



Freeman
Mathis & Gary LLP

100 Galleria Parkway
Suite 1600
Atlanta, GA 30339-5948

Tel: 770.818.0000

www.fmglaw.com

Robert E. Buckley

D: 770.818.1298

rbuckley@fmglaw.com

July 13, 2023

VIA EMAIL (consumer@ag.iowa.gov)

Consumer Protection Division
Security Breach Notifications
Office of Attorney General of Iowa
1305 E. Walnut Street
Des Moines, IA 50319-0106

**Re: Skogman Construction Company of Iowa, Inc.
Notice of Data Breach**

To Whom It May Concern:

Our firm represents Skogman Construction Company of Iowa, Inc. ("Skogman"), a company that provides realty and home building services with its principal office address at 417 First Ave. SE, Cedar Rapids, IA 52401. This letter is provided pursuant to Iowa Code Chapter 715C, which requires notice to the Office of the Attorney General's Consumer Protection Division in the event of a breach in the security of personal information affecting more than 500 residents of the state of Iowa.

Skogman recently was the victim of a ransomware attack that impacted its computer systems. Skogman promptly initiated incident response protocols to thoroughly investigate the incident and safely restore its systems. Skogman also reported the incident to law enforcement and cooperated with their efforts.

Through its investigation, Skogman discovered that an unauthorized actor gained access to its computer system and may have acquired certain files on or about April 11, 2023, before launching the ransomware attack. Skogman completed a detailed review of the potentially compromised files and, through that process, discovered on June 13, 2023, that personal information for some of its past and present employees and agents may have been impacted, including names, Social Security numbers, payment card numbers, driver's license number, routing numbers, and/or financial account numbers.

A sample of the notification letter mailed to residents is enclosed for your records. As reflected therein, as a precautionary measure, Skogman is offering all potentially affected residents free credit monitoring and identity restoration services through Experian IdentityWorksSM for a period of one year.

www.fmglaw.com



Freeman
Mathis & Gary LLP

July 13, 2023

Page 2

Going forward, Skogman is taking steps to help mitigate the potential for harm and prevent this from happening again. Skogman completed a global reset of all passwords for its computer network, restored affected systems, and implemented enhanced endpoint detection and response software throughout its systems. It also notified law enforcement about the incident and will cooperate with any further investigation by them. In addition, Skogman will continue reviewing its policies and procedures to identify any other measures to further strengthen security and help prevent a future incident from occurring.

I believe this provides you with all information necessary for your purposes and to comply with Iowa law. However, if anything further is needed, please contact me.

Very truly yours,

FREEMAN MATHIS & GARY, LLP

A handwritten signature in blue ink, appearing to read 'R. Buckley', written over a thin blue horizontal line.

Robert E. Buckley



Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

July 13, 2023

J6831-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345



SAMPLE A SAMPLE - L01 ADULT
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789



Notice of Data Breach

Dear Sample A. Sample:

At Skogman Construction Company of Iowa (“Skogman”) we take the issue of privacy seriously. As part of that commitment, we are sending you this letter to make you aware of a recent data security incident that may have affected your personal information. Please read this letter carefully.

What Happened

Recently, Skogman was the victim of a ransomware attack that impacted our computer systems. We were able to restore most of our files and the functionality of our system. Subsequent scans of our system show no further sign of the ransomware. However, our investigation of the incident did find that on or around April 11, 2023, an unauthorized individual(s) did access or acquire certain files from our network containing the personal information of some individuals. We then completed a detailed review of the potentially compromised files and, through that process, discovered on June 13, 2023, that some of your personal information may have been impacted. As a result, we are notifying all potentially affected individuals about this incident.

What Information Was Involved

Although Skogman is not aware of any actual or attempted misuse of your information, we are providing you this notification out of an abundance of caution because we have determined that certain information relating to you was contained in the documents that we believe were accessed or acquired from our computer network during this incident. The potentially impacted information relating to you includes your [PII].



What We Are Doing

We take the protection of information seriously and are taking steps to continue investigating this incident, help mitigate the potential for harm, and prevent future incidents. Among other things, we completed a global reset of all passwords for our computer network, restored affected systems, and implemented enhanced endpoint detection and response software throughout our systems. Going forward, we will be providing additional training to our employees and continuing to review our policies and procedures to identify any additional measures we can implement to further strengthen security and help prevent a future incident from occurring. We also notified law enforcement about the incident and will cooperate with any investigation.

What You Can Do

In light of this incident, we recommend that you remain vigilant by reviewing and monitoring your account statements and credit reports. If you find any errors or unauthorized activity, you should contact your financial institutions that may be affected. You also may file a report with law enforcement, your state attorney general, and/or the Federal Trade Commission. In addition, please refer to the enclosed documentation which contains additional steps you may take to protect your information from misuse.

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for 12 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 12 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 12-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** October 31, 2023 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code: ABCDEFGHI**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-653-0349 by October 31, 2023. Be prepared to provide engagement number B098539 as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

For More Information

We are sorry for any concern or inconvenience this incident may cause you. If you have any other questions or concerns that you would like to discuss, please contact us through our dedicated hotline at (877-653-0349) from Monday through Friday 8 am – 10 pm CST or Saturday and Sunday 10 am – 7 pm CST (excluding major U.S. holidays).

Sincerely,


PRESIDENT, SKOGMAN COMPANIES

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.



ADDITIONAL STEPS TO HELP PROTECT YOUR INFORMATION

Review personal account statements and credit reports. We recommend that you remain vigilant by reviewing personal account statements and monitoring credit reports to detect any errors or unauthorized activity. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call (877) 322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months. If you discover any suspicious items, you should report any incorrect information on your report to the credit reporting agency. The names and contact information for the credit reporting agencies are:

Equifax	Experian	TransUnion
1-866-766-0008	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
www.equifax.com	www.experian.com	www.transunion.com

Report suspected fraud. You have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You should report suspected incidents of identity theft to local law enforcement, your state's Attorney General, and/or the Federal Trade Commission.

Place Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. When you place a fraud alert, it will last one year. Fraud alerts are free and identity theft victims can get an extended fraud alert for seven years. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. To place a security freeze, contact the nationwide credit reporting agencies by phone or online. For more information, visit <https://www.consumer.ftc.gov/articles/0275-place-fraud-alert>.

Place a Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too. To place a security freeze, contact the nationwide credit reporting agencies by phone or online. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee. Also, do not confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock. For more information, visit <https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs>.

Change Online Account Credentials. If the information involved in this incident included credentials used to access any of your online accounts, such as a username, password, PIN, or answer security question, you should promptly change your username, password, PIN, security question and answer, or other access credentials and take other appropriate steps to protect all online accounts for which you use the same credentials.

Obtain Additional Information about the steps you can take to avoid identity theft from (i) the U.S. Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.ftc.gov, 1-877-IDTHEFT (438-4338); (ii) for Iowa residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. This office can be reached at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319, (515) 281-5164, www.iowaattorneygeneral.gov; (iii) for North Carolina Residents: You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at: North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699-9001, (877) 566-7226 (toll-free in North Carolina), (919) 716-6400, www.ncdog.gov; and (iv) for Rhode Island residents: You may obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General at: Rhode Island Office of the Attorney General, Consumer Protection Unit, 150 South Main Street, Providence, RI 02903, (401)-274-4400, www.riag.ri.gov.

Know Your Rights Under the Fair Credit Reporting Act. The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. You have certain rights under the FCRA, which you can read about by visiting <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf> and <https://www.consumer.ftc.gov/articles/0070-credit-and-your-consumer-rights>. States may enforce the FCRA, and many states have their own consumer reporting laws.