

Blair L. Dawson, FIP, CIPP/US, CIPP/E, CIPM
Direct Dial: 312-642-6131
E-mail: bdawson@mcdonaldhopkins.com

March 2, 2023

VIA EMAIL

March 2, 2023

Brian E. Frosh
Office of the Attorney General
St. Paul Plaza
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Email: ldtheft@oag.state.md.us

Re: Tenant, Inc. Data Security Incident

Dear Sir or Madam:

McDonald Hopkins has been retained by Tenant, Inc. ("Tenant", formerly known as "Storagefront.com") in relation to a recent data security incident. I am writing to provide notification of an incident that may affect the security of personal information of approximately eleven (11) Maryland residents. By providing this notice, Tenant does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

Tenant, Inc. ("Tenant", formerly known as "Storagefront.com") experienced a cybersecurity incident in 2020 that was remediated and investigated. Unbeknownst to Storagefront.com, the incident resulted in certain data being accessible during the incident. On or about November 15, 2022, Tenant became aware that one of Storagefront.com's database tables had been accessed by an unauthorized actor. The database table appeared to be from April 2020.

Upon learning of this issue, Tenant immediately commenced a prompt and thorough investigation. As part of its investigation, Tenant has been working very closely with external cybersecurity professionals experienced in handling these types of incidents, and on January 5, 2023, Tenant discovered that some personal information was among the data that may have potentially been accessed during the incident. Tenant does not have any evidence that Storagefront.com data was accessed or copied during the 2020 incident. Tenant is also not aware of any misuse of Storagefront.com information as a result of this incident. On February 24, 2023, Tenant confirmed address information for all of the potentially impacted individuals and notification letters were mailed out on February 28, 2023.

March 2, 2023

Page 2

Tenant is not aware of any reports of identity theft or fraud arising out of this incident. Nevertheless, out of an abundance of caution, Tenant wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. Tenant is providing the affected resident with written notification of this incident commencing on or about February 28, 2023 in substantially the same form as the letter attached hereto. Tenant is offering the affected residents complimentary one-year membership with a credit monitoring service. Tenant will advise the affected resident to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. Tenant will advise the affected resident about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. The affected resident is also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At Tenant, protecting the privacy of personal information is a top priority. Tenant is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Tenant continually evaluates and modifies its practices to enhance the security and privacy of the personal information it maintains.

If you have any additional questions, please contact me at (312) 642-6131 or bdawson@mcdonaldhopkins.com.

Very truly yours,

A handwritten signature in black ink, appearing to read 'BLD', followed by a long horizontal flourish.

Blair L. Dawson, FIP, CIPP/US, CIPP/E, CIPM

Encl. Sample Notification Letter

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



**IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY**

February 28, 2023

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] 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. 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.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: 515-281-5164.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 888-743-0023.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; <https://ag.ny.gov/consumer-frauds-bureau/identity-theft>; Telephone: 800-771-7755.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

* * * * *

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

*In Addition, New Mexico Consumers Have the Right to
Obtain a Security Freeze or Submit a Declaration of Removal*

As noted above, you may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following:

1. The unique personal identification number, password, or similar device provided by the consumer reporting agency;
2. Proper identification to verify your identity; and
3. Information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control, or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone, or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

To place a security freeze on your credit report, you must send a request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion. You may contact these agencies using the contact information provided above.

* * * * *

Rhode Island Residents: You may contact law enforcement, such as the Rhode Island Attorney General's Office, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. You can contact the Rhode Island Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 401-274-4400.

As noted above, you may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You have a right to place a "security freeze"



on your credit report pursuant to chapter 48 of title 6 of the Identity Theft Prevention Act of 2006.

The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, within five (5) business days you will be provided a personal identification number or password to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report for a specific period of time after the freeze is in place. To provide that authorization, you must contact the consumer reporting agency and provide all of the following:

1. The unique personal identification number or password provided by the consumer reporting agency.
2. Proper identification to verify your identity.
3. The proper information regarding the period of time for which the report shall be available to users of the credit report.

A consumer reporting agency that receives a request from a consumer to temporarily lift a freeze on a credit report shall comply with the request no later than three (3) business days after receiving the request.

A security freeze does not apply to circumstances where you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of an account review, collection, fraud control, or similar activities.

If you are actively seeking a new credit, loan, utility, telephone, or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze -- either completely, if you are shopping around, or specifically for a certain creditor -- with enough advance notice before you apply for new credit for the lifting to take effect.

You have a right to bring a civil action against someone who violates your rights under the credit reporting laws. The action can be brought against a consumer reporting agency or a user of your credit report.

To place a security freeze on your credit report, you must send a request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion. These agencies can be contacted using the contact information provided above.

In order to request a security freeze, you may need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Complete address;
5. Prior addresses;
6. Proof(s) of identification (state driver's license or ID card, military identification, birth certificate, etc.);
7. If you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

There were 3 Rhode Island residents impacted by this incident.