BakerHostetler

Baker&Hostetler LLP

312 Walnut Street
Suite 3200
Cincinnati, OH 45202-4074

T 513.929.3400
F 513.929.0303
www.bakerlaw.com

Craig A. Hoffman
direct dial: 513.929.3491
cahoffman@bakerlaw.com

December 28, 2017

VIA EMAIL (SECURITYBREACH@ATG.WA.GOV)
AND OVERNIGHT MAIL

Attorney General Bob Ferguson
Office of the Attorney General
Consumer Protection Division
800 5th Ave., Suite 2000
Seattle, WA 98104-3188

Re: Incident Notification

Dear Attorney General Ferguson:

Forever 21, Inc. ("Forever 21") understands the importance of protecting the payment card information of its customers, and Forever 21's payment processing system has been using encryption technology since 2015. In mid-October 2017, Forever 21 received a report from a third party suggesting that there may have been unauthorized access to data form payment cards that were used in certain Forever 21 stores. Forever 21 immediately began an investigation and engaged leading payment technology and security firms to assist. On November 14, 2017, Forever 21 issued a press release and posted information on its website notifying customers of its investigation.

Findings from the investigation indicate that the encryption technology on some point-of-sale (POS) devices at some stores was not always on. The investigation also found signs of unauthorized network access and installation of malware on some POS devices designed to search for payment card data. The malware searched only for track data read from a payment card as it was being routed through the POS device. In most instances, the malware only found track data that did not have cardholder name – only card number, expiration date, and internal verification code – but occasionally the cardholder name was found.

The investigation found that encryption was off and malware was installed on some devices in some U.S. stores at varying times during the period from April 3, 2017 to November 18, 2017. In some stores, this scenario occurred for only a few days or several weeks, and in

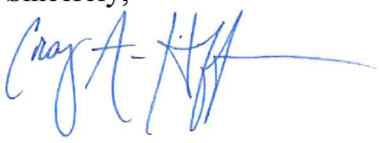
some stores this scenario occurred for most or all of the timeframe. Each Forever 21 store has multiple POS devices, and in most instances only one or a few of the POS devices were involved. Additionally, Forever 21 stores have a device that keeps a log of completed payment card transaction authorizations. When encryption was off, payment card data was being stored in this log. In a group of stores that were involved in this incident, malware was installed on the log devices that was capable of finding payment card data from the logs, so if encryption was off on a POS device prior to April 3, 2017 and that data was still present in the log file at one of these stores, the malware could have found that data. Payment cards used on Forever 21's website, www.forever21.com, were not affected.

Forever 21 does not have sufficient information to determine the name and mailing addresses of individuals that used their cards at the affected stores. Forever 21, therefore, is unable to identify the number of Washington residents that used a card during the timeframe of this incident. However, on December 28, 2017, pursuant to Wash. Rev. Code § 19.255.010, Forever 21 provided substitute notification to Washington residents who may have used their payment cards at Forever 21 stores in the U.S. by issuing a press release and updating the statement on its website. A copy of the press release and website statement are enclosed. Notification is being provided without unreasonable delay. In addition, Forever 21 established a dedicated call center that customers can call with related questions.

Forever 21 is working with its payment processor, POS device provider, and third-party experts to address the operation of encryption on the POS devices and will continue to work with security firms to evaluate ways to enhance its security measures. Forever 21 is in contact with law enforcement and we will continue to support law enforcement's investigation of this incident.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,



Craig A. Hoffman
Partner

Enclosure

Press Release

Media contact:
press@forever21.com

Forever 21 Reports Findings from Investigation of Payment Card Security Incident

LOS ANGELES, CA (December 28, 2017) - Forever 21, Inc. is providing additional information about the payment card security incident that we first reported on November 14, 2017. This press release explains the incident, measures we have taken, and some steps you can take in response.

Since 2015, Forever 21's payment processing system has been using encryption technology. After receiving a report from a third party in mid-October 2017 suggesting there may have been unauthorized access to data from payment cards that were used at certain Forever 21 stores, we immediately began an investigation. We hired leading payment technology and security firms to assist. The investigation determined that the encryption technology on some point-of-sale (POS) devices at some stores was not always on. The investigation also found signs of unauthorized network access and installation of malware on some POS devices designed to search for payment card data. The malware searched only for track data read from a payment card as it was being routed through the POS device. In most instances, the malware only found track data that did not have cardholder name – only card number, expiration date, and internal verification code – but occasionally the cardholder name was found.

The investigation found that encryption was off and malware was installed on some devices in some U.S. stores at varying times during the period from April 3, 2017 to November 18, 2017. In some stores, this scenario occurred for only a few days or several weeks, and in some stores this scenario occurred for most or all of the timeframe. Each Forever 21 store has multiple POS devices, and in most instances only one or a few of the POS devices were involved. Additionally, Forever 21 stores have a device that keeps a log of completed payment card transaction authorizations. When encryption was off, payment card data was being stored in this log. In a group of stores that were involved in this incident, malware was installed on the log devices that was capable of finding payment card data from the logs, so if encryption was off on a POS device prior to April 3, 2017 and that data was still present in the log file at one of these stores, the malware could have found that data.

Forever 21 has been working with its payment processors, POS device provider, and third-party experts to address the operation of encryption on the POS devices in all Forever 21 stores. Forever 21 stores outside of the U.S. have different payment processing systems, and our investigation is ongoing to determine if any of these stores are involved. *Payment cards used on Forever 21's website, www.forever21.com, were not affected.*

In addition to addressing encryption, Forever 21 is continuing to work with security firms to enhance its security measures. We also continue to work with the payment card networks so that the banks that issue payment cards can be made aware of this incident. Lastly, we will continue to support law enforcement's investigation of this incident.

It is always advisable to remain vigilant to the possibility of fraud by reviewing your payment card statements for any unauthorized activity. Customers should immediately report any unauthorized charges to their card issuer because payment card rules generally provide that cardholders are not responsible for unauthorized charges reported in a timely manner. The phone number to call is usually on the back of the payment card.

We regret this incident occurred and any concern this may have caused. If customers have questions, they can visit www.Forever21.com/ProtectingOurCustomers or call 1-855-560-4992 Monday through Friday between the hours of 8:00 a.m. to 6:00 p.m. P.S.T.

ABOUT FOREVER 21

Forever 21, Inc., headquartered in Los Angeles, California, is a fashion retailer of women's, men's and kids clothing and accessories and is known for offering the hottest, most current fashion trends at a great value to consumers. This model operates by keeping the store exciting with new merchandise brought in daily. Founded in 1984, Forever 21 operates more than 815 stores in 57 countries with retailers in the United States, Australia, Brazil, Canada, China, France, Germany, Hong Kong, India, Israel, Japan, Korea, Latin America, Mexico, Philippines and United Kingdom. For more information, please visit: www.newsroom.forever21.com.

Website Notice

Forever 21 Reports Findings from Investigation of Payment Card Security Incident

California residents please click here

Forever 21, Inc. is providing additional information about the payment card security incident that we first reported on November 14, 2017. This notice explains the incident, measures we have taken, and some steps you can take in response.

Since 2015, Forever 21's payment processing system has been using encryption technology. After receiving a report from a third party in mid-October 2017 suggesting there may have been unauthorized access to data from payment cards that were used at certain Forever 21 stores, we immediately began an investigation. We hired leading payment technology and security firms to assist. The investigation determined that the encryption technology on some point-of-sale (POS) devices at some stores was not always on. The investigation also found signs of unauthorized network access and installation of malware on some POS devices designed to search for payment card data. The malware searched only for track data read from a payment card as it was being routed through the POS device. In most instances, the malware only found track data that did not have cardholder name – only card number, expiration date, and internal verification code – but occasionally the cardholder name was found.

The investigation found that encryption was off and malware was installed on some devices in some U.S. stores at varying times during the period from April 3, 2017 to November 18, 2017. In some stores, this scenario occurred for only a few days or several weeks, and in some stores this scenario occurred for most or all of the timeframe. Each Forever 21 store has multiple POS devices, and in most instances only one or a few of the POS devices were involved. Additionally, Forever 21 stores have a device that keeps a log of completed payment card transaction authorizations. When encryption was off, payment card data was being stored in this log. In a group of stores that were involved in this incident, malware was installed on the log devices that was capable of finding payment card data from the logs, so if encryption was off on a POS device prior to April 3, 2017 and that data was still present in the log file at one of these stores, the malware could have found that data.

Forever 21 has been working with its payment processors, POS device provider, and third-party experts to address the operation of encryption on the POS devices in all Forever 21 stores. Forever 21 stores outside of the U.S. have different payment processing systems, and our investigation is ongoing to determine if any of these stores are involved. *Payment cards used on Forever 21's website, www.forever21.com, were not affected.*

In addition to addressing encryption, Forever 21 is continuing to work with security firms to enhance its security measures. We also continue to work with the payment card networks so that the banks that issue payment cards can be made aware of this incident. Lastly, we will continue to support law enforcement's investigation of this incident.

It is always advisable to remain vigilant to the possibility of fraud by reviewing your payment card statements for any unauthorized activity. You should immediately report any unauthorized charges to your card issuer because payment card rules generally provide that cardholders are not responsible for unauthorized charges reported in a timely manner. The phone number to call is usually on the back of your payment card. Please see the section that follows this notice for additional steps you may take.

We regret this incident occurred and any concern this may have caused you. If you have questions, please call 1-855-560-4992 Monday through Friday between the hours of 8:00 a.m. to 6:00 p.m. P.S.T.

MORE INFORMATION ON WAYS TO PROTECT YOURSELF

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

Equifax
Phone: 1-800-685-1111
P.O. Box 740256
Atlanta, Georgia 30348
www.equifax.com

Experian
Phone: 888-397-3742
P.O. Box 9554
Allen, Texas 75013
www.experian.com

TransUnion
Phone: 888-909-8872
P.O. Box 105281
Atlanta, GA 30348-5281
www.transunion.com

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

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

Fraud Alerts: To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain enhanced procedures to protect you. It also may delay your ability to obtain credit. You may place a fraud alert in your file by calling one of the three nationwide consumer reporting agencies

Equifax, PO Box 740256, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
Experian, PO Box 9554, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-680-7289

As soon as that agency processes your fraud alert, it will notify the other two, which then also must place fraud alerts in your file. You may choose between two types of fraud alert. An initial alert (Initial Security Alert) stays in your file for at least 90 days. An extended alert (Extended Fraud Victim Alert) stays in your file for seven years. To place either of these alerts, a consumer reporting agency will require you to provide appropriate proof of your identity, which may include your Social Security number. If you ask for an extended alert, you will have to provide an identity theft report. An identity theft report includes a copy of a report you have filed with a federal, state, or local law enforcement agency, and additional information a consumer reporting agency may require you to submit. For more detailed information about the identity theft report, visit www.ftc.gov/idtheft/.

Security Freeze: You may wish to place a "security freeze" (also known as a "credit freeze") on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the

consumer reporting agencies without your consent. There may be fees for placing, lifting, and/or removing a security freeze, which generally range from $5-$20 per action. *Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually.* In order to request a security freeze, the consumer reporting agencies may require proper identification prior to honoring your request and ask that you provide:

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 the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

As the instructions for establishing a security freeze differ from state to state, please contact the three consumer reporting agencies to find out more information.

Fair Credit Reporting Act: You also have rights under the federal Fair Credit Reporting Act (FCRA), which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has published a list of the primary rights created by the FCRA (https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf), and that article refers individuals seeking more information to visit www.ftc.gov/credit. The FTC's list of FCRA rights includes:

- You have the right to receive a copy of your credit report. The copy of your report must contain all the information in your file at the time of your request.
- Each of the nationwide credit reporting companies – Equifax, Experian, and TransUnion – is required to provide you with a free copy of your credit report, at your request, once every 12 months.
- You are also entitled to a free report if a company takes adverse action against you, like denying your application for credit, insurance, or employment, and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You are also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; if you are on welfare; or if your report is inaccurate because of fraud, including identity theft.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited. You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you receive based on information in your credit report.
- You may seek damages from violators.

Identity theft victims and active duty military personnel have additional rights.

If you are a resident of Maryland, you may contact the Maryland Attorney General's Office at 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

If you are a resident of North Carolina, you may contact the North Carolina Attorney General's Office at 9001 Mail Service Center, Raleigh, NC 27699, www.ncdoj.gov, 1-919-716- 6400.

If you are a resident of Massachusetts, note that you have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may charge you a fee of up to $5 to place a security freeze on your account, and may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request. There is no charge, however, to place, lift or remove a security freeze if you have been a victim of identity theft and you provide the consumer reporting agencies with a valid police report.

If you are a resident of Rhode Island, you may obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General at 150 South Main Street Providence, RI 02903, www.riag.ri.gov, (401)-274-4400. You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may charge you a fee of up to $10 to place a security freeze on your account, and may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request. There is no charge, however, to place, lift or remove a security freeze if you have been a victim of identity theft and you provide the consumer reporting agencies with a valid police report.

If you are a resident of West Virginia, you have the right to the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.