

Notice of Data Breach

June 23, 2023

The San Bernardino County Sheriff's Department has become aware of a data security incident that may have impacted certain protected personal information and protected health information. We take the privacy of information in our care seriously, and while we have no evidence to suggest that any information has been misused, in an abundance of caution, we are providing the information about the incident, our response, and steps that individuals can take to protect their information.

What Happened: On or around April 7, 2023, the San Bernardino County Sheriff's Department discovered unauthorized activity within its computer systems. Upon discovery, the Sheriff's Department immediately secured the network and swiftly engaged a third-party team of forensic investigators to determine the full nature and scope of the incident, including what type of information may have been improperly accessed. At this point, the investigation has been unable to rule out the possibility that a limited amount of protected personal information and/or protected health information may have been accessed in connection with this incident. At this time, San Bernardino County Sheriff's Department is not aware of any evidence to suggest that any information has been misused. However, in an abundance of caution, the Sheriff's Department has partnered with a third-party computer forensic company to perform a thorough forensic investigation to identify all impacted data. Furthermore, we have notified federal law enforcement of this event and we are cooperating with their investigation.

What Information Was Involved: The investigation remains ongoing and there is no evidence to suggest that any information has been misused. If the investigation determined that data was impacted by this event, we will provide notification as required by federal and state law. Information related to individuals may include individual's names in combination with addresses, social security numbers, dates of birth, driver's license or state ID, financial account number, medical information, and health insurance information. Importantly, the information potentially impacted may vary for each individual, and may include all, or just one, of the above-listed types of information.

What We Are Doing: San Bernardino County Sheriff's Department has taken every step necessary to address the incident and is committed to fully protecting all of the information entrusted to us. Upon learning of this incident, the Sheriff's Departments implemented additional security measures within its network and facilities and is reviewing its current policies and procedures related to data security to enhance the security of all information to help prevent similar incidents from occurring in the future. Additionally, San Bernardino County Sheriff's Department retained a third-party forensic firm to conduct a thorough investigation. This investigation remains ongoing.

What You Can Do: San Bernardino County Sheriff's Department recommends that individuals remain vigilant in regularly reviewing and monitoring their account statements, credit history, and

explanation of benefits forms to prevent identity theft and fraud. Additionally, individuals should report any suspicious incidents to local law enforcement and/or their state Attorney General. We have included additional information below, which contains more information about steps individuals can take to protect their identity. Individuals may also wish to contact the three major credit agencies to place a fraud alert on their credit report – the credit agencies’ contact information is: Equifax (888-378-4329); TransUnion (833-395-6938); and Experian (888-397-3472).

For More Information: Should you have questions or concerns regarding this matter, please do not hesitate to contact us at **844-665-7635**, or write us at 655 East Third Street, San Bernardino, California 92415-0061.

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you 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 your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver’s license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.
- 8.

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

<p>TransUnion 1-800-680-7289 www.transunion.com</p>	<p>Experian 1-888-397-3742 www.experian.com</p>	<p>Equifax 1-888-298-0045 www.equifax.com</p>
<p>TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000</p>	<p>Experian Fraud Alert P.O. Box 9554 Allen, TX 75013</p>	<p>Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069</p>
<p>TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094</p>	<p>Experian Credit Freeze P.O. Box 9554 Allen, TX 75013</p>	<p>Equifax Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788</p>

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

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

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: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to employers; (v) you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; (vi) and you may seek damages from violators. 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 https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, FTC, 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>.

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 contacted at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.

For Washington, D.C. residents, the District of Columbia Attorney General may be contacted at 441 4th Street NW #1100, Washington, D.C. 20001; 202-727-3400, and <https://oag.dc.gov/consumer-protection>.