Farren
International Total Logistics Solutions

At Farren International, LLC, we value transparency and respect the privacy of your information.

As you know, the company was impacted by a security incident which was first detected on December 15, 2023, which may have exposed your personal information.

While such incidents unfortunately have become all too common, we recognize that this news can be unsettling. We take the wellbeing and privacy of our personnel very seriously, and we want you to have information you may need to respond appropriately. To that end, I want you to know what we did in response to this incident, and the steps you can take to help protect yourself against possible misuse of the information.

As a company, to date we have already taken proactive measures to reinforce our environment, including resetting passwords; deploying additional protection software on our systems and servers; and hardening all systems and servers in our computer network.

We have also hired outside cybersecurity and legal experts to aid our in-house professionals and analyze the incident. We are cooperating with law enforcement and, to date, we have not received any reports regarding any unauthorized use of personal information beyond the initial incident.

At this time, based on our outside cyber forensic experts' investigation, we believe that the only categories of personally identifiable information believed to have been compromised during the incident are employee names, physical addresses, email addresses, company phone numbers and passwords to company systems. We do not at this time have confirmation that more sensitive information was exposed, such as social security numbers or driver's license information.

Please note, however, that if you saved to your desktop or hard drive any personal information or records, that information or those documents may have been compromised.

Out of an abundance of caution, we are offering you free credit monitoring services for a period of two years. You will be receiving additional information on how to sign up.

We encourage you to take the following steps and consider the following additional guidance and resources below. Should you receive a call, email, or other communication from someone who claims to have your personal information:

- Do not engage with the caller/correspondent, and do not offer details about the attack or what may have occurred.
- Listen carefully and immediately following the call, make notes about what you were told.
- As soon as possible, share the information with Mike Ryan in Human Resources at (973) 927-2777 x 121.
- We will make sure you receive the information you need to properly respond to the situation.

We strongly recommend you remain vigilant. Monitor and review all your financial and account statements, and immediately report any unusual activity to the institution that issued the record and to law enforcement. Attached to this letter is a resource sheet with additional information for your reference.

To help us successfully counter any future attempt to compromise our systems, we are instituting additional security measures, and we strongly recommend that you regularly change all your passwords on all accounts and devices (business and personal, whether email, financial or social media accounts) as a best practice. Do not recycle passwords from one account to another, and do not use the same password across multiple accounts or devices. We also recommend that you implement two-factor authentication on your accounts and devices wherever available.

We are continuing to work diligently to further secure your information and our office systems. We have supplemented our already robust protocols to further protect against these types of breaches. As mentioned above, we have informed appropriate governmental authorities and will continue to cooperate fully with law enforcement. If we learn of any additional information pertinent to you, we will share it with you.

We do ask that you keep this information confidential so as to avoid any interference with our ongoing investigation and recovery efforts.

If you have any questions regarding this information, please contact Mike Ryan in Human Resources at (973) 927-2777 x 121.

In the meantime, please also see the attached resource page for important numbers and websites for you to report this event to better protect your information.

We thank you for your continued hard work, digital diligence, and your commitment to our success.

Respectfully,

Phil Antonucci
CEO

To date, and based on our investigation in conjunction with a third-party forensics team, the only categories of your personally identifiable information believed to have been compromised during the security incident were your name, physical address, email address, and/or Company phone numbers, and your password to Farren's systems. However, it is possible that your social security number or driver's license may have also been exposed. Further, if you stored a personal file on your desktop, that may have been compromised. If we learn of more definitive details, we will provide you with further information accordingly. However, in addition to signing up for free credit monitoring services and considering the information that we have provided you, we nevertheless encourage you to take the following steps and consider the following additional guidance and resources below.

IF YOUR IDENTITY IS COMPROMISED STEPS YOU CAN TAKE:

- **Local Police Reporting**

  File a report with your local police department.

- **Passwords, Passcodes**

  Change passwords and passcodes on all personal accounts and devices. Often, people will use the same password that they use for one account or device for multiple accounts and/or devices. If you change passwords, this should include your personal social media accounts, online banking accounts, cellphones, tablets, home computers, etc. Best practice is not to use the same password for more than one account or device, nor to "recycle" or reuse passwords that were used in the last several years. If your accounts offer multi-factor authentication, we suggest you enable this for those accounts.

- **IRS**

Complete IRS Form 14039. The form can be found at: https://www.irs.gov/newsroom/tips-for-taxpayers-victims-about-identity-theft-and-tax-returns-2014 and a copy is attached here for your convenience.

You can contact the IRS Identity Protection Specialized Unit at 1-800-908-4490.

- **Review Your Account Statements and Notify Law Enforcement of Suspicious Activity**

Remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission.

To file with the FTC, go to www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies. Theft of your social security number should also be reported to the FTC. IdentityTheft.gov

- **Copy of Credit Report**

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com, calling

toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report, general inquiries, placing a fraud alert on your credit report, or requesting a credit freeze is provided below:

Experian	TransUnion	Equifax
1-888-EXPERIAN (397-3742)	1-800-680-7289	1-800-525-6285
P.O. Box 9532	Fraud Victim Assistance Division	P.O. Box 740241
Allen, TX 75013	PO Box 2000	Atlanta, GA 30374-0241
www.experian.com	Chester, PA 19016	www.equifax.com
	www.transunion.com	

- **Fraud Alert**

We recommend placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

- **Credit Freezes**

You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit. There is no fee to place or lift a security freeze.

Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five years, provide the addresses where you have lived over the prior five years

5. Proof of current address such as current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique PIN or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one hour after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specific period of time.

To remove the security freeze, you must submit a request through a toll-free number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze. The credit bureaus have one hour after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.

The State of Maine also offers a resource page on identity theft, which can be found at: Office of the Maine AG: Consumer Protection: Identity Theft & Privacy.