[COMPANY Letterhead]

[Recipient Name]
[Recipient Address 1]
[Recipient Address 2]

[Date]

Dear _____:

We previously notified you on May 17, 2013 about a security incident affecting your credit or debit card that you used on **(insert website)** recently.

This letter is a formal explanation of what happened and steps you can take to further protect your information.

On approximately May 14, 2013, an unauthorized third party obtained access to TJG, Inc. d/b/a Target Marketing ("Target Marketing")'s online e-commerce platform, and obtained certain personal information associated with recent purchases on the site. This information included your name, email, address, credit / debit card number, expiration date, and CVV code.

On May 15, 2013 (the day after the unauthorized access to the site), Target Marketing's service provider identified the site breach and immediately implemented security measures designed to stop the attack and prevent it from recurring. These measures included applying security patches to the relevant systems, and hiring experts to review and coordinate additional safeguards. Target Marketing is also working with the payment card brands concerning the specific payment cards at issue in this incident.

Nevertheless, we are writing to make you aware of this incident so that you can alert your financial institution to cancel and reissue you a new card, as they determine prudent.

If you have further questions, you may contact Target Marketing toll-free at 888-780-8316 between 9:00 am and 5:00 pm, EST. Additionally, we have enclosed information on steps you can take to further protect your information.

Target Marketing takes this matter very seriously and deeply regrets any inconvenience or concern that it may cause you.

Sincerely,

Target Marketing

Jay Nathanson
President
Target Marketing
11049 Lakeridge Parkway
Ashland, VA 23005
Enclosure

Steps You Can Take To Further Protect Your Information

- **Review Your Account Statements**

As a precautionary measure, we recommend that you review your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, or the Federal Trade Commission.

- **Credit Report Monitoring**

You may obtain a free copy of your credit report from each of the 3 major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at http://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies shown below.

Equifax (800) 685-1111 www.equifax.com P.O. Box 740241 Atlanta, GA 30374	Experian (888) 397-3742 www.experian.com 535 Anton Blvd., Suite 100 Costa Mesa, CA 92626	TransUnion (800) 916-8800 www.transunion.com P.O. Box 6790 Fullerton, CA 92834

- **Additional Free Resources on Identity Theft**

You may wish to review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit http://www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). **Maryland residents** may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at http://www.oag.state.md.us/idtheft, or by sending an email to idtheft@oag.state.md.us, or calling 410-576-6491. **North Carolina residents** may wish to review information provided by the North Carolina Attorney General at http://www.ncdoj.gov, by calling 8770566-7226, or writing to 9001 Mail Service Center, Raleigh, North Carolina 27699.

- **Fraud Alert**

You may consider placing a fraud alert on your credit report. This fraud alert statement informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

- **Security Freeze**

In some U.S. states, you have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. Additionally, if you request a security freeze from a consumer reporting agency there may be a fee up to $10 to place, lift, or remove the security freeze; however, this fee may be less in certain states (in MA, up to $5). In order to place a security freeze, you may be required to provide the

consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement. You must separately place a security freeze on your credit file with each credit reporting agency.