

18698

January 25, 2021

Re: Notice of Data Breach

Dear _____,

On behalf of Citibank, N.A. ("Citi"), we are writing to inform you about an incident involving potential unauthorized access to your personal information associated with your Home Depot account.

What Information Was Involved

Our investigation indicates that a Citi employee improperly accessed your account, deleted pending payments and set up new payment arrangements for the purpose of improving monthly incentive compensation. The employee accessed your name, account number, last 4 digits of your social security number, date of birth, address, phone number, email address, and the last 4 of digits of your checking account number.

We take the security of your personal information very seriously and wanted to bring this to your attention. We also wanted to apologize for any inconvenience this may cause you.

What Are We Doing

The employee in question was caught, immediately suspended, and terminated. They no longer have access to your Citi Account.

WHAT YOU CAN DO

To date we have not received any reports of actual access to or misuse of information as a result of this incident, but we recommend that you be aware of the following steps to monitor for any potential misuse of your personal information:

- You should regularly review your account statements and monitor free credit reports. Please promptly report suspicious or unusual activity on your accounts to us.
- Under federal law, you are entitled to obtain one free copy of your credit report every twelve months from each of the three nationwide consumer reporting agencies. You can obtain a free copy of your credit report from each of the three nationwide consumer reporting agencies by calling 1-877-322-8228 or visiting www.annualcreditreport.com. We recommend that you periodically obtain credit reports from each nationwide credit reporting agency. If you discover information on your credit report arising from a fraudulent transaction, you may request that the credit reporting agency delete that information from your credit report file.
- You may also consider contacting the credit reporting agencies directly if you wish to put in place a fraud alert or a security freeze. A fraud alert will notify any merchant checking your credit history that you may be the victim of identity theft and that the merchant should take additional measures to verify the application. Contacting any one of the three agencies will place an alert on your file at all three. A security freeze restricts all creditor access to your account but might also delay any requests you might make for new accounts. You may contact the nationwide credit reporting agencies at the following numbers to place a security freeze to restrict access to your credit report:
 - Equifax: 800-349-9960; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241
 - Experian: 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9554, Allen, TX 75013
 - TransUnion: 888-909-8872; transunion.com; Fraud Victim Assistance, P.O. Box 2000, Chester, PA 19022-2000

To report incidents of fraud and identity theft, you can contact the Federal Trade Commission (FTC) at 1-877-ID-THEFT, through their website at <http://identitytheft.gov>, or in writing at 600 Pennsylvania Ave. NW, Washington DC 20850. You can also contact local law enforcement or your state's attorney general.

If you have questions or concerns about this, or if we can be of further assistance to you, please do not hesitate to call us toll free at (will enter toll free number for Client Focus Team here.)

~~will remove, no signature~~