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

NOTICE OF DATA BREACH

What Happened

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.

What Information Was Involved

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.

What We Are Doing

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.

What You Can Do

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.

For More Information

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