

## Important Notice: Unauthorized access to payment card data in U.S. stores



We wanted to make you aware of unauthorized access to Target payment card data. The unauthorized access may impact guests who made credit or debit card purchases in our U.S. stores from Nov. 27 to Dec. 15, 2013. Your trust is a top priority for Target, and we deeply regret the inconvenience this may cause. The privacy and protection of our guests' information is a matter we take very seriously and we have worked swiftly to resolve the incident.

We began investigating the incident as soon as we learned of it. We have determined that the information involved in this incident included customer name, credit or debit card number, and the card's expiration date and CVV.

We are partnering with a leading third-party forensics firm to conduct a thorough investigation of the incident and to examine additional measures we can take that would be designed to help prevent incidents of this kind in the future. Additionally, Target alerted authorities and financial institutions immediately after we discovered and confirmed the unauthorized access, and we are putting our full resources behind these efforts.

We recommend that you closely review the information provided in this letter for some steps that you may take to protect yourself against potential misuse of your credit and debit information. You should remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and monitoring free credit reports. If you discover any suspicious or unusual activity on your accounts or suspect fraud, be sure to report it immediately to your financial institutions. In addition, you may contact the Federal Trade Commission ("FTC") or law enforcement to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC's Web site, at [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft), or call the FTC, at (877) IDTHEFT (438-4338) or write to Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

You may also periodically obtain credit reports from each nationwide credit reporting agency. If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit reporting agency delete that information from your credit report file. In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to [www.AnnualCreditReport.com](http://www.AnnualCreditReport.com) or by calling (877) 322-8228. You may contact the nationwide credit reporting agencies at:

Equifax  
(800) 525-6285  
P.O. Box 740241  
Atlanta, GA 30374-0241 Allen,  
TX 75013  
[www.equifax.com](http://www.equifax.com)

Experian  
(888) 397-3742  
P.O. Box 9532  
[www.experian.com](http://www.experian.com)

TransUnion  
(800) 680-7289  
Fraud Victim Assistance Division  
P.O. Box 6790  
Fullerton, CA 92834-6790  
[www.transunion.com](http://www.transunion.com)

In addition, you may obtain information from the FTC and the credit reporting agencies 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 reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file. In addition, you can contact the nationwide credit reporting

agencies regarding if and how you may place a security freeze on your credit report to prohibit a credit reporting agency from releasing information from your credit report without your prior written authorization.

Again, we want to stress that we regret any inconvenience or concern this incident may cause you. Be assured that we place a top priority on protecting the security of our guests' personal information. Please do not hesitate to contact us at 866-852-8680 or visit Target's website if you have any questions or concerns. If you used a non-Target credit or debit card at Target between Nov. 27 and Dec. 15 and have questions or concerns about activity on your card, please contact the issuing bank by calling the number on the back of your card.

IF YOU ARE AN IOWA RESIDENT: You may contact local law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. You can contact the Iowa Attorney General at:

Office of the Attorney General  
1305 E. Walnut Street  
Des Moines, IA 50319  
(515) 281-5164  
[www.iowaattorneygeneral.gov](http://www.iowaattorneygeneral.gov)

IF YOU ARE A MARYLAND RESIDENT: You may obtain information about avoiding identity theft from the FTC or the Maryland Attorney General's Office. These offices can be reached at:

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

Office of the Attorney General  
Consumer Protection Division  
200 St. Paul Place  
Baltimore, MD 21202  
(888) 743-0023  
[www.oag.state.md.us](http://www.oag.state.md.us)

IF YOU ARE A NORTH CAROLINA RESIDENT: You may obtain information about preventing identity theft from the FTC or the North Carolina Attorney General's Office. These offices can be reached at:

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

North Carolina Department of Justice  
Attorney General Roy Cooper  
9001 Mail Service Center  
Raleigh, NC 27699-9001  
(877) 566-7226  
<http://www.ncdoj.com>

IF YOU ARE A MASSACHUSETTS RESIDENT: 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.