Hogan Lovells US LLP
Columbia Square
555 Thirteenth Street, NW
Washington, DC 20004
T +1 202 637 5600
F +1 202 637 5910
www.hoganlovells.com

May 27, 2014

By Federal Express

Attorney General Joseph Foster
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

RE: Notification of Potential Data Breach Pursuant to N.H. Rev. Stat. § 359-C:20

Dear Attorney General Foster:

On behalf of our client, The Home Depot, Inc., ("Home Depot"), we are writing to provide notification pursuant to the above-referenced statute of a security incident involving customer credit card information belonging to one New Hampshire resident.

Commencing on or about May 7, 2014 and continuing through May 21, 2014, a Home Depot employee with authorized access to computer systems used that access to obtain credit card information from certain transactions conducted in the tool rental area of Home Depot stores. The employee obtained and distributed to third parties the following account information for less than 500 cards, including information belonging to the New Hampshire resident: account holder name, address, phone number, date of birth, and the brand, primary account number and expiration date of the credit card used. In addition, the employee obtained access to the same information for approximately 30,000 additional accounts. However, based on our review to date there is no evidence that information about these additional accounts was distributed outside Home Depot.

The data the employee obtained did not include drivers' license or Social Security numbers or the PIN, CVV, CCID, or other security codes often needed to clone a card or to purchase merchandise with stolen credit card data. The employee did not hack our systems; was quickly terminated, and his electronic devices have been seized by law enforcement. Home Depot has terminated his employment; we are cooperating with federal law enforcement, and will seek the prosecution of this individual to the full extent allowed by law. Home Depot will also review its access controls to help ensure that similar incidents do not occur in the future.

Home Depot will be providing written notification by mail on May 27, 2014 to impacted customers in accordance with applicable law. A copy of the form of notification to be issued is enclosed. As set forth in the notice, affected customers will be provided with credit monitoring services for a 12-month period without charge.

Please feel free to contact me if you have any questions or require additional information.

Sincerely,

Stuart M. Altman
stuart.altman@hoganlovells.com
202.637.3617

Enclosure

First Name, Last Name
Address
Address

AllClear ID Redemption Code: XXXXXXXX

May 23, 2014

Dear First Name:

Protecting the privacy and security of your personal information is extremely important to us. We are writing to notify you that sometime between May 7 and May 21, 2014, a now terminated IT department employee of The Home Depot improperly accessed the account number of a credit card that you may have used at a Home Depot tool rental center. The associate downloaded and may have distributed to a third party your credit card account number, its expiration date, and your name, address, phone number, and date of birth. The data distributed did not include your drivers' license or Social Security number or the PIN, CVV, CCID, or other security codes often needed to clone a card or to purchase merchandise with stolen credit card data. The associate did not hack our systems, rather, he took advantage of access that was required by his job responsibilities. His access to our systems has been terminated and his electronic devices have been seized by law enforcement. We are cooperating with law enforcement and will seek the prosecution of this individual to the full extent allowed by law.

We take the protection of your personal information very seriously, and we are deeply sorry that a Home Depot associate violated your trust and our values. You may be sure that we are taking every measure possible to prevent such a theft from happening again. We apologize for this incident and any inconvenience or concern that it may cause you.

We encourage you to review your account to check for any transactions that might reflect improper use of your information. You should immediately report any indication of inappropriate use of your information to your credit card company. Even if you do not see signs of misuse, to be cautious you may want to ask your credit card company to cancel your current card and issue you a new one.

To assist you in preventing "identity theft" or other misuse of your 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 1-866-979-2595. To sign up at enroll.allclearid.com, you will need 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.

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 any unauthorized transactions to your bank or credit card company and any unauthorized accounts to the credit reporting agency from which you obtained the credit 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).

We hope this information is useful and again apologize for any inconvenience or concern this incident may cause you. If you have questions about this matter, please contact us at 800 -910-7168.

Regards,

Stacey Keegan
Senior Corporate Counsel

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