CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

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

MEGHAN S. FARALLY
mfarally@c-wlaw.com

May 2, 2023

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 Summitt Trucking, LLC ("Summitt"), located at 1800 Progress Way, Clarksville, Indiana 47129, and write to inform you of a data security incident. By providing this notice, Summitt does not waive any rights or defenses under Maryland law, including the data breach notification statute.

On or around November 16, 2022, Summitt discovered suspicious activity related to one employee email account. Upon discovery, Summitt took swift action to secure its email system and network. Summitt also launched an internal investigation and engaged leading, independent cybersecurity specialists to investigate the full nature and scope of the incident. Through the investigation, it was determined that one employee email account was subject to unauthorized access. As a result, Summitt undertook a comprehensive and time-intensive process to identify what personal information, if any, was present within the affected account, and to whom that information related.

On March 15, 2023, the review was completed, and it was determined that information related to 25 Maryland residents was potentially subject to unauthorized access. The information believed to be at risk includes first name and last name, in combination with Social Security number, financial account number, routing number and/or health insurance information.

On April 27, 2023, Summitt provided written notice of this incident to the potentially impacted Maryland residents pursuant to Maryland law. The notice letter 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.

Please contact me should you have any questions.

Very truly yours,

Meghan Farally, Esq.
CIPRIANI & WERNER, P.C.

Exhibit A

P.O. Box 1907
Suwanee, GA 30024

To Enroll, Please Call:
1-888-429-9538
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code:
<<XXXXXXXX>>

<<First_Name>> <<Middle_Name>> <<Last_Name>> <<Suffix>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Postal_Code>>

April 27, 2023

<<NOTICE OF DATA BREACH>>

Dear <<First_Name>> <<Middle_Name>> <<Last_Name>> <<Suffix>>:

We are writing to inform you of a data security incident experienced by Summitt Trucking, LLC ("Summitt") that may have involved your information as described below. We take the privacy and security of all information very seriously, and while we have no evidence to suggest that any information was subject to actual or attempted misuse as a result of this incident, we are notifying potentially impacted individuals out of an abundance of caution. This letter includes information about the incident, our response, and steps you can take to help protect your information.

What Happened: On November 16, 2022, we discovered suspicious activity related to one employee email account. Upon discovery, we took swift action to secure our email system and network. We launched an internal investigation and engaged leading, independent cybersecurity specialists to investigate the full nature and scope of this incident. Based on this investigation, we confirmed that the email account was subject to unauthorized access. Upon discovery, we began a thorough review of the contents of the email account to determine the type of information contained within the account and to whom that information related. This process was completed on March 15, 2023. We are now notifying those individuals whose information was potentially impacted by the incident.

What Information Was Involved: The information contained within the affected email account and, therefore, believed to be potentially at risk includes your first and last name, in combination with the following data element(s): <<data elements>>.

What We Are Doing: We have taken every step necessary to address the incident and are committed to fully protecting all of the information that you have entrusted to us. Upon learning of this incident, we took the steps described above, including performing password resets. We have also implemented additional technical safeguards to further enhance the security of information in our possession and prevent similar incidents from happening in the future. Out of an abundance of caution, we have arranged for you to activate, at no cost to you, an online credit monitoring service for <<12/24>> months provided by IDX, A ZeroFox Company. Due to privacy laws, we cannot activate these services for you directly. Additional information regarding how to activate the complimentary credit monitoring service is enclosed. We have also provided additional information about steps you can take to help protect yourself against fraud and identity theft.

We have also engaged with a third-party consultant to evaluate our local and cloud infrastructure, and to advise of improvements that would ensure data security for our employees, partners, vendors and customers. Actions taken and implemented have exceeded the initial recommendations and expectations.

<u>What You Can Do</u>: We recommend that you remain vigilant against incidents of fraud and identity theft 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 your financial institution or company. Additionally, you can enroll to receive the complimentary credit monitoring service we are making available to you. You can also review the enclosed "Steps You Can Take to Help Protect Your Information" for additional resources.

<u>For More Information</u>: Should you have additional questions or concerns regarding this matter, please do not hesitate to contact us at 1-888-429-9538, from 9am – 9pm Eastern Time, Monday through Friday (excluding major US holidays). You can also write to us at 1800 Progress Way, Clarksville, Indiana 47129.

The security of information is of the utmost importance to us. We stay committed to protecting your trust in us and continue to be thankful for your support.

Sincerely,

David Summitt
President

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

1. **Website and Enrollment.** 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. The deadline to enroll in July 27, 2023.

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 1-888-429-9538 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 our 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.

ADDITIONAL ACTIONS TO HELP 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 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 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	Experian	Equifax
1-800-680-7289	1-888-397-3742	1-888-298-0045
www.transunion.com	www.experian.com	www.equifax.com
TransUnion Fraud Alert	**Experian Fraud Alert**	**Equifax Fraud Alert**
P.O. Box 2000	P.O. Box 9554	P.O. Box 105069
Chester, PA 19016-2000	Allen, TX 75013	Atlanta, GA 30348-5069
TransUnion Credit Freeze	**Experian Credit Freeze**	**Equifax Credit Freeze**
P.O. Box 160	P.O. Box 9554	P.O. Box 105788
Woodlyn, PA 19094	Allen, TX 75013	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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th St. NW Washington, D.C. 20001; 202-727-3400; and oag@dc.gov. Summitt Trucking, LLC may be contacted at 1800 Progress Way, Clarksville, Indiana 47129.

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. Summitt Trucking, LLC may be contacted at 1800 Progress Way, Clarksville, Indiana 47129.

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; 1-877-566-722 6 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 2 Rhode Island residents impacted by this incident.