

From: [IDX](#)
To: [Recipient](#)
Cc:
Subject: FW: Notice of Data Breach
Date: April 8, 2022

From: IDX <IDX@idx.help>
Sent: Friday, April 8, 2022
To: Recipient email address
Subject: Notice of Data Breach

April 08, 2022

Notice of Data Breach

Dear <<Firstname>> <<Lastname>>,

This notice is to provide you with information about a data security incident that may have affected your information. The privacy and security of your personal information is extremely important to us as we very much appreciate your business. We are writing to notify you of the incident, to provide you with information about the nature of the incident, and the steps you can now take to protect your personal information. As a result of this incident, we have partnered with IDX to provide you this notification.

What Happened. On October 15, 2021, <<Variable Entity>> Warehouse, LLC (“<<Variable Entity>> Warehouse”) became aware of a potential data security incident. We immediately began an internal investigation and engaged an independent computer forensics firm to determine whether any personal information was affected in the incident. The investigation has been extensive, requiring the analysis of a substantial amount of digital evidence. On or around November 6, 2021, we learned information was obtained without authorization on October 1, 2021. On November 29, 2021, the investigation determined the identities of impacted individuals. After further investigation and review, we learned that the password associated with your account at <<Variable Entity>> Warehouse’s retail website may have been obtained without authorization on October 1, 2021.

What Information Was Involved. The incident may have involved information including your name, email address, and password associated with your account on <<Variable Entity>> Warehouse’s retail website.

What We Are Doing. As soon as we discovered the incident, we took the measures referenced above, reported the incident to law enforcement, and will fully cooperate with any investigation. We have also worked closely with technical experts to enhance the security of our websites to facilitate safe and secure transactions and to mitigate against the evolving security risks that all businesses face. Additionally, all user account passwords on the <<Variable Entity>> Warehouse retail website have been reset to provide an additional layer of security.

What You Can Do. Receiving this letter does not mean that you are the victim of identity theft. We recommend, however, that you take the steps referenced on the following page to protect your personal information. Because the password associated with your account at <<Variable Entity>> Warehouse's retail website may have been involved, we wanted to notify you of this incident and encourage you to update or change your password(s) if you reuse the same password or login for different websites. The next time you attempt to log onto your account at <<Variable Entity>> Warehouse's retail website, you will be prompted to reset your password. We recommend you follow the instructions to access your account on <<Variable Entity>> Warehouse's retail website.

For More Information. If you have questions or need assistance, please never hesitate to call (833) 381-2293, Monday through Friday from 9 a.m. to 9 p.m. Eastern Time, excluding major U.S. holidays.

We sincerely apologize for this incident. We value you, your personal information, and your continued business.

Sincerely,

Mark Sczbecki
Co-Owner
<<Variable Entity>> Warehouse, LLC

Steps You Can Take to Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity:

As a precautionary measure, we recommend that you remain vigilant by reviewing your payment card account statements. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company that issued the payment card or with whom the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax: P.O. Box 105851 Atlanta, GA 30348, 1-800-525-6285, www.equifax.com

Experian: P.O. Box 9532 Allen, TX 75013, 1-888-397-3742, www.experian.com

TransUnion: P.O. Box 1000 Chester, PA 19016, 1-800-916-8800, www.transunion.com

Fraud Alert: Although the theft of payment card information should not affect access to credit, as a normal preventive practice, you may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies

identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission: 600 Pennsylvania Ave, NW Washington, DC 20580
www.consumer.ftc.gov and www.ftc.gov/idtheft, 1-877-438-4338

Maryland Attorney General: 200 St. Paul Place Baltimore, MD 21202, oag.state.md.us, 1-888-743-0023

New York Attorney General: Bureau of Internet and Technology Resources, 28 Liberty Street New York, NY 10005 1-212-416-8433

North Carolina Attorney General: 9001 Mail Service Center Raleigh, NC 27699,
ncdoj.gov, 1-877-566-7226

Rhode Island Attorney General: 150 South Main Street Providence, RI 02903 riag.ri.gov, 1-401-274-4400

Washington D.C. Attorney General: 441 4th Street, NW Washington, DC 20001,
oag.dc.gov, 1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit <https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act>.

This email was sent by: IDX to andrew.mayall@idx.us
10300 SW Greenburg Road Suite 570, Portland, OR, 97223 US

[Privacy Policy](#)

Click here to [unsubscribe](#)

□

This email has been scanned for spam and viruses by Proofpoint Essentials. Click [here](#) to report this email as spam.