[redacted]

STATE OF NH
DEPT OF JUSTICE

2015 JAN 26 PM 12:22

[redacted]

January 20, 2015

INTENDED FOR ADDRESSEE(S) ONLY

VIA U.S. MAIL
Attorney General Joseph Foster
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Park 'N Fly - Data Security Event Update

Dear Attorney General Foster:

We are writing to provide an update on the Park 'N Fly ("PNF") data privacy event.

On December 30, 2014, we provided preliminary notice to your office of a data security event that may have compromised the security of personal information of New Hampshire residents. Attached as ***Exhibit A*** please find a copy of our preliminary notice for your convenience. PNF's investigation into this event is ongoing; however, since our preliminary notice to your office, the third-party forensic experts for whom PNF has been working with, have confirmed PNF's ecommerce site was infiltrated by an unauthorized third party. The ecommerce site contained credit/debit card data including, card number, cardholder's name and billing address, card expiration date, and CVV code. Other loyalty customer data potentially affected includes email addresses, Park 'N Fly passwords, and telephone numbers.

Although the security compromise has been contained, the investigation of all elements of our data network is ongoing. To date, we have not identified New Hampshire residents affected by this event. However, on January 13, 2015, PNF began notifying the public that the security of PNF's ecommerce website had been compromised. This notice was distributed by a press release and a statement posted on PNF's dedicated website www.pnf.com/security-update. A copy of this statement is attached as ***Exhibit B***. While PNF has reason to believe that the intruder stole some data from certain payment cards

that were used on PNF's ecommerce website, PNF has not determined which specific cardholder's payment card data may have been stolen by the intruder. Further, PNF does not have sufficient contact information for all customers who may potentially be affected by this incident. PNF notified potentially affected customers by providing notice of this incident to major statewide media on January 13, 2015 in substantially the same form as the statement attached here as ***Exhibit C***. Potentially affected PNF customers have been provided access to identity monitoring and identity protection services for the next 12 months, at no charge to the customer. Additionally, PNF has established an informational Web page for customers (http://www.pnf.com/security-update), and are addressing questions and concerns from PNF customers through a confidential, toll-free hotline.

As soon as the third-party forensic experts finalize the nature and scope of this incident, PNF will supplement its public notice and send written notification of this incident to all affected individuals for whom have provided PNF with address information. Should PNF's investigation reveal that New Hampshire residents were affected by this incident, PNF's supplemental notice will be provided consistent with New Hampshire's data breach notification laws. PNF will continue to supplement its preliminary notice to your office with any new significant facts learned subsequent to this submission.

Should you have any questions regarding this update, please contact us a [redacted]

Very truly yours,

SMSchapfle

[redacted]

SMS:JEP

EXHIBIT A

[redacted]

[redacted]

December 30, 2014

VIA U.S. MAIL
Attorney General Joseph Foster
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Preliminary Notice of Data Security Event

Dear Attorney General Foster:

We represent Park 'N Fly ("PNF"), 3399 Peachtree Road NE, Atlanta, GA 30326, and are writing to notify you of a data security incident that may have compromised the security of personal information of New Hampshire residents. PNF's investigation into this event is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, PNF does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Nature of the Data Security Event

In September of 2014, PNF noticed an escalation in fraud-related claims from customers for whom had used credit cards to make reservations through the company's website, www.pnf.com. PNF commenced an internal investigation to determine whether there were vulnerabilities in its systems that resulted in unauthorized access to customer information. To assist with its investigation, PNF engaged independent third-party forensics experts. The third-party forensics experts reported suspicious activity on PNF's web server. This server contained credit/debit card data. PNF has been working continuously to understand the nature and scope of the incident. This investigation is ongoing.

To date, the forensic investigators have not identified New Hampshire residents affected by this event. However, should PNF's investigation reveal that New Hampshire residents were affected by this incident, notice will be provided pursuant to New Hampshire's data breach notification laws.

Other Steps Taken and To be Taken

PNF takes this matter, and the security of the customer information in its care, seriously and is taking measures to restore the secure functionality of its systems. Upon noticing an escalation in fraud-related claims from its customers, PNF immediately took steps to identify potential vulnerabilities with its systems, remediate, and enhance the security of its systems. PNF also contacted the vendor that maintains its server requesting maintenance on the server and site. PNF continues to work closely with the third-party experts to identify the nature and scope of this incident and to remediate accordingly. While remediation occurs, PNF is not collecting credit/debit card data through its reservation website.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us a[redacted]

Very truly yours,

[redacted]

SMS:JEP

EXHIBIT B

Park 'N Fly Notifies Customers of Data Security Compromise

ATLANTA – Jan. 13, 2015 – Park 'N Fly ("PNF") has become aware of a security compromise involving payment card data processed through its e-commerce website. PNF has been working continuously to understand the nature and scope of the incident, and has engaged third-party data forensics experts to assist with its investigation. The data compromise has been contained. While the investigation is ongoing, it has been determined that the security of some data from certain payment cards that were used to make reservations through PNF's e-commerce website is at risk. The data potentially at risk includes the card number, cardholder's name and billing address, card expiration date, and CVV code. Other loyalty customer data potentially at risk includes email addresses, Park 'N Fly passwords, and telephone numbers.

PNF is encouraging customers to take steps to protect their identity and financial information, and has established a toll-free call center to answer customer questions. As the investigation continues, and out of an abundance of caution, PNF also is offering identity monitoring and identity protection services to potentially affected customers, free of charge for the next 12 months. To learn more about these services and how to enroll, please visit https://pnf.allclearid.com.

PNF also suggests that customers remain vigilant and seek to protect against possible identity theft or other financial loss by reviewing account statements for any unusual activity, notifying their credit card companies of the potential data compromise, and monitoring their credit reports. Under U.S. law, individuals are entitled to one free credit report annually from each of the three major credit bureaus. To obtain a free credit report, visit www.annualcreditreport.com or call, toll-free, (877) 322-8228.

At no charge, PNF customers can also have these credit bureaus place a "fraud alert" on their files that alerts creditors to take additional steps to verify their identity prior to granting credit in their names. Please note, however, that because it tells creditors to follow certain procedures to protect the individual's credit, it may also delay the ability to obtain credit while the agency verifies the individual's identity. As soon as one credit bureau confirms an individual's fraud alert, the others are notified to place fraud alerts on that individual's file. Any individual wishing to place a fraud alert, or who has questions regarding their credit report, can contact any one of the following agencies: Equifax, P.O. Box 105069, Atlanta, GA 30348-5069, 800-525-6285, www.equifax.com; Experian, P.O. Box 2002, Allen, TX 75013, 888-397-3742, www.experian.com; or TransUnion, P.O. Box 2000, Chester, PA 19022-2000, 800-680-7289, www.transunion.com. Information regarding security freezes may also be obtained from these sources.

The Federal Trade Commission (FTC) also encourages those who discover that their information has been misused to file a complaint with them. To file a complaint with the FTC, or to obtain additional information on identity theft and the steps that can be taken to avoid identity theft, the FTC can be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580, or at www.ftc.gov/idtheft or (877) ID-THEFT (877-438-4338); TTY: (866) 653-4261. This notice has not been delayed because of law enforcement; however, instances of known or suspected identity

theft should be reported to law enforcement, the Attorney General in the individual's state of residence, and the FTC. State Attorneys General may also have advice on preventing identity theft. Individuals can also learn more about placing a fraud alert or security freeze on their credit files by contacting the FTC or their state's Attorney General. For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, (919) 716-6400, www.ncdoj.gov. For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, (888) 743-0023, www.oag.state.md.us.

To better assist our customers whose card data may potentially have been affected, PNF has established a confidential, toll-free hotline to answer questions. This hotline is available Monday through Saturday, 8:00 a.m. to 8:00 p.m. C.S.T. and can be reached at (855) 683-1165. Park 'N Fly will post updates on this website, as additional information becomes available.

Park 'N Fly regrets any inconvenience this security compromise may cause. PNF is committed to protecting its customers and their information, and will continue a comprehensive response to thoroughly investigate and respond to the incident and improve its data security. The company is also is working with law enforcement and credit card brands.

Massachusetts residents please click here

For Massachusetts Residents:

The state of Massachusetts requires specific information be shared with residents who have experienced a breach of security or the unauthorized acquisition or use of personal information. Relevant information is included in the notice below.

Park 'N Fly Notifies Customers of Data Security Compromise

ATLANTA – Jan. 13, 2015 – Park 'N Fly ("PNF") has become aware of a security compromise involving payment card data processed through its e-commerce website. PNF has been working continuously to understand the nature and scope of the incident, and has engaged third-party data forensics experts to assist with its investigation. The data compromise has been contained. Please visit https://pnf.allclearid.com to learn more about the identity protection services being provided for potentially affected customers.

Under Massachusetts law, individuals have the right to obtain any police report filed in regard to this incident. If an individual is the victim of identity theft, he/she also has the right to file a police report and obtain a copy of it.

To further protect against possible identity theft or other financial loss, PNF encourages its customers to remain vigilant, to review their account statements, and to monitor their credit reports. Specific steps consumers can take to protect against the possibility of identity theft include closely monitoring financial statements for any unusual activity and monitoring credit reports. Under U.S. law, individuals are entitled to one free credit report annually from each of the three major credit bureaus. To obtain a free credit report, visit www.annualcreditreport.com, or call, toll-free, (877) 322-8228.

Under Massachusetts law, consumers may place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on an individual's credit report may delay, interfere with, or prevent the timely approval of any requests he/she makes for new loans, credit mortgages, employment, housing, or other services.

If an individual has been a victim of identity theft, and provides the credit reporting agency with a valid police report, it cannot charge the individual to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge individuals up to $5.00 each to place, temporarily lift, or permanently remove a security freeze.

To place a security freeze on one's credit report, individuals must send a written request to each of the three major consumer reporting agencies: Equifax (www.equifax.com), Experian (www.experian.com), and TransUnion (www.transunion.com) by regular, certified or overnight mail to the addresses below:

Equifax
P.O. Box 105069

Experian
P.O. Box 2002

TransUnion
P.O. Box 2000

Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

In order to request a security freeze, the individual will need to provide the following information:

1. Their full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If he/she has moved in the past five (5) years, provide the addresses where he/she has 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 an individual is 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 an individual is 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 a request to place a security freeze on a credit file report. The credit bureaus must also send written confirmation to an individual within five (5) business days and provide him/her with a unique personal identification number (PIN) or password, or both, that can be used by him/her 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 an individual's credit report, he/she 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 the individual when he/she placed the security freeze, as well as the identities of those entities or individuals he/she would like to receive his/her credit report or the specific period of time he/she wants the credit report available. The credit reporting agencies have three (3) business days after receiving an individual's request to remove the security freeze.

To obtain additional information regarding identity theft and the steps one can take to avoid identity theft, an individual may contact the Federal Trade Commission. They can be reached at: Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580, or at www.ftc.gov/idtheft, 1-877-ID-THEFT (I-877-438-4338; TTY: 1-866-653-4261). The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. The Massachusetts Attorney General may also have advice on preventing identity theft.

To better assist our customers who may be affected, PNF has established a confidential, toll-free hotline to answer questions from affected customers. This hotline is available Monday through Saturday, 8:00 a.m. to 8:00 p.m. C.S.T. and can be reached at (855) 683-1165. PNF will post

updates on this data security event at www.pnf.com/security-update, as additional information becomes available.

Park 'N Fly regrets any inconvenience this security compromise may cause. PNF is committed to protecting its customers and their information, and will continue a comprehensive response to thoroughly investigate and respond to the incident and improve its data security. The company is also is working with law enforcement and credit card brands.

# # #

EXHIBIT C

Park 'N Fly Notifies Customers of Data Security Compromise

ATLANTA – Jan. 13, 2015 – Park 'N Fly ("PNF") has become aware of a security compromise involving payment card data processed through its e-commerce website. PNF has been working continuously to understand the nature and scope of the incident, and has engaged third-party data forensics experts to assist with its investigation. The data compromise has been contained. While the investigation is ongoing, it has been determined that the security of some data from certain payment cards that were used to make reservations through PNF's e-commerce website is at risk. The data potentially at risk includes the card number, cardholder's name and billing address, card expiration date, and CVV code. Other loyalty customer data potentially at risk includes email addresses, Park 'N Fly passwords, and telephone numbers.

PNF is encouraging customers to take steps to protect their identity and financial information, and has established a toll-free call center to answer customer questions. As the investigation continues, and out of an abundance of caution, PNF also is offering identity monitoring and identity protection services to potentially affected customers, free of charge for the next 12 months. PNF customers can visit www.pnf.com/security-update to learn more about this data security event and the support and services being provided.

PNF also suggests that customers remain vigilant and seek to protect against possible identity theft or other financial loss by reviewing account statements for any unusual activity, notifying their credit card companies of the potential data compromise, and monitoring their credit reports. Under U.S. law, individuals are entitled to one free credit report annually from each of the three major credit bureaus. To obtain a free credit report, visit www.annualcreditreport.com or call, toll-free, (877) 322-8228.

At no charge, PNF customers can also have these credit bureaus place a "fraud alert" on their files that alerts creditors to take additional steps to verify their identity prior to granting credit in their names. Please note, however, that because it tells creditors to follow certain procedures to protect the individual's credit, it may also delay the ability to obtain credit while the agency verifies the individual's identity. As soon as one credit bureau confirms an individual's fraud alert, the others are notified to place fraud alerts on that individual's file. Any individual wishing to place a fraud alert, or who has questions regarding their credit report, can contact any one of the following agencies: Equifax, P.O. Box 105069, Atlanta, GA 30348-5069, 800-525-6285, www.equifax.com; Experian, P.O. Box 2002, Allen, TX 75013, 888-397-3742, www.experian.com; or TransUnion, P.O. Box 2000, Chester, PA 19022-2000, 800-680-7289, www.transunion.com. Information regarding security freezes may also be obtained from these sources.

The Federal Trade Commission (FTC) also encourages those who discover that their information has been misused to file a complaint with them. To file a complaint with the FTC, or to obtain additional information on identity theft and the steps that can be taken to avoid identity theft, the FTC can be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580, or at www.ftc.gov/idtheft or (877) ID-THEFT (877-438-4338); TTY: (866) 653-4261. This notice has not been delayed because of law enforcement; however, instances of known or suspected identity

theft should be reported to law enforcement, the Attorney General in the individual's state of residence, and the FTC. State Attorneys General may also have advice on preventing identity theft. Individuals can also learn more about placing a fraud alert or security freeze on their credit files by contacting the FTC or their state's Attorney General. For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, (919) 716-6400, www.ncdoj.gov. For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, (888) 743-0023, www.oag.state.md.us.

To better assist our customers whose card data may potentially have been affected, PNF has established a confidential, toll-free hotline to answer questions. This hotline is available Monday through Saturday, 8:00 a.m. to 8:00 p.m. C.S.T. and can be reached at (855) 683-1165. Customers can also visit www.pnf.com/security-update for additional information and updates.

Park 'N Fly regrets any inconvenience this security compromise may cause. PNF is committed to protecting its customers and their information, and will continue a comprehensive response to thoroughly investigate and respond to the incident and improve its data security. The company is also is working with law enforcement and credit card brands.

Media Contact:
Mary Gallen
(404) 364-8145
media@pnf.com

###