

FOREVER  
TWENTY ONE

2001 SOUTH ALAMEDA STREET ■ LOS ANGELES, CALIFORNIA 90058 ■ PHONE (213) 741-5100 ■ FAX (213) 741-8995

September 16, 2008

**VIA US MAIL**

Office of the Attorney General  
900 East Main Street  
Richmond, VA 23219

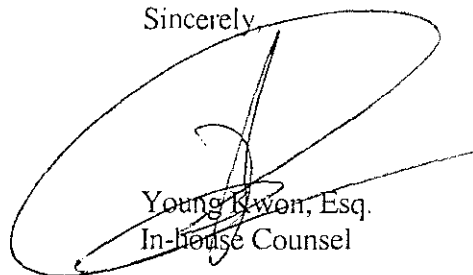
**Re: Notice of Security Breach Incident**

Dear State Official:

Forever 21, Inc. is writing to inform you of a recent security breach incident in which unauthorized persons, now in custody, illegally accessed certain customer payment card information. Please see details described in the form of customer security breach notice posted on our website, a copy of which is attached to this letter. Although the incident affected approximately 98,930 credit and debit card numbers, more than half of these payment card numbers are no longer active or have expired expiration dates. Because the data compromised did not include customer names or addresses, we do not know how many customers' personal information may have been affected in your state.

Please contact me at 213-741-8906 if you need additional information.

Sincerely,



Young Kwon, Esq.  
In-house Counsel

Encl.

September 12, 2008

## **Important Public Notice Regarding Customer Personal Information**

Dear Valued Customers:

Law enforcement recently informed us that our systems may have been illegally accessed to obtain customer payment card information. We have determined that this incident may have affected a subset of our customers who shopped at our stores on the following nine dates: March 25, 2004; March 26, 2004; June 23, 2004; July 2, 2004; July 3, 2004; August 4, 2007; August 5, 2007; August 13, 2007; and August 14, 2007. In addition, the incident may have affected customers who shopped at our Fresno, California store located at 567 E. Shaw Ave. between November 26, 2003 and October 24, 2005.

On August 5, 2008, the U.S. Department of Justice in Boston filed indictments against 3 individuals alleged to have committed crimes involving credit card fraud against 12 retailers. That morning, Forever 21 was contacted by the U.S. Secret Service and was advised that our company was identified in the indictment as one of the retail victims. We subsequently received from the Secret Service a disk of potentially compromised file data. We promptly retained forensic consultants to help us examine the file data and our systems. Based on that investigation, we believe that the unauthorized persons accessed older credit and debit card transaction data for approximately 98,930 credit and debit card numbers. Approximately 20,500 of these numbers were obtained from the Fresno store transaction data. The data included credit and debit card numbers and in some instances expiration dates and other card data, but did not include customer name and address. More than half of the affected payment card numbers are no longer active or have expired expiration dates.

We have been working with our acquiring bank and payment card networks to resolve the situation. Your card issuing institution may send you a written notice mailed to the address related to the account number about this incident. We have also contacted the three principal credit reporting bureaus, Equifax, Experian and TransUnion, to advise them of the situation. Since 2007 when the Payment Card Industry Data Security Standards (the

“PCI Standards”) were imposed, our systems have been certified to be in compliance with the PCI Standards, including the data encryption standards. After we were informed of this incident, we adopted additional proactive security measures and continue to regularly monitor our systems for intrusions.

*If you shopped at our stores on the nine dates above or at our Fresno store during the time period indicated, we are alerting you so that you may take steps to protect yourself from payment card fraud. It is important for you to carefully monitor your accounts and report suspicious transactions to your issuing financial institution immediately. As a further precaution, you may wish to place a fraud alert on your credit file. Specific information about protecting your credit lines and financial information is linked to this notice. **Please review it closely.** We also recommend that you review the identity theft materials posted for consumers on the Federal Trade Commission’s (the “FTC’s”) Web site, [www.consumer.gov/idtheft/](http://www.consumer.gov/idtheft/), and in particular, the posted copy of the FTC’s booklet, “*Take Charge: Fighting Back Against Identity Theft.*”*

Should you have any questions about this incident or need additional information, we have designated a customer service number for you to call, **1-888-757-4447.**

We regret any inconvenience or concern that this incident may have caused you and look forward to serving you in the years ahead.

Sincerely,

Forever 21, Inc.

## *[Information for the Additional Link]*

### **Steps to take to protect your credit and identity**

Should you believe your identity has been stolen or that you are at risk of having your identity stolen, you can follow the Federal Trade Commission's ("FTC's") guidelines on protecting yourself against identity theft. The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop and avoid them.

First, you should contact your credit and bank card issuers and other financial institutions as soon as possible to review your accounts for unauthorized charges or transactions. If there are unauthorized charges or if you otherwise believe that your card number has been taken by an unauthorized person, you should inform your card issuer on the phone and in writing that the charges were not authorized by you, and you should request that your current card account be closed and a new card issued in your name.

You may wish to consider placing a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing credit accounts. Because creditors seek additional verification from you when a fraud alert is in place on your credit file, one effect of the fraud alert is that it slows the processing time for opening new accounts and making changes on your existing accounts.

To place a fraud alert on your credit file, call any one of the three major credit bureaus. As soon as one credit bureau processes your fraud alert, it will notify the other credit bureaus on your behalf to place fraud alerts. All three credit reports will be sent to you, free of charge, for your review.

Equifax  
1-800-525-6285

Experian  
1-888-397-3742

TransUnionCorp  
1-800-680-7289

You may also have right under applicable state law to request in writing that a "security freeze" be put on your credit report. A security freeze will prohibit a credit reporting agency from releasing any information in your credit report without your express authorization.

Even if you do not initially find any suspicious activity on your card accounts, credit reports and/or bank statements, the FTC recommends that you check your credit reports, card charges and financial statements regularly. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports, card charges and financial statements periodically can help you spot problems and address them quickly. Once a year you can obtain a free credit report by calling 1- 877-322-8228 or going online to [www.annualcreditreport.com](http://www.annualcreditreport.com).

If you find suspicious activity on your accounts or have reason to believe that your personal information is being misused, it may be necessary for you to file a police report and obtain a copy of that police report. Many creditors require the information the police report contains to absolve you of the fraudulent debts.

You may also want to file a complaint with the FTC, which will be logged into its database of identity theft cases used by law enforcement agencies for investigations. To get free information or file a complaint with the FTC, you may call the FTC at 1-877-438-4338, or use the complaint form at <http://www.consumer.gov/idtheft/>.