

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 working with law enforcement and credit card brands.

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

###

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 working with law enforcement and credit card brands.

Massachusetts residents please [click here](#)