Reliability Matters
Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

NOTICE OF DATA BREACH

Dear <<Name 1>>:

SOS Intl, LLC is committed to the highest quality services with the highest level of integrity in dealing with our customers, which is why we are writing to let you know about a data security incident that involves your personally identifiable information.

What Happened?

On May 18, 2018, we learned that a cyber attacker breached our Microsoft Office 365 email communication software services. We immediately initiated an investigation and discovered that the attacker used phishing attacks on February 5, 2018 and again on March 22, 2018 to acquire the credentials for two SOS employee email accounts. The employee email accounts contained personally identifiable information in emails and attachments. As a result of this attack, the attacker was able to access, search, and read all of the sent and received emails and attachments in those employees' email accounts.

Once SOS discovered the intrusion, we acted swiftly to successfully terminate the attacker's access to our email system. Since discovering the breach, we have engaged and utilized multiple cyber security experts to assist us in a forensic investigation of this incident and a complete review of the emails and attachments exposed during this timeframe in order to identify the individuals affected by this incident. Based on the results of our investigation and review of all of the affected emails and attachments, we have determined that your personally identifiable information, which we describe below, was accessed and potentially acquired by the unauthorized third party.

SOS has reported this incident to the Federal Bureau of Investigation and will notify the applicable state regulatory authorities, where required, about this incident. We are committed to the on-going enhancement of our security infrastructure. As a result of this incident, we are implementing even more robust programs, policies, and procedures to prevent such an incident from occurring again.

What Information Was Involved

As a result of this incident, an unauthorized person may have accessed and acquired some of your personal information, including your first and last name, email address, individual or employer address information, phone number, credit card number, credit card security code, and credit card expiration date.

The above types of information existed in internal and/or external email communications related to enrollment, payment, and invoices regarding energy industry training and certification courses for which you paid with a credit card in your name. We have not been able to determine in all cases whether the card utilized for these training and certification courses was employer issued or personal.

We are notifying you so you can take appropriate steps to protect your credit card account and if necessary report this notification to your employer or human resources representative responsible for the issuance of your employee issued credit card. At this time, we do not have any evidence to suggest credit card information has been misused as a result of this security incident.

What We Are Doing

Complimentary Credit Monitoring Service

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (myTrueIdentity) for one year provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go to the myTrueIdentity website at www.mytrueidentity.com and in the space referenced as "Enter Activation Code," enter the following 12-letter Activation Code <<Insert Unique 12- letter Activation Code>> and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at 1-855-288-5422. When prompted, enter the following 6-digit telephone pass code <<Insert static 6-digit Telephone Pass Code>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and <<Insert Date>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion, or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address, and more. The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

What You Can Do

We encourage you to remain vigilant with respect to your personal information and we encourage you to consider the following steps:

- Contact your credit card company to alert them that your card information was compromised and request they immediately cancel and reissue you a new credit card.
- Closely monitor the credit card account utilized to obtain the energy industry training and certification courses, and contact the issuing bank or employer immediately if you see unauthorized activity.
- Monitor your credit report at all three of the national credit reporting agencies. Even if you do not find any suspicious activity on your credit reports, we recommend that you check your credit report periodically.
- You can order a free copy of your credit report by visiting www.annualcreditreport.com, calling 877-322-8228, or completing the Annual Credit Report Form on the Federal Trade Commission website at http://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf. The contact information for all three national credit reporting agencies is listed below.

Equifax	**Experian**	**TransUnion**
Phone: 800-685-1111 P.O. Box 740256 Atlanta, GA 30374 www.equifax.com	Phone: 1-888-397-3742 P.O. Box 9532 Allen, TX 75013 www.experian.com	Phone: 800-888-4213 P.O. Box 6790 Fullerton, CA 92834 www.transunion.com

- Consider placing a fraud alert message on your credit file. By placing this alert on your credit file, any company that requests your credit file will receive a message warning them that you may have been a victim of fraud. Companies that receive this alert may request that you provide proof of your identity. This step will help to protect you from accounts being opened or used by anyone other than yourself. If you would like to place a fraud alert on your credit file, call TransUnion at 1-800-680-7289 or request a fraud alert at https://www.transunion.com/fraud-victim-resource/place-fraud-alert.

- If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and the Attorney General's office in your state. You can also obtain information from these sources about additional methods to prevent identity theft, and you can obtain information from the Federal Trade Commission and the consumer reporting agencies for more information regarding fraud alerts and security freezes. Contact information for the Federal Trade Commission is as follows:

  Federal Trade Commission
  Consumer Response Center
  600 Pennsylvania Avenue, NW
  Washington, D.C. 20580
  1-877-438-4338
  www.ftc.gov/idtheft

- For Maryland Residents: You may contact the Maryland Office of the Attorney General's Consumer Protection Division for more information on how to prevent identity theft:
  Phone: 888-743-0023
  Online: www.oag.state.md.us
  U.S. Mail: 200 St. Paul Place, Baltimore, MD 21202

- For North Carolina Residents: You may contact the North Carolina Office of the Attorney General's Consumer Protection Division for more information on how to prevent identity theft:
  Phone: 919-716-6000
  Online: www.ncdoj.gov
  U.S. Mail: 9001 Mail Service Center, Raleigh, NC 27699-9001

For More Information

We take the protection of your personal information very seriously and apologize for any inconvenience that this incident may have caused. If you have any questions regarding this notification, please contact 877-580-9150 between 9:00 a.m. and 9:00 p.m. Eastern Time, Monday through Friday.

Sincerely,

Rocky L. Sease
CEO
SOS Intl, LLC