

# CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

## ATTORNEYS AT LAW

AMANDA RUGGIERI  
ARuggieri@c-wlaw.com

450 Sentry Parkway, Suite 200  
Blue Bell, PA 19422

Phone: (610) 567-0700  
Fax: (610) 567-0712

www.C-WLAW.com

A Mid-Atlantic Litigation Firm

Visit us online at  
www.C-WLAW.com

BREANNE POSPIECH  
BPospiech@c-wlaw.com

January 3, 2024

**Via E-Mail (IDTheft@oag.state.md.us)**

Office of the Attorney General  
200 St. Paul Place  
Baltimore, Maryland 21202

**RE: Data Incident Notification**

To Whom It May Concern:

We serve as counsel for the Housing Authority of the County of San Bernardino ("HACSB") located at 715 E. Brier Dr., San Bernardino, California 92408 and write to inform you of a data security incident. By providing this notice, HACSB does not waive any rights or defenses under Maryland law, including the data breach notification statute.

On or around June 19, 2023, HACSB became aware of potential unauthorized access to an employee email account. Upon discovery, HACSB performed a password reset for the affected account and immediately engaged a third-party forensic firm to investigate the incident. On December 26, 2023, following a full and thorough investigation, HACSB determined that information related to thirteen (13) Maryland residents may have been accessed by an unauthorized third party in connection with this matter. The information was limited to first and last name in combination with Social Security number.

On January 2, 2024, HACSB sent written notice of this incident to the potentially impacted Maryland residents pursuant to Maryland state law. The notice letters included an offer of complimentary credit monitoring and identity protection services for twelve (12) months. The notice letter sent to individuals is substantially similar to the letter attached hereto as Exhibit "A."

If you have any questions, please contact me.

Very truly yours,

*Amanda Ruggieri*

Amanda Ruggieri, Esquire  
CIPRIANI & WERNER, P.C.

## **Exhibit A**



Housing Authority of the  
County of San Bernardino  
Building Opportunities Together

P.O. Box 989728  
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>  
<<Address1>>  
<<Address2>>  
<<City>>, <<State>> <<Zip>>  
<<Country>>

Enrollment Code: <<ENROLLMENT>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

January 2, 2024

<<CA Only: RE: Notice of Data Breach>>

Dear <<First Name>> <<Last Name>>:

The Housing Authority of the County of San Bernardino ("HACSB") writes to notify you of an incident that may have impacted some of your personal information described below.

HACSB takes the privacy and security of information in our care very seriously. At this time, there is no evidence to suggest that any information was fraudulently misused. Out of an abundance of caution, we are providing you information about this incident, our response, and steps you can take to protect your information, should you feel it is appropriate to do so.

**What Happened:**

On June 19, 2023, HACSB became aware of potential unauthorized access to one (1) employee email account. Upon discovery, we immediately performed a password reset for the affected account and engaged a third-party team of forensic investigators in order to determine the full nature and scope of the incident. Following a full and thorough investigation, it was confirmed that one employee email account was subject to unauthorized access during this incident. Upon confirmation of unauthorized access to the employee email account, HACSB immediately investigated whether the affected account contained sensitive information pertaining to individuals. Following a thorough review, HACSB confirmed that a limited amount of information may have been accessed by an unauthorized third-party in connection with this incident.

At this time, there is no indication that any information has been actually viewed or misused. However, we are providing this notification to you out of an abundance of caution and so that you may take steps to safeguard your information if you feel it is necessary to do so.

**What Information Was Involved:**

The potentially accessed information may have included your first name or initial and last name, in combination with your <<Data Elements>>.

**What Are We Doing:**

HACSB has taken steps to address the incident and is committed to protecting personal information in its care. Upon learning of this incident, we immediately took steps to secure our email tenant and undertook a thorough investigation.

**Credit Monitoring:**

As an additional safeguard, we have arranged for you to enroll in, at no cost to you, an online credit monitoring service for <<Credit Monitoring Length>> provided by IDX. Due to state and federal privacy laws, HACSB cannot enroll you directly. If you wish to take advantage of this complimentary credit monitoring service, you must enroll yourself. Please note the deadline to enroll is April 2, 2024.

**What You Can Do:**

In addition to enrolling in the complimentary credit monitoring service detailed within, we recommend that you remain vigilant in regularly reviewing and monitoring all of your account statements and credit history to guard against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on any of your accounts, please promptly change your password, notify your financial institution or company if applicable, and take any additional steps needed to protect your account. Additionally, please report any suspicious incidents to local law enforcement and/or your state Attorney General. Please review the enclosed “Steps You Can Take to Help Protect Your Information” for additional resources.

**For More Information:**

Should you have additional questions or concerns regarding this matter, please do not hesitate to contact our dedicated call center at 1-888-859-8612. You can also write us at 715 E. Brier Drive, San Bernardino, CA 92408, Attn: Human Resources.

HACSB takes the security of information entrusted to our care very seriously. While it is regrettable this potential exposure occurred, please be assured that we are taking appropriate actions to rectify the situation and prevent such incidents in the future.

Sincerely,

Maria Razo  
Executive Director

## STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

### Activate Identity Monitoring Services

- 1. Website and Enrollment.** Scan the QR image or go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.
- 2. Activate the credit monitoring** provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.
- 3. Telephone.** Contact IDX at 1-888-859-8612 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

### Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms 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](http://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.

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

|                                                                                                   |                                                                                             |                                                                                          |
|---------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| <b>TransUnion</b><br>1-800-680-7289<br><a href="http://www.transunion.com">www.transunion.com</a> | <b>Experian</b><br>1-888-397-3742<br><a href="http://www.experian.com">www.experian.com</a> | <b>Equifax</b><br>1-888-298-0045<br><a href="http://www.equifax.com">www.equifax.com</a> |
| <b>TransUnion Fraud Alert</b><br>P.O. Box 2000<br>Chester, PA 19016-2000                          | <b>Experian Fraud Alert</b><br>P.O. Box 9554<br>Allen, TX 75013                             | <b>Equifax Fraud Alert</b><br>P.O. Box 105069<br>Atlanta, GA 30348-5069                  |

|                                                                      |                                                                   |                                                                           |
|----------------------------------------------------------------------|-------------------------------------------------------------------|---------------------------------------------------------------------------|
| <b>TransUnion Credit Freeze</b><br>P.O. Box 160<br>Woodlyn, PA 19094 | <b>Experian Credit Freeze</b><br>P.O. Box 9554<br>Allen, TX 75013 | <b>Equifax Credit Freeze</b><br>P.O. Box 105788<br>Atlanta, GA 30348-5788 |
|----------------------------------------------------------------------|-------------------------------------------------------------------|---------------------------------------------------------------------------|

### **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](http://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 District of Columbia residents*, the District of Columbia Attorney General may be contacted at: 400 6th St. NW Washington, D.C. 20001; 202-442-9828, and <https://oag.dc.gov/consumer-protection>.

*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 <https://www.marylandattorneygeneral.gov/>.

*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](http://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/>.

*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](http://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](http://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 0 Rhode Island residents impacted by this incident.