

June 29, 2023

Moore & Van Allen

VIA EMAIL AND FEDEX

Attorney General Anthony G. Brown
Office of the Attorney General
200 St. Paul Place, 25th Floor
Baltimore, MD 21202
Email: IDTheft@oag.state.md.us

Suzanne K. Gainey
Attorney at Law

T 704 331 3559
F 704 378 1959
suzannegainey@mvalaw.com

Moore & Van Allen PLLC

100 North Tryon Street
Suite 4700
Charlotte, NC 28202-4003

Dear Attorney General Brown:

We represent Nucor Corporation and its affiliates, subsidiaries and divisions (collectively, “**Nucor**”), and are writing to notify you of a recent incident of unauthorized access to the personal information of four (4) Maryland residents.

On approximately June 1, 2023, Nucor was informed by one of its third-party software vendors that a previously-unknown vulnerability existed in the widely-used file transfer software offered by the vendor. Nucor uses this software to transfer various types of files to third parties. Upon being notified of the vulnerability, Nucor immediately disabled external access to the software and applied the security fix provided by the vendor. Nucor also launched an extensive investigation and discovered that between approximately May 26, 2023 and June 1, 2023 – before Nucor was notified of the vulnerability and applied the security fix – certain electronic files were acquired by unauthorized third parties who were able to exploit the software vulnerability.

Nucor’s investigation revealed that the files that were acquired as a result of the vulnerability contained the name, bank account number, amounts deposited to such account, and routing number of the impacted Maryland residents (similar to the information found on the face of a personal check). Each of these residents will receive notice of such incident shortly via a written letter, a sample of which is attached.

Please note that Nucor is offering the impacted Maryland residents twenty-four (24) months of free credit monitoring and identity theft prevention services. Nucor takes the security of personal information seriously and is working to prevent similar incidents from happening in the future.

If you should have any further questions or need additional information, please contact me (Suzanne Gainey) at 704-331-3559 or suzannegainey@mvalaw.com.

Sincerely,



Suzanne K. Gainey
Moore & Van Allen PLLC

cc: Doug Wilner (Nucor)

Charlotte, NC
Charleston, SC



Nucor Corporation
1915 Rexford Road
Charlotte, NC 28211

<<DATE>>

<<FULL NAME>>

<<STREET ADDRESS>>

<<CITY, STATE ZIP CODE>>

RE: Notice of Data Breach

Dear <<FIRST NAME>>,

As you may already be aware, Nucor was recently impacted by a cybersecurity attack. We are writing to let you know that this attack impacted your personal information. We take the security of your personal information seriously and want to provide you with information about this incident, our response, and steps you can take to prevent fraud, should you feel it necessary to do so.

What Happened? On approximately June 1, 2023, we were informed by one of our third-party software vendors that a previously-unknown vulnerability existed in the widely-used file transfer software offered by the vendor. Nucor uses this software to transfer various types of files to third parties. Upon being notified of the vulnerability, we immediately disabled external access to the software and applied the security fix provided by the vendor. We also launched an extensive investigation and discovered that between approximately May 26, 2023 and June 1, 2023, before we were notified of the vulnerability, certain electronic files were acquired by unauthorized third parties.

What Information Was Involved? Our investigation revealed that the files that were acquired contained your name, bank account number, routing number and amounts deposited to your account, which is similar to the information that appears on the face of a personal check.

What We Are Doing. As noted above, as soon as we were notified of the vulnerability, we immediately disabled external access to the file transfer software and applied the security fix provided by the vendor. We also launched an extensive investigation with assistance from an external cybersecurity firm to determine the full impact of the vulnerability. Additionally, we are providing written notice of this incident to those impacted so that they can take steps to prevent possible fraud, and have notified, or will notify, state regulators and consumer reporting agencies, where required.

As an added precaution, **we are offering a two (2) year subscription to Equifax's Complete™ Premier service at no cost to you.** Key features of the Complete™ Premier service include:

- Annual access to your 3-bureau credit report and VantageScore credit scores;
- Daily access to your Equifax credit report and 1-bureau VantageScore credit score;
- 3-bureau credit monitoring with email notifications of key changes to your credit reports;
- WebScan notifications when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites;
- Automatic fraud alerts, which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock;

- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf;
- Up to \$1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft; and
- Lost Wallet Assistance if your wallet is lost or stolen, and one-stop assistance in canceling and reissuing credit, debit and personal identification cards.

To accept this offer, please activate your subscription by **September 30, 2023** by visiting www.equifax.com/activate. Enter your unique Activation Code of **<ACTIVATION CODE>** and click "Submit". Then, complete the following steps:

1. **Register:** Complete the form with your contact information and click "Continue". Or, if you already have a myEquifax account, click the "Sign in here" link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4 below.
2. **Create Account:** Enter your email address, create a password and accept the terms of use.
3. **Verify Identity:** To enroll in the product, Equifax will ask you to complete its identity verification process.
4. **Checkout:** Upon successful verification of your identity, you will see the Checkout Page. Click "Sign Me Up" to finish enrolling.

The confirmation page will show your completed enrollment. You can click on "View My Product" to access the product features. We encourage you to enroll in these services, as we are unable to do so on your behalf.

What You Can Do. In addition to enrolling in Equifax's Complete™ Premier service, we recommend that you:

- use good judgment in not responding to emails or other inquiries by those posing as a financial institution or other entities seeking your personal information;
- carefully review all account statements and, if anything seems suspicious, place a fraud alert on your credit file. A fraud alert tells creditors to contact you before opening any new accounts or changing your existing accounts; and
- check your credit reports periodically. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

Additionally, you can review the enclosed *Steps You Can Take to Protect Against Identity Theft and Fraud*, which includes guidance on steps you can take to better protect against the possibility of fraud and identify theft.

For More Information. We sincerely regret any inconvenience or concern this incident may have caused you. If you have questions or concerns that are not addressed in this letter, please call **<<PHONE NUMBER>>** weekdays between 9 am and 9 pm EST.

Sincerely,

Greg Murphy
Executive Vice President, Business Services & General Counsel
Nucor Corporation

Steps You Can Take to Protect Against Identity Theft and Fraud

Monitor Your Accounts:

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements closely, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

At no charge, you can also have these credit bureaus place a “fraud alert” on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the credit reporting bureaus below.

Alternatively, you may place a security freeze on your credit reports, which prohibits a credit bureau from releasing any information from your credit report without your written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide some or all of the following information to the credit reporting agency, depending on whether you do so online, by phone or by mail:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of Birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
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.

To find out more on how to place a security freeze, please contact the credit reporting bureaus below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services	www.experian.com/freeze/center.html	www.transunion.com/credit-freeze
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069, Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788, Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information:

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting the credit reporting bureaus, Federal Trade Commission or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such

a complaint by way of the contact information listed above. 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 be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

If you are a resident of the District of Columbia, you may obtain information about preventing and avoiding identity theft from the Office of the Attorney General for the District of Columbia at: 400 6th Street NW, Washington, D.C. 20001, 1-202-727-3400, <https://oag.dc.gov/>.

If you are a resident of Iowa, you are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General at: Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319, 1-888-777-4590, consumer@ag.iowa.gov.

If you are a resident of Maryland, you may obtain information from the Maryland Attorney General about steps you can take to avoid identity theft at: 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, consumer@oag.state.md.us.

If you are a resident of New Mexico, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing to Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

If you are a resident of New York, you may obtain information about security breach response and identity theft prevention and protection from the New York Attorney General at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>.

If you are a resident of North Carolina, you may obtain information about preventing identity theft from the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-919-716-6400, <https://www.ncdoj.gov>.

If you are a resident of Oregon, you are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Office of the Attorney General at: 1162 Court St. NE, Salem, OR 97301-4096, 1-877-877-9392, www.doj.state.or.us.