Towne Park Security Incident

Towne Park, LLC, and its affiliates (collectively, "Company"), is a professional parking and hospitality service provider that takes seriously the privacy and security of the personal information provided to us by our customers. This notice is to inform our customers about an incident involving elements of that information.

The Company recently discovered that cyber attackers executed a sophisticated attack to gain unauthorized access to certain Company point of sale systems. In the course of this incident, the attackers may have obtained some elements of customers' personal information involved in the use of their payment cards at parking facilities operated by Company. After discovering the incident, we promptly commenced an investigation, including working with the card brands, and leading investigation and IT security firms to determine the facts. We value and respect the privacy and security of your information, and we sincerely apologize for any concern or inconvenience this may cause you.

What Happened

On June 20, 2016, the Company discovered that certain of its point of sale systems at certain locations were affected by malware. The attacks did not affect all of our locations, and depending on the location, the malware may have operated between January 22, 2016 and June 20, 2016, although most of the systems were affected during a shorter timeframe.

What Information Was Involved

The malware was designed to collect certain payment card information, including credit/debit card number, security code and expiration date. However, our equipment generally does not capture the cardholder's name, we do not believe that information was involved in this attack. Additionally, we do not believe other elements of personal information, such as address, Social Security numbers, dates of birth, or drivers' license numbers were captured by the malware.

What We Are Doing

We have been and continue to work with the investigation and IT security firms that we engaged and which were approved by the major credit card companies. We believe we have contained the attack and presently we are in the process of adding to the security of our point of sale and other relevant systems and equipment.

What You Can Do

We have outlined below steps that you can take to protect your personal information in the event you are affected by this incident. If you used a payment card at one of the facilities we operate, it does not mean you were affected; we believe most of our customers were not affected. However, we believe that you should review and take some of the steps below in the abundance of caution,

and consider adopting some or all of these best practices in the future. Of course, if you believe your payment card may have been affected, please contact your bank or card issuer immediately.

For More Information

If you have any further questions, please call **410-295-8066**, or email at securitynotifications@townepark.com.

What You Should Do To Protect Your Personal Information

We recommend you remain vigilant and consider taking one or more of the following steps to protect your personal information:

1. Contact the nationwide credit-reporting agencies as soon as possible to:
   - Add a fraud alert statement or security freeze to your credit file at all three national credit-reporting agencies: Equifax, Experian, and TransUnion. You only need to contact one of the three agencies listed below; your request will be shared with the other two agencies. This fraud alert will remain on your credit file for 90 days.
   - Remove your name from mailing lists of pre-approved offers of credit for approximately six months.
   - Obtain a free copy of your credit report by going to www.annualcreditreport.com.

Equifax	Experian	TransUnion
P.O. Box 740256	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
(800) 525-6285	(888) 397-3742	(800) 888-4213
www.equifax.com	www.experian.com/consumer	www.transunion.com

2. Please review all bills and credit card statements closely to determine whether you have been charged for items you did not contract for or purchase. Review all of your bank account statements frequently for checks, purchases, or deductions not made by you. Note that even if you do not find suspicious activity initially, you should continue to check this information periodically since identity thieves sometimes delay their use of stolen personal information.

3. The Federal Trade Commission ("FTC") offers consumer assistance and educational materials relating to identity theft, privacy issues, and how to avoid identity theft. You may contact the FTC by visiting www.ftc.gov or www.consumer.gov/idtheft, calling (877) 438-4338, or writing to the FTC at the address below. If you suspect or know that you are the victim of identity theft, you should contact local police or your state attorney general. You can also report such activity to the Fraud Department of the FTC, which will collect all relevant information and make it available to law-enforcement agencies. The mailing

address for the FTC is: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580.

You also can obtain additional information from the FTC and the nationwide credit bureaus about fraud alerts and security freezes. You can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide credit bureaus listed above. As soon as that bureau processes your fraud alert, it will notify the other two bureaus, which then must also place fraud alerts in your file. In addition, you can visit the credit bureau links above to determine if and how you may place a security freeze on your credit report to prohibit a credit bureau from releasing information from your credit report without your prior written authorization.

4. ***For North Carolina Residents***: For more information on identity theft please contact either the Federal Trade Commission at the contact information provided above, or North Carolina's Attorney General's Office, Address: 9001 Mail Service Center, Raleigh, NC 27699-9001; Telephone: (919) 716-6400; Fax: (919) 716-6750; website: www.ncdoj.com/

5. ***For Maryland Residents***: To obtain additional information about avoiding identity theft, please contact the Maryland Attorney General's Office, using the contact information below: Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202, Phone: (410) 576-6300, Toll-Free (in Maryland): (888) 743-0023, Website: https://www.oag.state.md.us/contact.htm

6. ***For Rhode Island Residents***: To obtain additional information about avoiding identity theft, please contact the Rhode Island Office of the Attorney General at 150 South Main Street, Providence, Rhode Island 02903, Phone (401) 274-4400.

7. ***For Massachusetts Residents***: Under Massachusetts law, you 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.

   Massachusetts law also allows consumers to 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 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, 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. In all other cases, a credit reporting agency may charge you up to $5.00 each to place, temporarily lift, or permanently remove a security freeze. To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies listed above.

   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, the addresses where you have lived over the prior five years;
5. Proof of current address (e.g., a current utility bill or telephone bill);
6. A legible photocopy of a government issued identification card (e.g., state driver's license or ID card or military identification);
7. If you are a victim of identity theft, 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, 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 reporting agencies 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 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. The credit reporting agencies have three (3) business days after receiving your request to remove the security freeze.