



CHRIS CHRISTIE
Governor

KIM GUADAGNO
Lt. Governor

New Jersey Office of the Attorney General

Division of Consumer Affairs
Office of the Director
124 Halsey Street, 7th Floor, Newark NJ 07102



JOHN J. HOFFMAN
Acting Attorney General

ERIC T. KANEFSKY
Director

Mailing Address:
P.O. Box 45027
Newark, NJ 07101
(973) 504-6534

Important ALERT for New Jersey Consumers:

Important Steps to Protect Yourself After the Data Breach at Target

Updated January 16, 2014

The New Jersey Division of Consumer Affairs and the Office of the Attorney General are paying close attention to the data breach in which criminals hacked Target's computer system, possibly compromising the security and stealing the personal information of tens of millions of credit and debit card holders who shopped at Target stores in the United States.

The Division of Consumer Affairs urges consumers to take the following steps, to protect themselves against identity theft following this data breach:

First, take advantage of Target's offer for free credit monitoring.

Target is partnering with Experian, a credit card monitoring firm, to offer 12 months of free credit card monitoring through Experian's "ProtectMyID" service.

According to Target, this offer is available to all consumers who shopped in U.S. Target stores, regardless of whether they were affected by the data breach.

To take advantage of this free offer:

- Enter your name and email address at creditmonitoring.target.com before **April 23, 2014**.
- Within 72 hours, you will receive an email from Target with an activation code and instructions on what to do next.
- You will have until **April 30, 2014** to follow those steps and register with ProtectMyID.
- NOTE: Consumers who do not have Internet access can obtain an access code by calling Target at 866-852-8680. They can then enroll in the free credit monitoring by calling Experian at 888-270-0056.

For more information from Target about this free offer and about the data breach, go to target.com/databreach, or contact Target directly at **866-852-8680**.

An important note: Be wary of calls or email scams that may appear to offer protection – but are really trying to get personal information from you.

Next, take basic steps to protect yourself against identity theft.

Consumers who shopped at Target stores between November 27 and December 15, 2013, and who paid by credit or debit cards, may be exposed to identity theft.

The information stolen during the breach of Target’s computer system included customer names, credit and debit card numbers, card expiration dates, the three-digit security codes on the backs of cards, and debit card PINs.

Consumers should be on alert for possible fraudulent charges on any credit or debit cards that were used at Target.

You should also take the following actions to protect yourself.

These are the same basic actions any consumer should take if he or she is a potential victim of identity theft, whether their personal information was stolen due to computer hacking, a phishing scam, or the theft of a wallet and personal ID cards.

- 1) **File a complaint with the Federal Trade Commission** at www.ftc.gov/complaint or **877-438-4338** (TTY: 866-653-4261). Your completed complaint is called an “FTC Affidavit.” You will want to bring a copy of the FTC Affidavit to your local police department; see Step 2.
- 2) **File a report with your local police department**, and bring the police a copy of your FTC Affidavit. Once your police report has been filed, request a copy so it will be available to send to credit reporting agencies and creditors.
- 3) **Obtain a copy of your credit report from all three credit reporting agencies.**
Contact them at:

Equifax Credit Information Services-Consumer Fraud Division
P.O. Box 740250
Atlanta, GA 303748
(800) 525-6285 • www.equifax.com

Experian
P.O. Box 1017
Allen, TX 75013-2104
(888) 397-3742 • www.experian.com/consumer
(800) 301-7196 (fax)

Trans Union
Fraud Victim Assistance Department
P.O. Box 6790

Fullerton, CA 92634
(800) 680-7289 • www.tuc.com

Tell these credit reporting agencies about the possible theft of information from the credit or debit cards you used at Target, and ask that all of your accounts be flagged with a fraud alert.

- 4) **Keep a close watch on the activity on your credit or debit cards.** Many card issuers offer online account access. If you can, check the accounts daily. If you are unable to access this information online, call the numbers on the back of the affected cards.
- 5) **Contact all of your credit card companies, creditors, banks, and any financial institutions you do business with.** Close the affected credit card and bank accounts, and get replacement cards with new account numbers. Change any passwords on the accounts, including PINs. Follow up all telephone contact with a written confirmation.
- 6) **Contact the United States Social Security Administration** at:

Social Security Administration, Fraud Hotline
Office of the Inspector General
P.O. Box 17768
Baltimore, MD 21235
(800) 269-0271
(410) 597-0018 (fax)
www.ssa.gov/oig/hotline
oig.hotline@ssa.gov

- 7) **Keep a complete set of records.** Keep a log with notes on all telephone conversations with credit reporting bureaus, creditors, or debt collection agencies. Confirm all telephone conversations in writing. Keep copies of all paper or electronic correspondence you send and receive related to the data breach. Send correspondence by certified mail, return receipt requested. Keep a record of the time spent and any expenses you incurred, in case it one day becomes possible to claim restitution in a judgment against the identity thief.
- 8) **You can also contact nongovernmental nonprofit groups established to provide assistance to victims of identity theft.** For example:

Privacy Rights Clearinghouse
Identity Theft Resource Center
3108 Fifth Avenue, Suite A
San Diego, California 92103
(858) 693-7935
www.privacyrights.org
www.idtheftcenter.org

- 9) **Finally, NEVER respond to unsolicited phone calls, emails, or letters** that claim to be about the Target data breach or identity theft. These may be scams, attempting to get personal information from you.

###