Storagefront.com
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

storagefront

[redacted]

NOTICE OF DATA BREACH

February 28, 2023

Re: Storagefront.com Data Breach

Dear [redacted]:

We are writing to inform you of a security incident affecting a portion of our stored electronic data. That data may have included your personal information, the privacy and security of which are of the utmost importance to Storagefront.com, ("Storagefront.com"). We wanted to provide you with information about the incident and let you know that we continue to take significant measures to protect your information.

What Happened?

Storagefront.com experienced a cybersecurity incident in 2020 that was remediated and investigated. Unbeknownst to Storagefront.com, the incident resulted in one table in a database being copied from the Storagefront.com environment. On November 15, 2022, we were alerted that some Storagefront.com data from this table was available on the dark web. Upon learning of the issue, we immediately commenced an investigation. Our investigation concluded that data from one table in a database was taken during the 2020 incident and leaked online in August 2022. Storagefront.com confirmed that the leaked file was a Storagefront.com file. ***The leaked file did not contain any sensitive or personally identifiable information.***

After confirming that the leaked file came from a Storagefront.com database, we reviewed other data that existed within other tables in the database. We discovered on January 5, 2023 that your personal information was stored on other tables in the impacted database. ***We have no evidence that the tables where your data was stored were accessed or copied during the 2020 incident.***

What Information Was Involved?

Other tables within the impacted database included your name, driver's license number, and Social Security number.

What You Can Do:

To date, we have no evidence that the tables where your data was stored were accessed or copied during the 2020 incident. We are also not aware of any misuse of your information as a result of this incident. Out of an abundance of caution, however, we want to advise you on the incident, explain the services we are making available to help safeguard you against identity fraud, and suggest steps that you should take as well. To protect you from potential misuse of your information, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for twelve months from the date of enrollment when changes occur to your credit files. This notification is sent to you the same day that the change or update

takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services. For information about how to enroll in these services, please see page 3 of this letter. This letter also provides other precautionary measures you can take to protect your personal information, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information:

Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions. Please call 1-833-570-2895 between the hours of 8:00 am and 8:00 pm Eastern time, Monday through Friday, excluding holidays, for any additional questions you may have. Representatives are available for 90 days.

Sincerely,

Lance Watkins
Chief Executive Officer
Storagefront.com
4920 Campus Drive, Suite B
Newport Beach, CA 92660

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary 12-Month Credit Monitoring.

To enroll in Single Bureau Credit Monitoring services at no charge, please log on to **https://secure.identityforce.com/benefit/tenant** and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted] In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

2. Placing a Fraud Alert on Your Credit File.

You may place an initial 1-year "fraud alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
(800) 525-6285

Experian
P.O. Box 9554
Allen, TX 75013
https://www.experian.com/fraud/center.html
(888) 397-3742

TransUnion LLC
P.O. Box 6790
Fullerton, PA 92834-6790
https://www.transunion.com/fraud-alerts
(800) 680-7289

3. Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "security freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
https://www.equifax.com/personal/credit-report-services/credit-freeze/
(888) 298-0045

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
http://experian.com/freeze
(888) 397-3742

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
https://www.transunion.com/credit-freeze
(888) 909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies.

000030202C0000

P

Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.