26690

To Enroll, Please Call:
1-833-774-2039
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: <<Enrollment>>

Metro Builders Supply, Inc.
P.O Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

June 7, 2022

NOTICE OF <<Variable1>>

Dear <<First Name>> <<Last Name>>,

Metro Builders Supply, Inc. d/b/a Metro Appliances & More ("Metro") is writing to notify you of a recent incident that may have impacted the security of some of your information. This letter provides an overview of the incident, our response, and resources available to you to help protect your information, should you wish to do so.

We are aware that you may have received a letter in the mail from us dated May 18, 2022, with an incorrect name and/or address. Please disregard that letter, and accept the information provided in this one. We apologize for any confusion or inconvenience this may have caused.

What Happened? On April 20, 2022, Metro discovered unauthorized access to certain computer systems on our network. In response, we immediately took steps to secure our systems and launched an investigation into the nature and scope of the event with the assistance of third-party computer forensic specialists. On April 26, 2022, Metro determined that certain files stored on our systems were accessed and/or obtained by an unknown actor on or about April 19, 2022. We identified the affected files and conducted a thorough review of the files in order to identify whether any personal information is contained therein and to whom that information relates. Our review determined that some of the affected files contained information of our vendors, and current and former employees and their dependents and/or beneficiaries, including you. Metro has no evidence of any actual or attempted fraudulent use of the potentially impacted information.

What Information Was Involved? Our review determined that the following types of information was present in the files that were accessed or acquired by the unauthorized actor: your name, <<Variable2>>. The investigation was unable to determine whether your specific information was actually viewed, and we have no evidence of any actual or attempted fraudulent use of your information resulting from this incident. If information of your dependent(s) was involved, we are providing separate notifications to you for each dependent.

What We Are Doing. The security of information on our systems is one of our highest priorities, and we have strict security measures in place to protect the information in our care. Following discovery of this incident, we took immediate steps to secure our environment and are in the process of implementing additional security measures.

We are also offering credit and identity monitoring services for <<12/24>> months through IDX at no cost to you. The deadline to enroll in these services is September 7, 2022. Information and instructions on how to activate these complimentary services can be found in the "*Steps You Can Take to Help Protect Your Personal Information*" below.

What You Can Do. While Metro has no evidence of any actual or attempted misuse of your information related to this incident, we encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account

statements and monitoring your free credit reports for suspicious activity and to detect errors. You may also activate the complimentary credit and identity monitoring services we are making available to you. Further information can be found in the "*Steps You Can Take to Help Protect Your Personal Information.*"

For More Information. If you have questions regarding this letter, please call 1-833-774-2039 between the hours of 9:00 a.m. and 9:00 p.m., Eastern Time, Monday through Friday.

We sincerely regret any inconvenience this incident may cause you. Protecting your information is very important to us, and we remain committed to safeguarding the information in our care.

Sincerely,

Mark Howell
Chief Operating Officer

STEPS YOU CAN TAKE TO HELP PROTECT YOUR PERSONAL INFORMATION

Enroll in Credit Monitoring

1. **Website and Enrollment.** Go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-833-774-2039 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

By providing this notice, Metro Builders Supply, Inc. d/b/a Metro Appliances & More ("Metro") does not waive any rights or defenses regarding the applicability of Massachusetts law, the applicability of the Massachusetts data event notification statute, or personal jurisdiction.

Nature of the Data Event

On April 20, 2022, Metro discovered unauthorized access to certain computer systems on its network. In response, Metro immediately took steps to secure its systems and launched an investigation into the nature and scope of the event with the assistance of third-party computer forensic specialists. On April 26, 2022, Metro determined that certain files stored on its systems were accessed and/or obtained by an unknown actor on or about April 19, 2022. Metro identified the affected files and began a thorough review of the files in order to identify whether any personal information is contained therein and to whom that information relates. Metro's review determined that some of the affected files contained information of its current and former employees and their dependents and/or beneficiaries. Metro has no evidence of any actual or attempted fraudulent use of the potentially impacted information.

The information affected by this event includes the following: name, Social Security number, health insurance enrollment information, and/or financial account information.

Notice to Massachusetts Resident

On June 7, 2022, Metro provided written notice of this incident to approximately one (1) Massachusetts resident. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Please be advised that, pursuant to G.L. c. 93H § 3(b), Metro does not maintain a written information security program (WISP) for the protection of personal information of residents of Massachusetts. However, Metro does have the majority of the WISP requirements in place and is in the process of developing a policy that requires encryption of all personal information stored within its systems as well as developing and implementing education and training of its employees on the importance of information security.

Other Steps Taken and To Be Taken

Upon discovering the event, Metro moved quickly to investigate and respond to the incident, assess the security of its systems, and identify potentially affected individuals. Further, Metro notified federal law enforcement regarding the event. Metro is also working to implement additional safeguards and training to its employees. Metro is providing access to credit monitoring services for two (2) years through IDX, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Metro is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Metro is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Metro is also providing written notice of this incident to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

EXHIBIT A

Exhibit 1