

WINSTON & STRAWN LLP

BEIJING
CHARLOTTE
CHICAGO
GENEVA
HONG KONG
HOUSTON
LONDON
LOS ANGELES

35 WEST WACKER DRIVE
CHICAGO, ILLINOIS 60601

+1 (312) 558-5600

FACSIMILE +1 (312) 558-5700

www.winston.com

MOSCOW
NEW YORK
NEWARK
PARIS
SAN FRANCISCO
SHANGHAI
WASHINGTON, D.C.

LIISA M. THOMAS
Partner
(312) 558-6149
lmthomas@winston.com

February 10, 2014

VIA FEDEX

Joseph Foster, Attorney General of the State of New Hampshire
Office of the Attorney General, NH Department of Justice
33 Capitol Street
Concord, New Hampshire 03301

Re: Notice Concerning Data Incident

Dear Mr. Foster:

We are writing on behalf of our client, The Home Depot, to report that three of its former human resources employees have been arrested on allegations that include the unlawful use of personal information (including name, contact information, financial information, drivers' license and social security numbers) maintained in databases that store information of The Home Depot's employees. These databases contain information about current and former employees, as well as hiring candidates. On December 16, 2013, an employee of The Home Depot notified a supervisor of the potential misuse of personal information by a fellow co-worker. The Home Depot immediately began an internal investigation, confirmed that improper activities were occurring, and notified the United States Secret Service, which began a thorough investigation. The Home Depot has actively provided full and continuous support to the Secret Service and other appropriate government authorities in their investigations, and continued conducting its own investigation of this matter. While the investigations are ongoing, initial arrests have been made, the three employees have been terminated, and on January 24, 2014, as part of its investigations, The Home Depot confirmed that at least one of the individuals had used personal information without authorization and for unlawful purposes.

Based on the investigative results to-date, The Home Depot has confirmed that there are 77 New Hampshire residents whose information was contained in the databases accessed by the terminated employees. While the investigations have not shown any evidence that these individuals' information was misused, out of an abundance of caution, and in order to provide potentially impacted employees with information they can use to protect themselves as soon as possible, The Home Depot has sent notification by letter to these individuals by February 10, 2014. In the notice, The Home Depot has indicated that the potential illegal activities may have started on February 7, 2011, the date of hire for the longest-serving of the three terminated employees. A copy of that notice is attached.

To protect its employees, The Home Depot is taking several steps to prevent further unauthorized use of personal information contained in its HR databases. This includes terminating the individuals in question, conducting an audit of its protocols and practices for those employees who have access to personal information, and continuing to work with law enforcement officials in their prosecution of these three individuals. The Home Depot has also provided all potentially impacted individuals with free credit monitoring services. The Home Depot has a call center set up for employees who have received notice, and will be actively working with its employees to ensure that they are aware of (and to help them take) steps to protect themselves.

We assure you that our client takes this issue, and the privacy and security of its employees, very seriously and is working diligently to ensure that this does not occur again. Please feel free to contact me if you have any questions.

Best regards,

A handwritten signature in black ink that reads "Liisa Thomas / MHT". The signature is written in a cursive, slightly slanted style.

Liisa M. Thomas

Enclosure[s]



Processing Center
P.O. Box 3825
Suwanee, GA 30024

John Q. Sample
123 Fake St.
Apt. 99
Austin, TX 77022

February 7, 2014

AllClear ID Redemption Code: [REDEMPTION_CODE]

Dear John Q. Sample,

Please read this letter carefully. As part of an ongoing investigation, we have been informed that three HR associates have been arrested on allegations that include the unlawful use of personal information belonging to current and former associates and a small number of candidates. These HR associates were employed by The Home Depot in positions of trust and therefore had authorized access to your personal information to perform assigned job duties. Out of an abundance of caution, we are notifying you of the possible unlawful use of your personal information. Our investigation indicates that your information may have been accessed by one of these three associates for unlawful purposes. The information that could have been accessed by the arrested associates includes your name, contact information, social security number, driver's license number, and any financial account numbers you may have provided us, and the longest period of employment for any of the three arrested associates goes back to February 7, 2011. Because we take this matter very seriously, we are conducting a thorough internal investigation, and we are working closely with appropriate government authorities.

Although we have found no evidence that your information was inappropriately used at this time, we want to make sure you can take appropriate steps to help prevent the misuse of your personal information. We have arranged for you to receive 12 months of identity protection from AllClear ID at no cost to you. AllClear ID offers Credit Monitoring that delivers secure, actionable Alerts to you by phone. This service also includes a \$1,000,000 Identity Theft Insurance Policy, the AllClear ID Investigations Team to assist you in the event that your information is used fraudulently, and AllClear ID Resolution Services, if needed, to assist you in restoring your credit file.

You may sign up online at enroll.allclearid.com or by phone by calling 1-877-263-7996. To sign up online, go to enroll.allclearid.com. You will need to provide the redemption code that is listed at the top of this page. Once you have entered your redemption code, click on "Sign up now" on the right side of the page and follow the website's instructions. Please note, part of the sign-up process may include receiving a phone call from AllClear ID soon after you initiate the registration process. You have 90 days from the receipt of this letter to register. The AllClear ID service will be valid for one year from the date you register.

The AllClear ID service may be helpful because one possible misuse of your information would be to open credit card or consumer loan accounts in your name without your permission. This is called "identity theft." The theft of your identity can lead to the loss of your credit worthiness and can cause collection agencies to try to collect debts from you that you did not create. To see if someone is misusing your information you can check your credit reports and your banking and other account statements to make sure that all of the accounts and transactions on those reports were made by you.

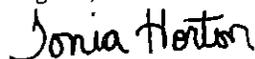
We encourage you to remain vigilant, and to regularly review and monitor relevant account statements and credit reports. If you find any indication of unauthorized accounts or transactions, you should report the possible threat to your identity to local law enforcement, your State Attorney General's office, *or* the Federal Trade Commission. Information on how to make some of these reports is included in the Reference Guide that is part of this notice to you. You should also report the unauthorized accounts or transactions to the credit reporting agency from which you obtained the report.

You are entitled to one free credit report annually from each of the three national credit bureaus. To order your free credit reports, please read the Reference Guide. It includes contact information for each of the three major credit agencies. You also have the right to place a fraud alert or security freeze on your credit file to prohibit temporarily the opening of new credit accounts in your name. The Reference Guide below explains how to take these steps. You can also learn more about how to protect yourself from becoming a victim of identity theft by contacting the Federal Trade Commission www.ftc.gov/idtheft/ (full contact information is in the Reference Guide below).

Although we are contacting you only as a precaution, we encourage you to take advantage of these free AllClear ID identity protection services. We take the protection of your personal information very seriously and are taking steps to prevent a similar occurrence. We are very sorry for any inconvenience this event may cause you. If you have questions about this matter or the AllClear ID services, please call 1-877-263-7996. AllClear ID is available to answer any questions you may have Monday – Saturday, 8AM – 8PM CST. You may also call The Home Depot’s HR Service Center at 1-866-698-4347 any time Monday – Friday, 8AM – 8PM EST and Saturday 8AM – 5PM EST.

We hope this information is useful and again apologize for any concern this incident may cause you.

Regards,



Tonia Horton
Senior Director, HR Services

Reference Guide

Even if you do not feel the need to use the identity protection services we are offering to you free of charge through AllClear ID, we encourage you to read this Reference Guide carefully and to take the steps described here:

Order Your Free Credit Report. You are entitled under U.S. law to one free credit report annually from each of the three national credit bureaus, whose contact information is below. To order your free credit report, you can also visit www.annualcreditreport.com, call toll-free at 877-322-8228 or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission’s website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. When you receive your credit reports, review them carefully to ensure that the information they contain is accurate. If you see anything on your credit reports or credit card account statements that appears incorrect, contact the credit reporting agencies and/or your credit card provider, and report suspected incidents of identity theft to local law enforcement, the Attorney General, or the FTC (contact information below). Even if you do not find any signs of fraud on your reports or account statements, the FTC suggests that you check your credit reports and account statements periodically, or at least every few months, as identity thieves may not use personal information released in a security incident right away. Some businesses may give victims of security incidents free services; make sure that those offers are legitimate before signing up.

Place a Fraud Alert or Security Freeze on Your Credit Report. To protect yourself from possible identity theft, you may want to consider placing a fraud alert or security freeze on your credit report with the major credit reporting agencies. Their contact information is as follows:

Equifax	P.O. Box 740241 Atlanta, Georgia 30374-0241	888-766-0008	www.equifax.com
Experian	475 Anton Blvd. Costa Mesa, CA 92626	888-397-3742	www.experian.com
TransUnion	Fraud Victim Assistance Division P.O. Box 6790 Fullerton, California 92834-6790	800-680-7289	www.transunion.com

A fraud alert lasts 90 days, and requires potential creditors to use reasonable policies and procedures to verify your identity before issuing credit in your name (as soon as one agency is notified, the others are notified to place fraud alerts as well). You can keep a fraud alert in place for an extended seven years by contacting the agencies again after 90 days and providing a police report. You can also ask these same credit reporting agencies to put a “freeze” on your credit report. A security freeze prohibits a credit reporting agency from releasing any information from your credit report without your written authorization. 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, credit mortgages, employment, housing or other services. Unless you are the victim of identity theft, each agency may charge a fee which could range based on your state, but generally the credit reporting agencies will charge \$5.00, unless you have a police report, in which case it may be free. Individuals in some states, like North Carolina, can now get free security freezes online. Identity theft victims who have filed a police report, their spouses, and consumers over the age of 62 can also get free security freezes by mail or phone. You will be asked to provide the agency with certain identifying information, like name, social security number, date of birth, current and prior addresses (and proof thereof). You may also have to provide a copy of your government ID. You have the right under the laws of many states to obtain a police report. Many law enforcement agencies will not issue a police report until

information is actually misused. If you have been the victim of identity theft, you will need to provide a copy of the police report or complaint to law enforcement when requesting your security freeze; if you have not, you will need to provide the required fee by check or credit card (do not send cash in the mail).

Helpful Contacts. You can learn more about how to protect yourself from becoming a victim of identity theft by contacting the Federal Trade Commission or your state's regulatory authority to obtain additional information about how to avoid identity theft, how to place a fraud alert, and how to place a security freeze on your credit report.

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the:

Maryland Office of the Attorney General, Consumer Protection Division
200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from the:

North Carolina Attorney General's Office, Consumer Protection Division
9001 Mail Service Center, Raleigh, NC 27699-9001, 1-919-716-6000, www.ncdoj.gov