can Do. The Y encourages individuals to remain vigilant against incidents of identity theft and fraud by reviewing their account statements and monitoring their free credit reports for suspicious activity

and to detect errors. Individuals may also review and consider the information and resources outlined in the below "*Steps Individuals Can Take to Protect Personal Information*."

For More Information. If individuals have additional questions, please call our dedicated assistance line at 855-912-1520 Monday-Friday: 6:00 am – 3:00 pm PST. Individuals may also write to the Y at 1020 Southwood Dr., San Luis Obispo, California 93401.

STEPS INDIVIDUALS CAN TAKE TO PROTECT PERSONAL INFORMATION

Monitor Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, individuals may visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Individuals may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on their credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If an individual is a victim of identity theft, the individual is entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should an individual wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in individuals' names without their consent. However, individuals should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application individuals make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, individuals cannot be charged to place or lift a credit freeze on their credit report. To request a security freeze, individuals will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and

7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if an individual is a victim of identity theft.

Should an individual wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

If any individuals had a username and password involved in this incident, we recommend those individuals change the password and any security question or answer for those account(s) immediately. If individuals reuse usernames and passwords for other online accounts, it is recommended those individuals change the password and any security question or answer for those online accounts, as well. Further, as a general precaution, individuals should never use the same password for more than one online account. When creating passwords, they should be complex and not contain personal information.

Individuals may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect their personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Individuals can obtain further information on how to file such a complaint by way of the contact information listed above. Individuals have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, individuals will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 441 4th St. NW #1100 Washington, D.C. 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

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.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are no Rhode Island residents impacted by this incident.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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/