

CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

Jason Goodwin
jgoodwin@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, Pennsylvania 19422

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

February 2, 2024

Via Email

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
idtheft@oag.state.md.us

RE: Data Security Incident Notification

To Whom It May Concern:

We serve as counsel for Jacobson and Company, ("Jacobson") 1079 E Grand Street, Elizabeth, New Jersey 07201. We write to provide notification of a recent data security incident. By providing this notice, Jacobson does not waive any rights or defenses under Maryland law, including the data breach notification statute.

On September 23, 2023, Jacobson experienced a network disruption that affected their ability to access certain systems. Upon discovery, Jacobson took immediate steps to respond and remediate the disruption. Further, Jacobson engaged third-party forensic specialists to assist in a thorough investigation into the nature and scope of the incident. The investigation revealed that certain information was acquired by an unauthorized individual. Jacobson immediately worked to review the data at risk to determine the types of information affected and to whom it relates. Once this review was completed, on December 19, 2023, Jacobson learned that the impacted data included personal information and immediately initiated efforts to obtain up-to-date address information for all affected individuals, including performing a National Change of Address (NCOA) search.

On January 30, 2024, Jacobson received its results from the NCOA search and confirmed this incident potentially affected 1 Maryland resident. The information potentially impacted included the individual's first and last name and their Social Security number.

In response to this incident, Jacobson took steps to secure their environment, conducted an investigation, and notified law enforcement. Additionally, Jacobson began providing notice to the potentially impacted individuals on February 2, 2024 via U.S. mail. A copy of the notice is attached as **Exhibit A**. In an abundance of caution, Jacobson is offering the potentially impacted individuals complimentary credit monitoring and identity protection services.

Very truly yours,



Jason Goodwin, Esq.

EXHIBIT A



Return to IDX
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>

February 2, 2024

<<NOTICE OF DATA BREACH>>

Dear <<First and Last Name>>:

We are writing to inform you of a recent incident experienced by Jacobson & Co. ("Jacobson") which may have impacted certain information we hold on our systems. We take this incident very seriously and are providing you with information about the incident, our response, and steps you can take to protect your information out of an abundance of caution.

What Happened: On September 23, 2023, Jacobson experienced a network disruption impacting access to certain Jacobson systems. We immediately took steps to respond and remediate the disruption. Further, Jacobson engaged third-party specialists to assist in our investigation to determine the nature and scope of the activity. Our investigation revealed that certain information within our systems was acquired by an unauthorized individual. Upon discovery, we immediately began a comprehensive and thorough review of the data at risk to determine the specific types of information that were potentially impacted, and to whom it relates. Once this review was completed, on December 19, 2023, we learned that the impacted data included personal information and we immediately initiated efforts to obtain up-to-date address information for all affected individuals. On January 16, 2024, this process was completed, and we worked to provide you with this notification as soon as possible.

What Information Was Involved: The information potentially impacted during the incident included your first and last name, in combination with the following data elements: <<Breached Elements>>.

What We Are Doing: We have taken the steps necessary to address and investigate the incident. Upon learning of this incident, we immediately took the steps to secure our systems and undertook a thorough investigation. We have also implemented additional technical safeguards to further enhance the security of information in our possession and to prevent similar incidents from happening in the future. Additionally, we are offering you <<CM Length>> months of complimentary credit monitoring and identity protection services through IDX.

What You Can Do: We recommend that you remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements for suspicious activity and to detect errors. If you discover any suspicious or unusual activity on your accounts, please promptly contact the financial institution or company. We have provided additional information below, which contains more information about steps you can take to help protect yourself against fraud and identity theft should you feel it appropriate to do so.

For More Information: Should you have any questions or concerns, please contact IDX, A ZeroFox Company at (888) 491-6184. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Jacobson & Co. can also be contacted by mail at 1079 E Grand Street, Elizabeth, NJ 07201.

Sincerely,

Jacobson & Company, Inc.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

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. Please note the deadline to enroll is May 2, 2024.

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 (888) 491-6184 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help. If you file a request for help or report suspicious activity, you will be contacted by a member of the IDX ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

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.

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

TransUnion 1-800-680-7289 www.transunion.com	Experian 1-888-397-3742 www.experian.com	Equifax 1-888-298-0045 www.equifax.com
TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000	Experian Fraud Alert P.O. Box 9554 Allen, TX 75013	Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069
TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	Equifax Credit Freeze P.O. Box 105788 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; 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 <https://www.marylandattorneygeneral.gov>. You may also write to Capital Formation Group at 62 Walnut Street, Wellesley, MA 02481.

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 Washington, D.C. residents, the District of Columbia Attorney General may be contacted at 400 6th Street NW, Washington, D.C. 20001; 202-442-9828, and <https://oag.dc.gov/consumer-protection>. You may also write to Capital Formation Group at 62 Walnut Street, Wellesley, MA 02481.

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. There are 2 Rhode Island residents impacted by this incident.