KING & SPALDING

King & Spalding LLP
1180 Peachtree Street N.E. Ste. 1600
Atlanta, GA 30309-3521
Tel: +1 404 572 4600
Fax: +1 404 572 5100
www.kslaw.com

Elizabeth D. Adler
Direct Dial: +1 404 572 3555
Direct Fax: +1 404 572 5100
eadler@kslaw.com

July 18, 2018

VIA U.S. MAIL

To: Attorney General Joseph Foster
Office of the Attorney General of New Hampshire
New Hampshire Department of Justice
33 Capitol Street
Concord, New Hampshire 03301

Re: Cyber Security Incident Affecting Delta Global Services

Dear Attorney General Foster,

I write on behalf of Delta Global Services ("DGS") regarding an incident that may have impacted certain personal information of current and former DGS employees. DGS takes the importance and responsibility of protecting the personal information of employees very seriously. I write to provide information on DGS' investigation into the incident, and to explain steps DGS is taking to notify potentially affected employees and provide them with ways to protect their personal information. By providing this information, DGS does not waive any objections based on scope, use, privilege, immunity, or any other protection or exemption.

On June 18, 2018, a spreadsheet containing information relating to approximately 700 DGS employees was inadvertently emailed to a small group of approximately 45 current or former DGS employees who would not normally have had access to such information. Within hours of realizing the mistake, DGS on the same day advised the recipients of the confidential nature of the contents of the file and instructed the recipients to refrain from accessing, printing or using any of the information contained in the file. Recipients were also instructed to permanently delete the file, including from their "deleted items" folder. The information in the spreadsheet that was inadvertently sent included name, address, telephone number, email address, date of birth, social security number, and some information related to employees' position and application process when they applied to work with DGS.

DGS believes the risk of harm to the affected employees is likely low, as DGS's internal policies require all DGS employees to protect the confidentiality of DGS's confidential and proprietary information, including employee data. Additionally, all DGS employees are required

to sign a confidentiality agreement protecting DGS information when they apply for employment with DGS. Notwithstanding their obligation to protect the confidential information that was inadvertently sent to them, as explained above, DGS also took immediate steps to remind the individuals receiving the file, all of whom are current or former DGS employees, to delete and refrain from accessing or using the confidential information contained in the file they received. DGS has no reason to believe that anyone's information has been used in an unauthorized manner.

DGS takes the responsibility of protecting employee personal information seriously and is taking steps to prevent a similar occurrence, including providing additional training on the handling of DGS confidential information. Out of an abundance of caution, DGS is offering the affected employees 12 months of identity theft protection services from AllClearID at no cost to the employees.

Based on its investigation to date, DGS has determined that the incident potentially impacted approximately 700 DGS employees. Approximately two (2) of those DGS employees potentially impacted reside in New Hampshire. On June 27, 2018, DGS began mailing notices to the potentially impacted employees to inform them of the incident and offer a 12 month paid subscription for AllClear ID identity theft protection services at no cost to the employees. An unaddressed copy of the letter is attached as Exhibit A. DGS has also established a call center to answer employees' questions.

DGS remains committed to protecting its employees' personal information and assisting those employees who may have been impacted by this incident. Please do not hesitate to contact me if you have any questions regarding this letter.

Sincerely,

Elizabeth D. Adler

Enclosure

cc: Phyllis B. Sumner, Esq.

Processing Center • P.O. BOX 141578 • Austin, TX 78714

00001
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

June 27, 2018

NOTICE OF DATA BREACH

Dear John,

We are writing to inform you of an incident that may have involved some of your personal information.

What Happened

On June 18, 2018, a spreadsheet containing information relating to approximately 700 Delta Global Services (DGS) employees was inadvertently emailed to a small group of approximately 45 current or former DGS employees who would not normally have had access to such information. Within hours of realizing the mistake, DGS on the same day advised the recipients of the confidential nature of the contents of the file and instructed the recipients to refrain from accessing, printing or using any of the information contained in the file. Recipients were also instructed to permanently delete the file, including from their "deleted items" folder.

What Information Was Involved

The information in the spreadsheet that was inadvertently sent included name, address, telephone number, email address, date of birth, Social Security number, and some information related to your position and application process when you applied to work with DGS. Based on our investigation, we determined that your information was included on this spreadsheet.

What We Are Doing

We believe the risk of harm to you is likely low, as DGS's internal policies require all DGS employees to protect the confidentiality of DGS's confidential and proprietary information, including employee data. Additionally, all DGS employees are required to sign a confidentiality agreement protecting DGS information when they apply for employment with DGS. Notwithstanding their obligation to protect the confidential information that was inadvertently sent to them, as explained above, DGS also took immediate steps to remind the individuals receiving the file, all of whom are current or former DGS employees, to delete and refrain from accessing or using the confidential information contained in the file they received. We have no reason to believe that anyone's information has been used in an unauthorized manner.

We take the responsibility of protecting your personal information seriously and are taking steps to prevent a similar occurrence, including providing additional training on the handling of DGS confidential information. We also want to make you aware of steps you may take to guard against identity theft or fraud. Please review the enclosed Identity Theft Prevention Tips.

What You Can Do

While we believe the risk of harm to you is likely low, we are committed to protecting your personal information. Out of an abundance of caution, we are offering you identity theft protection services at no cost to you for 12 months from AllClear ID. Information on how to enroll in these services is included below and additional information is enclosed with this notice.

As an added precaution, we have arranged to have AllClear ID protect your identity for 12 months at no cost to you. The following identity protection services start on the date of this letter, and you can use them at any time during the next 12 months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-686-9433 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Fraud Alerts with Credit Monitoring: This service offers the ability to set, renew, and remove 90-day fraud alerts on your credit file to help protect you from credit fraud. In addition, it provides credit monitoring services, a once annual credit score and credit report, and a $1 million identity theft insurance policy. To enroll in this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-855-686-9433 using the following redemption code: Redemption Code.

Please note: Following enrollment, additional steps are required by you in order to activate your phone alerts and fraud alerts, and to pull your credit score and credit file. Additional steps may also be required in order to activate your monitoring options.

For More Information

If you have further questions or concerns about this incident, you can contact AllClear ID at 1-855-686-9433 between the hours of 8:00 a.m. and 8:00 p.m. Central Time, Monday through Saturday. We sincerely regret any inconvenience or concern caused by this incident.

Sincerely,

Lisa Burns

Lisa Burns, Vice President – Human Resources - Atlanta
DAL Global Services
980 Virginia Ave., 4th Floor, Atlanta, GA 30354

Enclosures: Identity Theft Prevention Tips
AllClear Identity Repair Terms of Use

Identity Theft Prevention Tips

We recommend that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit reports. You may obtain a free copy of your credit report from each company listed below once every 12 months by requesting your report online at www.annualcreditreport.com, calling toll-free 1-877-322-8228, or mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting any of the credit reporting agencies below:

Equifax	Experian	TransUnion
PO Box 740241	PO Box 9554	PO Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
888-766-0008	888-397-3742	800-680-7289

If you believe you are the victim of identity theft, you should contact the proper law enforcement authorities, including local law enforcement, and you should consider contacting your state attorney general and/or the Federal Trade Commission ("FTC"). You also may contact the FTC to obtain additional information about avoiding identity theft.

Federal Trade Commission
Bureau of Consumer Protection
600 Pennsylvania Avenue NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft

State Attorneys General: Information on how to contact your state attorney general may be found at www.naag.org/naag/attorneys-general/whos-my-ag.php.

You may obtain information from the FTC and the credit reporting agencies listed above about placing a fraud alert and/or credit freeze on your credit report.

AllClear Identity Repair Terms of Use

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- 12 months of coverage with no enrollment required.
- No cost to you — ever. AllClear Identity Repair is paid for by the participating Company.

Services Provided
If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services ("Services") to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Identity Repair is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

Coverage Period
Service is automatically available to you with no enrollment required for 12 months from the date of the breach incident notification you received from Company (the "Coverage Period"). Fraud Events (each, an "Event") that were discovered prior to your Coverage Period are not covered by AllClear Identity Repair services.

Eligibility Requirements
To be eligible for Services under AllClear Identity Repair coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident eighteen (18) years of age or older, and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

How to File a Claim
If you become a victim of fraud covered by the AllClear Identity Repair services, you must:

- Notify AllClear ID by calling 1.855.434.8077 to report the fraud prior to expiration of your Coverage Period;
- Provide proof of eligibility for AllClear Identity Repair by providing the redemption code on the notification letter you received from the sponsor Company;
- Fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require; and
- Fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft.

Coverage under AllClear Identity Repair Does Not Apply to the Following:
Any expense, damage or loss:

- Due to
  - Any transactions on your financial accounts made by authorized users, even if acting without your knowledge, or
  - Any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your "Misrepresentation");
- Incurred by you from an Event that did not occur during your coverage period; or
- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Identity Repair coverage period.

Other Exclusions:

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity.
- AllClear ID is not an insurance company, and AllClear Identity Repair is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur.
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud.
- AllClear ID reserves the right to reasonably investigate any asserted claim to determine its validity. All recipients of AllClear Identity Repair coverage are expected to protect their personal information in a reasonable way at all times. Accordingly, recipients will not deliberately or recklessly disclose or publish their Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information.

Opt-out Policy
If for any reason you wish to have your information removed from the eligibility database for AllClear Identity Repair, please contact AllClear ID:

E-mail	Mail	Phone
support@allclearid.com	AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701	1.855.434.8077