TANNENBAUM HELPERN SYRACUSE & HIRSCHTRITT LLP

900 Third Avenue
New York, NY 10022
(212) 508-6700
FACSIMILE: (212) 371-1084

Michael J. Riela
Writer's Direct Dial: 212-508-6773
Writer's Direct Fax: 646-390-7034
E-mail: riela@thsh.com

February 27, 2018

VIA OVERNIGHT MAIL

Office of the Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Incident Notification – Laufer Group International Ltd.

Dear Attorney General MacDonald:

I am outside counsel to Laufer Group International ("Laufer Group") with respect to a data breach that it suffered on February 16, 2018. That day, Laufer Group was the victim of an email spoofing scam. As a result, an unknown person or persons received copies of the 2017 Internal Revenue Service (IRS) W-2 forms of approximately 240 current and former employees of Laufer Group. According to Laufer Group's records, one affected individual is a New Hampshire resident.

The facts of the breach are as follows: On February 16, 2018, an email that purportedly was sent from Mr. Mark Laufer (Laufer Group's chief executive officer) requested that the recipient (an employee of Laufer Group) provide him the 2017 W-2 forms for employees who were employed by the company last year, via a reply email. Unfortunately, the 2017 W-2 forms were provided in response to that email before it was discovered that the email was not actually sent by Mr. Laufer. Laufer Group does not know the identity of the individual or group that sent the email. Laufer Group discovered the fraudulent nature of the request on the same day.

Laufer Group notified its current employees of the incident via email on February 16, and sent a written notice dated February 26, 2018 to all affected individuals. Laufer Group has also notified the Federal Bureau of Investigation of the incident through its IC3 online reporting system, and Laufer Group has contacted its local police department. In addition, Laufer Group notified the Internal Revenue Service and state taxing authorities about this incident. Notification was not delayed as a result of a law enforcement investigation.

Laufer Group has offered to provide the affected individuals with an "IDShield" identity theft protection individual plan for one year. As an alternative, Laufer Group has offered to reimburse individuals who purchase the "LifeLock Standard" product from IDShield.

Please feel free to contact me if you have any questions regarding this matter. My contact information is above.

Sincerely,

Michael J. Riela

Outside counsel to Laufer Group International Ltd.

LAUFER GROUP INTERNATIONAL

February 26, 2018

Re: NOTICE OF DATA BREACH

Dear Laufer Employee:

We are writing to let you know about a data breach involving your personal information that has occurred at our company, Laufer Group International Ltd. (the "Company").

What Happened?

On February 16, 2018, the Company was the victim of an email spoofing scam. As a result, an unknown person or persons received copies of your 2017 Internal Revenue Service (IRS) W-2 form. You may have already received an email notification about this incident from the Company.

On February 16, an email that purportedly was sent from the Company's chief executive officer requested that the recipient (an employee of the Company) provide the 2017 W-2 forms for employees who were employed by the company last year, via a reply email. Unfortunately, the 2017 W-2 forms were provided in response to that email before it was discovered that the email was not actually sent from the Company's chief executive officer. Rather, that email was sent by an unknown individual or group.

What Information Was Involved?

We are sending you this notice because your 2017 W-2 form was among those that were sent out in response to the fraudulent request. Thus, your personal information that is contained in your 2017 W-2 form was accessed.

A W-2 form includes the following categories of employee information, among others:

- Name;
- Address;
- Social Security number;
- Wage or salary information; and
- Amount of taxes withheld.

LAUFER GROUP INTERNATIONAL

To our knowledge, the data accessed did not include any employee's bank account information, credit card numbers, date of birth, driver's license number, or health information.

What We Are Doing.

The Company discovered the fraudulent nature of the request the same day, and it has been addressing the matter since then. The Company has already notified the Federal Bureau of Investigation of the incident through its IC3 online reporting system, and the Company has contacted the New York Police Department (First Precinct). In addition, the Company has notified the Internal Revenue Service and state taxing authorities about this incident. Notification was not delayed as a result of a law enforcement investigation.

What You Can Do.

Please review the attachment to this letter (entitled "Steps You Can Take to Further Protect Your Information") for further information on steps you can take to protect your personal information. For example, you can obtain information about fraud alerts and security freezes from the three major credit reporting agencies (credit bureaus) and the Federal Trade Commission. Their contact information is below:

Equifax: www.equifax.com or 1-866-349-5191

Experian: www.experian.com or 1-888-397-3742

TransUnion: www.transunion.com or 1-800-680-7289

Federal Trade Commission: http://www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338).

Other Important Information.

For the next 90 days, we are offering to provide you with an "IDShield" identity theft protection individual plan (not a family plan) for one year, at no cost to you. Alternatively, you may purchase the LifeLock Standard product directly and provide us with a receipt and we will reimburse you. More information about this plan is enclosed and available at https://www.idshield.com/. If you would like to take advantage of this offer, please contact Jovina Johnson at the Company, who may be reached at jjohnson@laufer.com or 646.738.8762 within 90 days after you receive this letter.

For More Information.

For further information and assistance, please contact **Jovina Johnson at 646.738.8762 or jjohnson@laufer.com.**

LAUFER GROUP INTERNATIONAL

We take the privacy of your personal information seriously, and we sincerely regret the inconvenience this has caused.

Sincerely,

_____

Jovina Johnson
Director, Human Resources

Enclosure

LAUFER GROUP INTERNATIONAL

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

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

You should remain vigilant by reviewing your account statements and your 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 incidents of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission.

To file a complaint 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.

- **Obtain a Copy of Your Credit Report**

You may request that all three credit reports be sent to you, free of charge, for your review. Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Thieves may hold stolen information to use at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

Equifax: www.equifax.com or 1-866-349-5191

Experian: www.experian.com or 1-888-397-3742

TransUnion: www.transunion.com or 1-800-680-7289

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, you may file a police report. Get a copy of the police report; you may need it to clear up the fraudulent debts.

If your personal information has been misused, visit the FTC's site at IdentityTheft.gov to get recovery steps and to file an identity theft complaint. Your complaint will be added to the FTC's Consumer Sentinel Network, where it will be accessible to law enforcers for their investigations.

- **Fraud Alert**

You may consider placing a fraud alert on your credit report. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Contact any one of the three major credit bureaus (see contact information above). The initial fraud alert stays on your credit report for 90 days. You can renew it after 90 days.

- **Security Freeze**

You also may want to consider contacting the major credit bureaus at the telephone numbers above to place a credit freeze on your credit file. A credit freeze means potential creditors cannot get your credit report. That makes it less likely that an identify thief can open new accounts in your name. The cost to place and lift a freeze depends on state law. Find your state Attorney General's office at www.naag.org to learn more. Using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. Additionally, if you request a security freeze from a consumer reporting agency there may be a fee to place, lift or remove the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

- **Additional Free Resources on Identity Theft**

You may wish to review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit http://www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338).

A copy of Taking Charge: What to Do if Your Identity is Stolen, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.shtm.