





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>

August 12, 2024

NOTICE OF <<SECURITY INCIDENT/DATA BREACH>>

Dear <<first Name>> <<last Name>>:

Kerber, Eck & Braeckel LLP (“KEB”) is an accounting and tax services firm that provides services to a client organization with which you are affiliated. On behalf of its client, <<Variable Data 1 – Data Owner>>, KEB’s Marion, Illinois branch is writing to inform you of an incident that may impact the privacy of some of your information. We are providing you with this notice, which provides details about the incident, our response to it, and the resources available to assist you in safeguarding your information, should you feel it is appropriate to do so.

Who is KEB / Why Do You Have My Information? KEB provides services to <<Variable Data 1 – Data Owner>>, and we understand you to be associated with this organization. As part of those services, KEB handles information relating to individuals. This cybersecurity incident occurred with KEB and did not impact the computer systems of <<Variable Data 1 – Data Owner>>.

What Happened? On February 7, 2023, KEB’s Marion, Illinois branch became aware of suspicious activity on our computer network. We immediately launched an investigation to determine the nature and scope of the issue. The investigation determined that an unauthorized actor accessed our network between January 27 and February 7, 2023, and viewed or copied certain files stored on our network. As a result, KEB quickly began working with a third-party to perform a thorough and time-intensive review of the potentially impacted files determine the types of information contained in the account and to whom the information belonged. This review determined that impacted files contained certain information related to you. KEB then notified <<Variable Data 1 – Data Owner>> regarding this incident and worked with them to obtain good address information for you, if that was not available to KEB. On <<Date Depended on Date Owner>>, the address enrichment process completed, and KEB began providing notice to you.

What Information Was Involved? Our review determined the following information related to you was present within the impacted files: <<Variable Data 2 & 3 – Impacted Data Elements>> and name. At this time, we have no evidence of identity theft or fraud in relation to this incident.

What We Are Doing. The security of information in our care is a top priority for KEB. We quickly responded to this incident by securing our network and determining what sensitive information may have been impacted. As part of our ongoing commitment to the privacy and security of information in our care, we have implemented an advanced threat detection and response tool throughout our network and are reviewing existing policies and procedures related to data security. We also reported this event to federal law enforcement and appropriate privacy regulators where required.

As an added precaution, we are also offering <<12/24>> months of complimentary access to identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. Individuals who wish to

receive these services must enroll by following the below enrollment instructions, as we are unable to activate them on your behalf.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and ss reports for suspicious activity. You can find out more about how to better protect against the potential misuse of information in the enclosed *Steps You Can Take to Protect Personal Information*. There, you will also find additional details about the identity theft protection services we are offering and how to enroll.

For More Information. We understand you may have questions about this incident that are not addressed in this letter. To ensure your questions are answered in a timely manner, please call 1-877-205-9168, Monday through Friday from 9 am to 9 pm Eastern time, excluding U.S. holidays.

We apologize for any inconvenience this incident may cause you. We are committed to the privacy and security of information in our possession.

Sincerely,

Mark Dallas, Partner
Kerber, Eck & Braeckel LLP

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring

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.

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. The deadline to enroll is November 12, 2024. 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.

Telephone. Contact IDX at 1-877-205-9168 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

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 your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a 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 you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you 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 your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report 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 security freeze, you 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 you are a victim of identity theft.

Should you wish to place a 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	1 (800) 916-8800
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

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your 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. You can obtain further information on how to file such a complaint by way of the contact information listed above. 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 and your 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: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag.dc.gov. You may also write to KEB at 3200 Robbins Road, Suite 200A, Springfield, Illinois 62704.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>. You may also write to KEB at 3200 Robbins Road, Suite 200A, Springfield, Illinois 62704.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their 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 consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their 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>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 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, individuals have the right to obtain any police report filed in regard to this event. There is approximately 1 Rhode Island resident that may be impacted by this event.