

# KING & SPALDING

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

Phyllis B. Sumner  
Direct Dial: +1 404 572 4799  
Direct Fax: +1 404 572 5100  
psumner@kslaw.com

April 11, 2018

To: Exhibit A; Distribution List

Re: Cyber Security Incident Affecting Delta Air Lines, Inc.

Dear Sir or Madam,

I write on behalf of Delta Air Lines, Inc. ("Delta") regarding a cyber security incident involving [24]7.ai, a third-party vendor of chat services for Delta and many other companies, that may have resulted in unauthorized access to payment card information relating to purchases certain customers made on delta.com. At Delta, the security and confidentiality of customers' information is of critical importance and a responsibility the company takes very seriously. I write to provide information on Delta's investigation into the incident, and to explain steps Delta is taking to notify potentially affected customers and provide them ways to protect their personal information.

On March 28, 2018, [24]7.ai notified Delta that [24]7.ai had been involved in a cyber security incident impacting an online chat tool [24]7.ai provides on the desktop version of delta.com. While [24]7.ai advised that the incident was contained and stopped on October 12, 2017, Delta immediately launched its own investigation and engaged federal law enforcement and forensics teams. Delta's investigation to date has revealed that the incident occurred at [24]7.ai from September 26, 2017 to October 12, 2017, and that during this time certain customer payment information for [24]7.ai clients, including Delta, may have been accessed. Specifically, Delta understands that malware present in [24]7.ai's software during this time made unauthorized access possible for some customers' payment card information when the information was manually entered to complete a payment card purchase on any page of the delta.com desktop platform during the same timeframe. The customer information potentially impacted by the incident included name, address, payment card number, CVV number, and expiration date. No other type of customer personal information, such as passport, government ID, security or SkyMiles information was impacted, nor was there any impact to the Fly Delta app, mobile delta.com or any Delta computer system.

Based on its investigation to date, Delta has determined that the incident potentially impacted approximately 800,000 to 825,000 U.S. Delta customers. The approximate number of customers in your state who were potentially impacted is identified on Exhibit B. Today Delta is beginning to mail notices to the potentially impacted customers to inform them of the incident and offer a paid subscription for AllClear ID credit monitoring and identity theft protection

RECEIVED  
18 APR 13 PM 2:04  
CONSUMER PROTECTION DIV.

April 11, 2018

Page 2

services at no cost to the customers. Unaddressed copies of the letters are attached as Exhibit C. Delta has also established a call center to answer customers' questions and a dedicated website, [delta.com/response](http://delta.com/response), to provide the latest information to customers.

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

Sincerely,

A handwritten signature in black ink, appearing to read "Phyllis B. Sumner", with a long horizontal flourish extending to the right.

Phyllis B. Sumner

Enclosures

**Exhibit A; Distribution List**

<p>Steve Marshall Office of the Alabama Attorney General Office of the Attorney General P.O. Box 300152 Montgomery, AL 36130-0152</p>	<p>Jahna Lindemuth Alaska Attorney General Office 1031 West 4th Avenue, Suite 200 Anchorage, AK 99501 attorney.general@alaska.gov</p>
<p>Mark Brnovich Office of the Arizona Attorney General 1275 West Washington Street Phoenix, AZ 85007-2926</p>	<p>Leslie Rutledge Arkansas Attorney General Office 323 Center Street, Suite 200 Little Rock, AR 72201 oag@ArkansasAG.gov</p>
<p>Xavier Becerra Office of the California Attorney General California Department of Justice P.O. Box 944255 Sacramento, CA 94244-2550</p>	<p>Cynthia H. Coffman Office of the Colorado Attorney General Colorado Department of Law Ralph L. Carr Judicial Building 1300 Broadway, 10th Floor Denver, CO 80203</p>
<p>George Jepsen State of Connecticut Attorney General's Office 55 Elm Street Hartford, CT 06106 ag.breach@ct.gov</p>	<p>Karl A. Racine District of Columbia Attorney General 441 4th Street, NW Washington, DC 20001 dc.oag@dc.gov</p>
<p>Matt Denn Delaware Attorney General Delaware Department of Justice Carvel State Building 820 N. French St. Wilmington, DE 19801 attorney.general@state.de.us</p>	<p>Pam Bondi Office of the Attorney General of Florida State of Florida The Capitol PL-01 Tallahassee, FL 32399-1050</p>
<p>Chris Carr Office of the Georgia Attorney General 40 Capitol Square, SW Atlanta, GA 30334</p>	<p>Russell Suzuki Department of the Attorney General of Hawaii 425 Queen Street Honolulu, HI 96813</p>
<p>Hawaii Office of Consumer Protection Leiopapa A Kamehameha Building aka State Office Tower 235 South Beretania Street Honolulu, Hawaii 96813</p>	<p>Lawrence Wasden State of Idaho Attorney General's Office 700 W Jefferson St., Suite 210 Boise, ID 83720-0010</p>

<p>Lisa Madigan  Illinois Attorney General's Office  100 W. Randolph Street  Chicago, IL 60601  databreach@atg.state.il.us</p>	<p>Curtis T. Hill, Jr.  Indiana Attorney General's Office  Indiana Government Center South  302 W. Washington St., 5th Floor  Indianapolis, IN 46204</p>
<p>Tom Miller  Office of the Attorney General of Iowa  Hoover State Office Bldg.  1305 E. Walnut Street  Des Moines, IA 50319  consumer@iowa.gov</p>	<p>Derek Schmidt  Kansas Attorney General  120 S.W. 10th Ave., 2nd Floor  Topeka, KS 66612-1597</p>
<p>Andy Beshear  Office of the Kentucky Attorney General  700 Capitol Ave, Suite 118  Frankfort, KY 40601-3449</p>	<p>Jeff Landry  Office of the Louisiana Attorney General  P.O. Box 94005  Baton Rouge, LA 70804-4095</p>
<p>Janet T. Mills  Office of the Maine Attorney General  6 State House Station  Augusta, ME 04333</p>	<p>Brian E. Frosh  Office of the Maryland Attorney General  200 St. Paul Place  Baltimore, MD 21202-2202  Idtheft@oag.state.md.us</p>
<p>Maura Healey  Office of the Attorney General of  Massachusetts  One Ashburton Place  Boston, MA 02108-1518</p>	<p>Bill Schuette  Michigan Department of Attorney General  525 W. Ottawa St.  Lansing, MI 48909</p>
<p>Lori Swanson  Office of the Minnesota Attorney General  445 Minnesota Street, Suite 1400  St. Paul, MN 55101-2131</p>	<p>Jim Hood  Mississippi Attorney General's Office  550 High Street  Jackson, MS 39201</p>
<p>Josh Hawley  Missouri Attorney General's Office  Supreme Court Building  207 W. High St.  Jefferson City, MO 65102  attorney.general@ago.mo.gov</p>	<p>Tim Fox  Office of the Montana Attorney General  Justice Building, Third Floor  215 North Sanders  Helena, MT 59620-1401  contactdoj@mt.gov</p>
<p>Montana Office of Consumer Protection  P. O. Box 200151  Helena, MT 59620-0151</p>	<p>Doug Peterson  Nebraska Attorney General's Office  2115 State Capitol  Lincoln, NE 68509</p>

<p>Adam Paul Laxalt Office of the Nevada Attorney General 100 North Carson Street Carson City, NV 89701 AgInfo@ag.nv.gov</p>	<p>Gordon J. MacDonald New Hampshire Department of Justice 33 Capitol Street Concord, NH 03301</p>
<p>Gurbir Grewal Office of the New Jersey Attorney General RJ Hughes Justice Complex 25 Market Street, Box 080 Trenton, NJ 08625-0080 databreach@cyber.nj.gov</p>	<p>Hector Balderas Office of the New Mexico Attorney General 408 Galisteo Street Villagra Building Santa Fe, NM 87501</p>
<p>Eric T. Schneiderman Office of the New York Attorney General The Capitol Albany, NY 12224-0341</p>	<p>Josh Stein North Carolina Attorney General's Office 9001 Mail Service Center Raleigh, NC 27699-9001</p>
<p>Wayne Stenehjem North Dakota Attorney General's Office 600 E. Boulevard Ave. Dept. 125 Bismarck, ND 58505</p>	<p>Mike DeWine Ohio Attorney General's Office 30 E. Broad Street, 14th Floor Columbus, OH 43215</p>
<p>Mike Hunter Oklahoma Office of the Attorney General 313 NE 21st Street Oklahoma City, OK 73105</p>	<p>Ellen F. Rosenblum Office of the Oregon Attorney General Oregon Department of Justice 1162 Court Street, NE Salem, OR 97301-4096</p>
<p>Josh Shapiro Pennsylvania Office of Attorney General 16th Floor, Strawberry Square Harrisburg, PA 17120</p>	<p>Peter F. Kilmartin Office of the Rhode Island Attorney General 150 South Main Street Providence, RI 02903</p>
<p>Alan Wilson Office of the South Carolina Attorney General P.O. Box 11549 Columbia, SC 29211</p>	<p>Consumer Protection Division of the Department of Consumer Affairs P.O. Box 5757 Columbia, SC 29250</p>
<p>Marty J. Jackley South Dakota Attorney General's Office 1302 East Highway 14, Suite 1 Pierre, SD 57501-8501</p>	<p>Herbert H. Slatery, III Office of the Tennessee Attorney General and Reporter P.O. Box 20207 Nashville, TN 37202-0207</p>

<p>Ken Paxton Office of the Texas Attorney General P.O. Box 12548 Austin, TX 78711-2548</p>	<p>Sean D. Reyes Utah Office of the Attorney General Utah State Capitol Complex 350 N. State St., Suite 230 Salt Lake City, UT 84114-2320 uag@agutah.gov</p>
<p>TJ Donovan Vermont Attorney General's Office 109 State Street Montpelier, VT 05609-1001</p>	<p>Mark R. Herring Office of the Virginia Attorney General 202 North Ninth Street Richmond, VA 23219</p>
<p>Bob Ferguson Washington State Office of the Attorney General 1125 Washington St SE Olympia, WA 98504-0100 SecurityBreach@atg.wa.gov</p>	<p>Patrick Morrisey Office of the West Virginia Attorney General State Capitol Complex Bldg. 1, Room E-26 Charleston, WV 25305</p>
<p>Brad Schimel Office of the Wisconsin Attorney General Wisconsin Department of Justice P.O. Box 7857 Madison, WI 53707-7857</p>	<p>Peter K. Michael Wyoming Attorney General's Office Kendrick Building 2320 Capitol Avenue Cheyenne, WY 82002</p>
<p>Puerto Rico Departamento de Asuntos del Consumidor Ave. José De Diego, Pda. 22 Centro Gubernamental Minillas Edificio Torre Norte, Piso 7 San Juan, PR 00940</p>	

**Exhibit B – Approximate Number of Potentially Impacted Residents**

Iowa – Approximately 4,920

# Exhibit C



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

04484  
JOHN Q. SAMPLE  
1234 MAIN STREET  
ANYTOWN US 12345-6789

April 11, 2018

NOTICE OF DATA BREACH

Dear John Sample:

We are writing to tell you about a cyber incident involving [24]7.ai, a company that provides online chat services for Delta and many other companies. This incident may have resulted in unauthorized access to payment card information relating to a purchase you made on delta.com. The security and confidentiality of our customers' information is of critical importance to us and a responsibility we take very seriously. We've included in this letter the information we have on the incident as well as instructions to contact the team dedicated to answering your questions should you need additional assistance.

We cannot at this point say definitively whether any of our customers' information was accessed. However, out of an abundance of caution and as part of our commitment to the security of your information, we are partnering with AllClear ID, a leading customer security and fraud protection firm, to offer a suite of identity theft protection and credit monitoring services for two years from the date of this letter at no cost to you. **As an eligible customer, you can enroll in this service by calling (855) 815-0534 or visiting delta.allclearid.com.**

The latest updates on this incident will be available at delta.com/response.

**What Happened**

On March 28, 2018, Delta was notified by [24]7.ai, a company that provides online chat services for Delta and many other companies, that [24]7.ai had been involved in a cyber incident. It is our understanding that the incident occurred at [24]7.ai from Sept. 26 to Oct. 12, 2017 and that during this time certain customer payment information for [24]7.ai clients, including Delta, may have been accessed – **no other customer personal information, such as passport, government ID, security or SkyMiles information was impacted.**

We understand malware present in [24]7.ai's software between Sept. 26 and Oct. 12, 2017, made unauthorized access possible for the following fields of information when manually completing a payment card purchase on any page of the delta.com desktop platform during the same timeframe: name, address, payment card number, CVV number, and expiration date. There was no impact to the Fly Delta app, mobile delta.com or any Delta computer system.

At this point, even though only a small subset of our customers would have been exposed, we cannot say definitively whether any of our customers' information was actually accessed or subsequently compromised.



01-03-3-00

### **What Information Was Involved**

Based on our investigation to date, we have determined that the payment card information of customers who completed a purchase on the delta.com desktop platform between Sept. 26, 2017 and Oct. 12, 2017 may have been exposed. Our records indicate that you may have completed such a purchase during this time frame. As a result, information relating to the payment card used for that purchase may have been exposed, including name, address, payment card number, CVV number, and expiration date. No other customer personal information, such as passport, government ID, security or SkyMiles information was impacted.

### **What We Are Doing**

While [24]7.ai recently advised us that the incident was contained and stopped on Oct. 12, 2017, upon learning of the incident, Delta immediately launched an investigation and engaged federal law enforcement and forensic teams. We have also initiated diligent efforts to directly contact customers, including by first-class postal mail, who may have been impacted by the [24]7.ai cyber event.

Delta is committed to protecting your personal information and, out of an abundance of caution, is offering you a paid subscription for AllClear ID credit monitoring and identity theft protection services for two years at no cost to you. Information on how to enroll in these services is included with this notice.

The latest information will be available to you at [delta.com/response](http://delta.com/response).

### **What You Can Do**

We encourage you to enroll in the AllClear ID credit monitoring and identity theft protection services being offered to you free of charge for two years. In addition, please see the attached Identity Theft Prevention Tips and related state-specific information. This information provides additional steps you can take to help protect your personal information from potential unauthorized use. If you believe your card has been used to make a fraudulent purchase, please contact the card issuer immediately and follow their instructions.

### **For More Information**

We understand that this incident is concerning to you, and we will share updates on [delta.com/response](http://delta.com/response). In the meantime, we have established a dedicated call center, available at (855) 815-0534 between the hours of 8:00 a.m. and 8:00 p.m. Central Time, Monday through Saturday, to answer questions and provide additional information regarding this incident. We recognize the inconvenience and concern this incident may cause you and remain committed to ensuring the security and confidentiality of our customers' information.

Sincerely,



Deborah Wheeler  
VP, Chief Information Security Officer

Enclosures: AllClear ID Offer and Information  
Identity Theft Prevention Tips

### **AllClear ID Offer and Information**

We have arranged to have AllClear ID protect your identity for 24 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 24 months.

**AllClear Identity Repair:** This service is automatically available to you with no enrollment required. If a problem arises, simply call (855) 815-0534 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 [delta.allclearid.com](http://delta.allclearid.com) or by phone by calling (855) 815-0534.

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.



### **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](http://www.annualcreditreport.com), calling toll-free 1-877-322-8228, or mailing an Annual Credit Report Request Form (available at [www.annualcreditreport.com](http://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  
PO Box 740241  
Atlanta, GA 30374  
[www.equifax.com](http://www.equifax.com)  
888-766-0008

Experian  
PO Box 9554  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)  
888-397-3742

TransUnion  
PO Box 2000  
Chester, PA 19016  
[www.transunion.com](http://www.transunion.com)  
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](http://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](http://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.

#### **IF YOU ARE A MARYLAND RESIDENT**

You may obtain information about avoiding identity theft from the Maryland Attorney General's Office. This office can be reached at:

**Office of the State of Maryland Attorney General**  
200 St. Paul Place  
Baltimore, MD 21202  
1-888-743-0023  
[www.marylandattorneygeneral.gov](http://www.marylandattorneygeneral.gov)

#### **IF YOU ARE A NEW MEXICO RESIDENT**

Under New Mexico law, you also have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. You may also consider placing a fraud alert message or security freeze on your credit file by calling the toll-free telephone numbers for each of the three national consumer credit reporting agencies listed above. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing or other services.

If you have been a victim of identity theft and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. Alternatively, if you are over the age of 65, then the fee will also be waived. In all other cases, a credit reporting agency may charge you up to \$10.00 each to place, temporarily lift, or permanently remove a security freeze. To place a security freeze on your credit file, you must send a written request to **each** of the three national consumer reporting agencies listed above by regular, certified or overnight mail. In order 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 (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a 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 either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (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 in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) **and** the PIN number or password provided to you when you placed the security freeze as well as the identities 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 three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and Social Security number) **and** the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

#### **IF YOU ARE A NORTH CAROLINA RESIDENT**

You may obtain information about avoiding identity theft from the North Carolina Attorney General's Office. This office can be reached at:

**North Carolina Attorney General's Office**  
9001 Mail Service Center  
Raleigh, NC 27699-9001  
919-716-6400  
[www.ncdoj.gov](http://www.ncdoj.gov)

#### **IF YOU ARE A RHODE ISLAND RESIDENT**

You may obtain information about avoiding identity theft from the Rhode Island Attorney General's Office. This office can be reached at:



**Office of the State of Rhode Island Attorney General**

150 South Main Street  
Providence, RI 02903  
www.riag.ri.gov  
401-274-4400

Under Rhode Island law, you also have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. You may also consider placing a fraud alert message or security freeze on your credit file by calling the toll-free telephone numbers for each of the three national consumer credit reporting agencies listed above. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing or other services.

If you have been a victim of identity theft and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. Alternatively, if you are over the age of 65, then the fee will also be waived. In all other cases, a credit reporting agency may charge you up to \$10.00 each to place, temporarily lift, or permanently remove a security freeze. To place a security freeze on your credit file, you must send a written request to **each** of the three national consumer reporting agencies listed above by regular, certified or overnight mail. In order 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 (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a 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 either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (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 in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) **and** the PIN number or password provided to you when you placed the security freeze as well as the identities 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 three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and Social Security number) **and** the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.



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

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

April 11, 2018

NOTICE OF DATA BREACH

Dear John Sample:

We are writing to tell you about a cyber incident involving [24]7.ai, a company that provides online chat services for Delta and many other companies. This incident may have resulted in unauthorized access to payment card information relating to a purchase made for you on delta.com. The security and confidentiality of our customers' information is of critical importance to us and a responsibility we take very seriously. We've included in this letter the information we have on the incident as well as instructions to contact the team dedicated to answering your questions should you need additional assistance.

We cannot at this point say definitively whether any of our customers' information was accessed. However, out of an abundance of caution and as part of our commitment to the security of your information, we are partnering with AllClear ID, a leading customer security and fraud protection firm, to offer a suite of identity theft protection and credit monitoring services for two years from the date of this letter at no cost to you. **As an eligible customer, you can enroll in this service by calling (855) 815-0534 or visiting delta.alleclearid.com.**

The latest updates on this incident will be available at delta.com/response.

**What Happened**

On March 28, 2018, Delta was notified by [24]7.ai, a company that provides online chat services for Delta and many other companies, that [24]7.ai had been involved in a cyber incident. It is our understanding that the incident occurred at [24]7.ai from Sept. 26 to Oct. 12, 2017 and that during this time certain customer payment information for [24]7.ai clients, including Delta, may have been accessed – **no other customer personal information, such as passport, government ID, security or SkyMiles information was impacted.**

We understand malware present in [24]7.ai's software between Sept. 26 and Oct. 12, 2017, made unauthorized access possible for the following fields of information when manually completing a payment card purchase on any page of the delta.com desktop platform during the same timeframe: name, address, payment card number, CVV number, and expiration date. There was no impact to the Fly Delta app, mobile delta.com or any Delta computer system.

At this point, even though only a small subset of our customers would have been exposed, we cannot say definitively whether any of our customers' information was actually accessed or subsequently compromised.



01-03-1-00

### **What Information Was Involved**

Based on our investigation to date, we have determined that the payment card information of customers who completed a purchase on the delta.com desktop platform between Sept. 26, 2017 and Oct. 12, 2017 may have been exposed. Our records indicate that a purchase may have been made for you during this time frame. As a result, information relating to the payment card used for that purchase may have been exposed, including name, address, payment card number, CVV number, and expiration date. No other customer personal information, such as passport, government ID, security or SkyMiles information was impacted.

### **What We Are Doing**

While [24]7.ai recently advised us that the incident was contained and stopped on Oct. 12, 2017, upon learning of the incident, Delta immediately launched an investigation and engaged federal law enforcement and forensic teams. We have also initiated diligent efforts to directly contact customers, including by first-class postal mail, who may have been impacted by the [24]7.ai cyber event.

Delta is committed to protecting your personal information and, out of an abundance of caution, is offering you a paid subscription for AllClear ID credit monitoring and identity theft protection services for two years at no cost to you. Information on how to enroll in these services is included with this notice.

The latest information will be available to you at [delta.com/response](http://delta.com/response).

### **What You Can Do**

We encourage you to enroll in the AllClear ID credit monitoring and identity theft protection services being offered to you free of charge for two years. In addition, please see the attached Identity Theft Prevention Tips and related state-specific information. This information provides additional steps you can take to help protect your personal information from potential unauthorized use. If you believe your card has been used to make a fraudulent purchase, please contact the card issuer immediately and follow their instructions.

### **For More Information**

We understand that this incident is concerning to you, and we will share updates on [delta.com/response](http://delta.com/response). In the meantime, we have established a dedicated call center, available at (855) 815-0534 between the hours of 8:00 a.m. and 8:00 p.m. Central Time, Monday through Saturday, to answer questions and provide additional information regarding this incident. We recognize the inconvenience and concern this incident may cause you and remain committed to ensuring the security and confidentiality of our customers' information.

Sincerely,



Deborah Wheeler  
VP, Chief Information Security Officer

Enclosures: AllClear ID Offer and Information  
Identity Theft Prevention Tips

### **AllClear ID Offer and Information**

We have arranged to have AllClear ID protect your identity for 24 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 24 months.

**AllClear Identity Repair:** This service is automatically available to you with no enrollment required. If a problem arises, simply call (855) 815-0534 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 [delta.allclearid.com](http://delta.allclearid.com) or by phone by calling (855) 815-0534.

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.



### **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](http://www.annualcreditreport.com), calling toll-free 1-877-322-8228, or mailing an Annual Credit Report Request Form (available at [www.annualcreditreport.com](http://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  
PO Box 740241  
Atlanta, GA 30374  
[www.equifax.com](http://www.equifax.com)  
888-766-0008

Experian  
PO Box 9554  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)  
888-397-3742

TransUnion  
PO Box 2000  
Chester, PA 19016  
[www.transunion.com](http://www.transunion.com)  
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](http://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](http://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.

#### **IF YOU ARE A MARYLAND RESIDENT**

You may obtain information about avoiding identity theft from the Maryland Attorney General's Office. This office can be reached at:

**Office of the State of Maryland Attorney General**  
200 St. Paul Place  
Baltimore, MD 21202  
1-888-743-0023  
[www.marylandattorneygeneral.gov](http://www.marylandattorneygeneral.gov)

#### **IF YOU ARE A NEW MEXICO RESIDENT**

Under New Mexico law, you also have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. You may also consider placing a fraud alert message or security freeze on your credit file by calling the toll-free telephone numbers for each of the three national consumer credit reporting agencies listed above. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing or other services.

If you have been a victim of identity theft and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. Alternatively, if you are over the age of 65, then the fee will also be waived. In all other cases, a credit reporting agency may charge you up to \$10.00 each to place, temporarily lift, or permanently remove a security freeze. To place a security freeze on your credit file, you must send a written request to **each** of the three national consumer reporting agencies listed above by regular, certified or overnight mail. In order 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 (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a 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 either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (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 in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) **and** the PIN number or password provided to you when you placed the security freeze as well as the identities 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 three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and Social Security number) **and** the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

### **IF YOU ARE A NORTH CAROLINA RESIDENT**

You may obtain information about avoiding identity theft from the North Carolina Attorney General's Office. This office can be reached at:

**North Carolina Attorney General's Office**  
9001 Mail Service Center  
Raleigh, NC 27699-9001  
919-716-6400  
[www.ncdoj.gov](http://www.ncdoj.gov)

### **IF YOU ARE A RHODE ISLAND RESIDENT**

You may obtain information about avoiding identity theft from the Rhode Island Attorney General's Office. This office can be reached at:



**Office of the State of Rhode Island Attorney General**

150 South Main Street  
Providence, RI 02903  
www.riag.ri.gov  
401-274-4400

Under Rhode Island law, you also have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. You may also consider placing a fraud alert message or security freeze on your credit file by calling the toll-free telephone numbers for each of the three national consumer credit reporting agencies listed above. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing or other services.

If you have been a victim of identity theft and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. Alternatively, if you are over the age of 65, then the fee will also be waived. In all other cases, a credit reporting agency may charge you up to \$10.00 each to place, temporarily lift, or permanently remove a security freeze. To place a security freeze on your credit file, you must send a written request to **each** of the three national consumer reporting agencies listed above by regular, certified or overnight mail. In order 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 (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a 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 either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (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 in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) **and** the PIN number or password provided to you when you placed the security freeze as well as the identities 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 three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and Social Security number) **and** the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

Domestic Shipments

- To qualify for the Letter rate, UPS Express Envelope correspondence, urgent documents, and/or weigh 8 oz. or less. UPS Express Envelopes those listed or weighing more than 8 oz. will

International Shipments

- The UPS Express Envelope may be used only value. Certain countries consider electronic m. ups.com/importexport to verify if your shipment is classified as a document.

- To qualify for the Letter rate, the UPS Express Envelope must weigh 8 oz. or less. UPS Express Envelopes weighing more than 8 oz. will be billed by weight.

Note: Express Envelopes are not recommended for shipments of electronic media containing sensitive personal information or breakable items. Do not send cash or cash equivalent.

# Reusable Express Envelope Letter Size

Reduce paper waste by using this envelope a second time – either to return to sender or with another recipient. See reuse instructions on flap above.

## Decision Green<sup>SM</sup>

Decision Green is UPS's environmental platform, reflecting our pursuit of sustainable business practices worldwide. For example, this envelope is made from 100% recycled paper and is both reusable and recyclable.

1 fiber

Call 1-800-PICK-UPS (1-800-742-7108) 1030  
 173286688016130 087  
**AIR - 3250**  
 P: BROWN S: SLIDE I: BXA  
 DES MOINES IA 50319  
 1305 E WALNUT ST  
 OFFICE OF THE ATTORNEY GENERAL

SHIPPING MANAGER  
 (404) 572-4600  
 KING & SPALDING LLP  
 1160 PEACHTREE ST NE  
 ATLANTA GA 30309-3531

UPS 0.3 LBS / ALTR  
 UPS  
 UPS

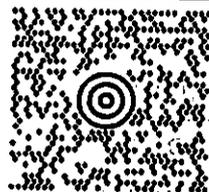
1 OF 1

SHIP TO:

TOM MILLER  
 (404) 572-4600  
 OFFICE OF THE ATTORNEY GENERAL OF I  
 HOOVER STATE OFFICE BLDG  
 1305 E. WALNUT STREET  
 DES MOINES IA 50319

Do not use this envelope for

of



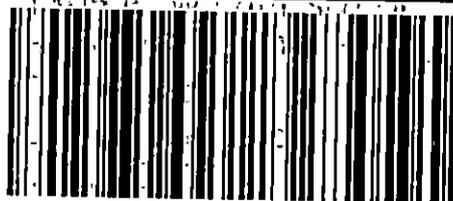
IA 503 9 - 30



UPS NEXT DAY AIR

TRACKING #: 1Z 329 658 01 6130 3587

1



BILLING: P/P

Employee Id: 5029

REF 1:16600  
 REF 2:268001

WS 21.0.19 Zebra ZP 460 99.0A 04/2018

SEE NOTICE ON REVERSE regarding UPS Terms and notice of limitation of liability. Where allowed by law, shipper authorizes UPS to act as forwarding agent for export control and customs purposes. If exported from the US, shipper certifies that the commodities, technology or software were exported from the US in accordance with the Export Administration Regulations. Diversion contrary to law is prohibited.

Serving you for more than 100 years  
 United Parcel Service.



