Our ref 1261609

Kennedys

1600 Market Street
Suite 1410
Philadelphia, PA 19103
USA

t +1 267.479.6700
f +1 215.665.8475

kennedyslaw.com

t +1 267 479 6795

Nicholas.Jajko@kennedyslaw.com

27 June 2025

Via Online Reporting
Nebraska Office of Attorney General
Consumer Affairs Response Team
2115 State Capitol
Lincoln, NE 68509

RE: Weathercraft Co. of Scottsbluff – Notice of Data Event

Dear Attorney General Hilgers:

We represent The Weathercraft Company of Scottsbluff ("Weathercraft"), a roofing, siding, gutter, and window contractor based in North Platte, Nebraska. We write in accordance with the Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006, NEB. REV. STAT. § 87-801, *et seq.*, requiring reporting of a data event to your Office that impacts residents of the State of Nebraska. In making this submission, Weathercraft does not waive its rights or defenses regarding the applicability of Nebraska law or personal jurisdiction. This notice may be supplemented with new information learned after submission.

On May 9, 2025, Weathercraft experienced a disruption to its company's computer network. Weathercraft disconnected its systems and partnered with cyber incident specialists to investigate the nature and scope of the disruption. On or about May 12, 2025, Weathercraft determined certain files were taken from its network by someone without authorization. Weathercraft performed a thorough review of the files for the presence of sensitive personal information. On May 28, 2025, Weathercraft concluded that review and is notifying potentially impacted individuals out of an abundance of caution. The types of data impacted include names in combination with Social Security number and direct deposit account information.

On June 27, 2025, Weathercraft provided written notice of the event to three hundred and forty (340) Nebraska residents by regular U.S. mail. A sample copy of the notification letter is attached as Exhibit A.

Weathercraft's notice of this event includes a brief description of the incident, encouragement to remain vigilant for incidents of fraud or misuse, from any source, by reviewing account

Kennedys

statements and credit reports. The notice also includes the recommendation to report any suspicious activity to their financial institution or the service provider, file a report with law enforcement, notify their state attorney general, and/or contact the Federal Trade Commission for more information. Weathercraft confirmed the types of personal information subject to unauthorized access for each recipient and enclosed contact information for the major consumer reporting bureaus, state-specific regulators, and the number for a dedicated call center for obtaining resources to protect against fraud or misuse, should the individual find it appropriate to do so. Weathercraft is also offering impacted individuals twelve (12) months of identity monitoring at no cost to the individual.

Upon learning of the disruption Weathercraft immediately disconnected its systems and partnered with cyber incident specialists to investigate. Weathercraft contacted federal law enforcement and commenced a thorough review of files taken for notifying those potentially impacted. Weathercraft is also reviewing its policies and existing security controls it has in place to remain resilient against future threats. Weathercraft is reporting this event to other state regulatory offices where required.

This notice provides your Office with all information necessary to comply with Nebraska law. If you have any questions or need additional information, please do not hesitate to contact me directly.

Respectfully,

Nicholas S. Jajko

Nicholas Jajko
Partner
for Kennedys

Exhibit A

\.

<<Date>> (Format: Month Day, Year)

<<FIRST_NAME>> <<MIDDLE_NAME>> <<LAST_NAME>> <<SUFFIX>>
<<ADDRESS_1>>
<<ADDRESS_2>>
<<CITY>>, <<STATE_PROVINCE>> <<POSTAL_CODE>>
<<COUNTRY>>

Re: Notice of Data Event

Dear <<First_name>> <<Last_name>>:

The Weathercraft Company of Scottsbluff takes the privacy and security of its employee's information seriously. As part of that commitment, we are providing you with this notice of data event that impacted our company's computer systems within which your personal information was stored. This notice includes resources and steps you may take to help protect your information, should you feel it appropriate to do so.

What Happened?

On May 9, 2025, Weathercraft experienced a disruption to our company's computer network. We disconnected our systems and partnered with cyber incident specialists to investigate the nature and scope of the disruption. On or about May 12, 2025, we determined certain files were taken from our network by someone without authorization. We performed a thorough review of the files for the presence of sensitive personal information. On May 28, 2025, we concluded that review and we are notifying potentially impacted individuals out of an abundance of caution.

What Information Was Involved?

We are notifying you because our review confirmed that your name, Social Security number, and direct deposit financial account information were contained within files taken from our network. We stress that to date, we have no indication of any actual or attempted fraud or misuse of your information.

What We Are Doing?

We take this event and the privacy and security of your information seriously. Upon learning of the disruption we immediately disconnected our systems and partnered with cyber incident specialists to investigate. We contacted federal law enforcement and commenced a thorough review of files taken for notifying those potentially impacted. We are also reviewing the policies and existing security controls we have in place to remain resilient against future threats.

As an added precaution we have secured the services of Kroll to provide identity monitoring at no cost to you for <<Monitoring Term Length (Months)>> months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. Instructions for how to activate are below. Additional information about these services is enclosed.

What You Can Do.

We encourage you to remain vigilant for incidents of identity theft and fraud, from any source, by reviewing your account statements and monitoring credit reports. You should report any suspicious activity to the provider or your financial institution. You may also file a report with law enforcement, the state attorney general, and/or the Federal Trade Commission. Please refer to the enclosed "Steps You Can Take to Help Protect Your Information" which contains additional resources to take advantage of, should you find it appropriate to do so.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

*You have until **<<b2b_text_6(activation deadline)>>** to activate your identity monitoring services.*

Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

For More Information.

Weathercraft regrets any concern or inconvenience this may cause you and we remain committed to protecting the privacy and security of information entrusted in our care. If you have additional questions, please contact our dedicated response line at (866) 461-3178, Monday through Friday, from 8 a.m. and 5:30 p.m. Central Time, excluding major U.S. holidays. Please be sure to have your membership number ready when you call.

Very truly yours,

Scott Erickson

Scott Erickson
Weathercraft Company of Scottsbluff

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts and Credit Reports. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To obtain a free annual credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

Report Suspected Fraud. 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, your state Attorney General, and the FTC.

Place Fraud Alerts. You have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert, 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 lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

Place Security Freeze. As an alternative to a fraud alert, you 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 your 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 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 should provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);.
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); 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.

To place a fraud alert or credit freeze, contact the three major credit reporting bureaus listed below:

TransUnion 1- 800-916-8800 www.transunion.com **TransUnion Fraud Alert** P.O. Box 2000 Chester, PA 19016-2000 **TransUnion Credit Freeze** P.O. Box 160 Woodlyn, PA 19094	**Experian** 1-888-397-3742 www.experian.com **Experian Fraud Alert** P.O. Box 9554 Allen, TX 75013 **Experian Credit Freeze** P.O. Box 9554 Allen, TX 75013	**Equifax** 1-888-378-4329 www.equifax.com **Equifax Fraud Alert** P.O. Box 105069 Atlanta, GA 30348-5069 **Equifax Credit Freeze** P.O. Box 105788 Atlanta, GA 30348-5788

Obtain 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 Federal Trade Commission (FTC). The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. This notice has not been delayed by law enforcement.

For New Mexico Residents, you have certain rights under the FCRA, which include: (1) You must be told if information in your file has been used against you; (2) You have the right to know what is in your file (you "file disclosure"); (3) You have the right to ask for a credit score; (4) You have the right to dispute incomplete or inaccurate information; (5) Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (6) Consumer reporting agencies may not report outdated negative information; (7) Access to your file is limited to people with a valid need; (8) You must give your consent for reports to be provided to employers; (8) You may limit "pre-screened" offers of credit and insurance you get based on information in your credit report; (9) You may seek damages from violators; and (10) identity theft victims and active duty military personnel have additional rights. For more information contact the Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave NW, Washington, DC 20580.

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.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.