NOTICE OF DATA BREACH

February 13, 2017

On behalf of Frosch International Travel, Inc. ("Frosch"), I am writing to inform you about a recent incident that involved Frosch employee information, including information about you. We take the protection of employee information very seriously. This is why we are contacting you directly to let you know what occurred and how we are responding to assist you.

WHAT HAPPENED. On February 10, 2017, a Frosch employee inadvertently provided W-2 information about Frosch employees to an unauthorized third party who was posing as a Frosch employee.

WHAT INFORMATION WAS INVOLVED. The employee information involved was your 2016 W-2 Form, which listed your name, address, Social Security number, 2016 gross wages and the state(s) in which you file income taxes.

WHAT WE ARE DOING. Upon learning of the incident, we immediately began conducting an investigation. We attempted to retrieve the information, but our efforts were unsuccessful. We are in the process of notifying the Federal Bureau of Investigation and the Internal Revenue Service ("IRS") of this incident.

WHAT YOU CAN DO. We recommend that you review the information provided in this letter for some steps that you may take to protect yourself against potential misuse of your personal information.

First, as a precautionary measure to safeguard your information from potential misuse, we have pre-enrolled all relevant employees in complimentary identity theft protection services through IDShield, a data breach and recovery service, for a period of one (1) year, effective February 10, 2017 through February 18, 2018. This service will provide you with 12 months of fully managed identity monitoring and restoration.* You should expect to receive some materials from IDShield in the mail in the coming days. For any further questions regarding IDShield, please do not hesitate to reach out to Dave DeNure at 361-816-6387.

You should remain vigilant for incidents of fraud and identity theft, including by regularly reviewing your account statements and monitoring free credit reports. If you discover any suspicious or unusual activity on your accounts or suspect identity theft or fraud, be sure to report it immediately to your financial institutions.

In addition, you may contact the Federal Trade Commission ("FTC") or law enforcement, including your Attorney General, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC's Web site, at www.consumer.gov/idtheft, or call the FTC at (877) IDTHEFT (438-4338), or write to Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

You may also periodically obtain credit reports from each nationwide credit reporting agency. If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit reporting agency delete that information from your credit report file. In addition, under federal law, you are entitled to one free copy of your credit report every twelve (12) months from each of the three (3) nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to

www.AnnualCreditReport.com or by calling (877) 322-8228. You may contact the nationwide credit reporting agencies at:

Equifax	Experian	TransUnion
(800) 525-6285	(888) 397-3742	(800) 916-8800
P.O. Box 740241	P.O. Box 9701	Fraud Victim Assistance Division
Atlanta, GA 30374-0241	Allen, TX 75013	P.O. Box 2000
www.equifax.com	www.experian.com	Chester, PA 19022
		www.transunion.com.

In addition, you may obtain additional information from the FTC and the credit reporting agencies about fraud alerts and security freezes. You can also contact the nationwide credit reporting agencies at the following numbers to add a fraud alert to your credit report file to help protect your credit information and to place a security freeze to restrict access to your credit report:

Equifax – (800) 349-9960 Experian – (888) 397-3742 TransUnion – (888) 909-8872

You will need to supply your name, address, date of birth, Social Security number and other personal information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it may also delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three (3) nationwide credit reporting agencies. As soon as that agency processes your fraud alert, it will notify the other two (2) credit reporting agencies, which then must place fraud alerts in your file.

The fee to place a credit freeze varies based on where you live. After receiving your request, each credit reporting agency will send you a confirmation letter containing a unique PIN or password that you will need in order to lift or remove the freeze. You should keep the PIN or password in a safe place.

Additionally, the FTC and the IRS both generally recommend that individuals who believe that they may be at risk of taxpayer refund fraud should, in addition to the above-described steps, file their income taxes as soon as possible. The IRS further suggests that a taxpayer who is an actual or potential victim of identity theft complete and submit to the IRS Form 14039 (Identity Theft Affidavit). Form 14039 is available at https://www.irs.gov/pub/irs-pdf/f14039.pdf. Upon receipt of this affidavit, the IRS may flag your taxpayer account to identify questionable activity.

FOR MORE INFORMATION. Please know that we sincerely regret any inconvenience or concern this incident may cause you.

Please do not hesitate to contact us at 1-844-688-0959 if you have any questions or concerns.

Sincerely,

Enrique Espinoza
SVP, Finance & Human Resources, FROSCH

*For any relevant employees who enrolled in IDShield prior to this occurrence, you will no longer incur the monthly fee for IDShield service.

IF YOU ARE AN IOWA RESIDENT: You may contact local law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. You can contact the Iowa Attorney General at:

Office of the Attorney General
1305 E. Walnut Street
Des Moines, IA 50319
(515) 281-5164
http://www.iowaattorneygeneral.gov/

IF YOU ARE A MARYLAND RESIDENT: You may obtain information about avoiding identity theft from the FTC or the Maryland Attorney General's Office. These offices can be reached at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
http://www.ftc.gov/idtheft/

Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023
www.oag.state.md.us

IF YOU ARE A NORTH CAROLINA RESIDENT: You may obtain information about preventing identity theft from the FTC or the North Carolina Attorney General's Office. These offices can be reached at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
www.consumer.gov/idtheft

North Carolina Department of Justice
Attorney General Roy Cooper
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
http://www.ncdoj.com