

STATE OF NORTH CAROLINA
COUNTY OF WAKE

IN THE GENERAL COURT OF JUSTICE
SUPERIOR COURT DIVISION
CASE No: _____

CHRISTOPHER BURLESON,)
on behalf of himself and all)
others similarly situated,)
Plaintiff,)
v.)
NUCOR CORPORATION,)
Defendant.)

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Christopher Burleson, individually and on behalf of all similarly situated persons, alleges the following against Nucor Corporation (“NUCOR” or “Defendant”) based upon personal knowledge with respect to himself and on information and belief derived from, among other things, investigation by his counsel and review of public documents, as to all other matters:

NATURE OF THE ACTION

1. Plaintiff brings this class action against NUCOR for its failure to properly secure and safeguard Plaintiff’s and other similarly situated NUCOR employees’ sensitive information, including names, bank account number, routing number and amounts deposits to employees’ accounts ("personally identifiable information" or “PII”).

2. Defendant is an American producer of steel and related products based in Charlotte, North Carolina.

3. Upon information and belief, former and current employees of Defendant are required to entrust Defendant, directly or indirectly, with sensitive, non-public PII, without which

Defendant could not perform its regular business activities. Defendant retains this information for at least many years and even after the employee-employer relationship has ended.

4. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

5. On or about June 1, 2023, Defendant learned that one of its IT vendors had been penetrated by a cyberattack and that a “previously-unknown vulnerability existed in the widely-used file transfer software offered by the vendor.”¹ In response, Defendant “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.”² As a result of its investigation, Defendant concluded that Plaintiff’s and Class Members’ PII was compromised in the Data Breach.³

6. According to NUCOR’s letter, sent to Plaintiff and Class Members on behalf of Defendant (the “Notice Letter”), the compromised PII included individuals’ names, bank account number, routing number and amounts deposits to employees’ accounts.⁴

7. Defendant failed to adequately protect Plaintiff’s and Class Members PII—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted PII was compromised due to Defendant's negligent and/or careless acts and omissions and their utter failure to protect employees’ sensitive data. Hackers targeted and obtained Plaintiff’s and Class Members’ PII because of its value in exploiting and stealing the identities of Plaintiff and Class

¹ The "Notice Letter." Attached hereto as *Exhibit A*.

² *Id.*

³ *Id.*

⁴ *Id.*

Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

8. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts at least to negligence and violates federal and state statutes.

9. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures and ensure those measures were followed by its IT vendors to ensure that the PII of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party.

10. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

11. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) invasion of privacy; (ii) lost or diminished value of PII; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to

access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

12. Plaintiff and Class Members seek to remedy these harms and prevent any future data compromise on behalf of himself and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

13. Plaintiff seeks remedies including, but not limited to, compensatory damages, nominal damages, and reimbursement of out-of-pocket costs.

14. Plaintiff also seeks injunctive and equitable relief to prevent future injury on behalf of himself and the putative Class.

PARTIES

15. Plaintiff Christopher Burleson, is, and at all times mentioned herein was, an individual citizen of Texas and an employee of Defendant.

16. Defendant Nucor Corporation is a Delaware corporation with its principal place of business located in North Carolina.

JURISDICTION AND VENUE

17. This Court has jurisdiction over Defendant because Nucor Corporation regularly conducts business in North Carolina. Defendant intentionally avails itself of the consumers and markets within the State of North Carolina, which renders the exercise of jurisdiction by North Carolina courts over Defendant permissible under judicially accepted notions of fair play and substantial justice.

18. Venue is proper in Wake County. The proposed Class includes individuals who reside in Wake County; and the parties have met and conferred and have agreed to litigate this matter in Wake County without prejudice to Nucor's right to object to venue in Wake County in any future matter.

FACTUAL ALLEGATIONS

Defendant's Business

19. Defendant is a commercial steel manufacturer, which Plaintiff is an employee of.
20. Plaintiff and Class Members are current and former employees of Defendant's.
21. As a condition of receiving employment, NUCOR requires that its employees, including Plaintiff and Class Members, entrust it with highly sensitive personal information.
22. The information held by Defendant in its computer systems or those of its vendors at the time of the Data Breach included the unencrypted PII of Plaintiff and Class Members.
23. Upon information and belief, Defendant made promises and representations to its employees, including Plaintiff and Class Members, that the PII collected from them as a condition of obtaining employment from Defendant, employee PII would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

24. Indeed, Defendant's Privacy Policy provides that:

We take the protection of your Personal Information seriously. We protect Personal Information against loss and theft as well as unauthorized access, disclosure, copying, use, and modification using security safeguards, including physical, organization and technological measures, commensurate with the sensitivity of your Personal Information. Employees who have access to your information are made aware of the importance of keeping it confidential.

Where we use service providers who might have access to your

Personal Information, we require them to have privacy and security standards that are comparable to ours. We use contracts and other measures with our service providers to maintain the confidentiality and security of your Personal Information and to prevent it from being used for any other purpose.

However, since no method of electronic storage is 100% secure, we cannot guarantee the absolute security of the information stored. We also cannot guarantee that information you supply will not be intercepted while being transmitted to us over the Internet.

We retain Personal Information that we collect only as long as reasonably necessary to fulfill the purposes for which it was collected or to meet any applicable legal requirements.

In some instances, you may be required to choose a user ID and password when you register for the Services. To the extent user IDs and passwords are utilized, you may not share your user ID and password with anyone else, and you are solely responsible for maintaining and protecting the confidentiality of your user ID and password. You are fully responsible for all activities that occur through the use of your user ID and password.⁵

25. Plaintiff and Class Members provided their PII to Defendant, directly or indirectly, with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

26. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiff and Class Members relied on the sophistication of Defendant to keep their PII confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members value the confidentiality of their PII and demand security to safeguard their PII.

⁵ <https://nucor.com/privacy> (last accessed Aug. 9, 2023).

27. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties and to audit, monitor, and verify the integrity of its IT vendors and affiliates. Defendant has a legal duty to keep consumer's PII safe and confidential.

28. Defendant had obligations created by FTC Act, contract, industry standards, and representations made to Plaintiff and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

29. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class Members' PII. Without the required submission of PII, Defendant could not perform the services it provides.

30. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

The Data Breach

31. On or about June 30, 2023, Defendant, began sending Plaintiff and other Data Breach victims an untitled letter (the "Notice Letter"), informing them that:

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.⁶

32. Omitted from the Notice Letter were the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their PII remains protected.

33. This “disclosure” amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach’s critical facts. Without these details, Plaintiff’s and Class Members’ ability to mitigate the harms resulting from the Data Breach is severely diminished.

34. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed. Moreover, Defendant failed to exercise due diligence in selecting its IT vendors or deciding with whom it would share sensitive PII.

35. The attacker accessed and acquired files Defendant shared with a third party containing unencrypted PII of Plaintiff and Class Members, including their bank account numbers and other sensitive information. Plaintiff’s and Class Members’ PII was accessed and stolen in the Data Breach.

36. Plaintiff further believes his PII, and that of Class Members, was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals

⁶ Notice Letter.

that commit cyber-attacks of this type.

Data Breaches Are Preventable

37. Defendant could have prevented this Data Breach by, among other things, properly encrypting PII being shared with its vendors or otherwise ensuring that such PII was protected while in transit or accessible.

38. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed.

39. The unencrypted PII of Class Members will end up for sale to identity thieves on the dark web, if it has not already, or it could simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII of Plaintiff and Class Members.

40. As explained by the Federal Bureau of Investigation, “[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection.”⁷

41. To prevent and detect cyber-attacks and/or ransomware attacks Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework

⁷ How to Protect Your Networks from RANSOMWARE, at 3, *available at: <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view>* (last visited August 9, 2023).

(SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.⁸

⁸ *Id.* at 3-4.

42. To prevent and detect cyber-attacks or ransomware attacks Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office[Visual Basic for Applications].⁹

⁹ See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), available at: <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/> (last visited August 9, 2023).

43. Given that Defendant was storing and sharing the PII of its current and former employees, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

44. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the PII of more than eight thousand current and former employees of Defendant, including that of Plaintiff and Class Members.

Defendant Acquires, Collects, And Stores Plaintiff's and the Class's PII

45. As a condition to obtain employment from NUCOR, Plaintiff and Class Members were required to give their sensitive and confidential PII, directly or indirectly, to Defendant.

46. Defendant retains and stores this information and derives a substantial economic benefit from the PII that they collect. But for the collection of Plaintiff's and Class Members' PII, Defendant would be unable to offer employment to Plaintiff and Class Members.

47. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that they were responsible for protecting the PII from disclosure.

48. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep their PII confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

49. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the PII of Plaintiff and Class Members or by exercising due diligence in selecting its IT vendors and properly auditing those vendor's security

practices.

50. Upon information and belief, Defendant made promises to Plaintiff and Class Members to maintain and protect their PII, demonstrating an understanding of the importance of securing PII.

51. Indeed, Defendant's Privacy Policy provides that:

We take the protection of your Personal Information seriously. We protect Personal Information against loss and theft as well as unauthorized access, disclosure, copying, use, and modification using security safeguards, including physical, organization and technological measures, commensurate with the sensitivity of your Personal Information. Employees who have access to your information are made aware of the importance of keeping it confidential.

Where we use service providers who might have access to your Personal Information, we require them to have privacy and security standards that are comparable to ours. We use contracts and other measures with our service providers to maintain the confidentiality and security of your Personal Information and to prevent it from being used for any other purpose.

However, since no method of electronic storage is 100% secure, we cannot guarantee the absolute security of the information stored. We also cannot guarantee that information you supply will not be intercepted while being transmitted to us over the Internet.

We retain Personal Information that we collect only as long as reasonably necessary to fulfill the purposes for which it was collected or to meet any applicable legal requirements.

In some instances, you may be required to choose a user ID and password when you register for the Services. To the extent user IDs and passwords are utilized, you may not share your user ID and password with anyone else, and you are solely responsible for maintaining and protecting the confidentiality of your user ID and password. You are fully responsible for all activities that occur through the use of your user ID and

password.¹⁰

52. Defendant's negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

Defendant Knew or Should Have Known of the Risk Because Companies In Possession Of PII Are Particularly Susceptable To Cyber Attacks

53. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting companies that collect and store PII, like Defendant, preceding the date of the breach.

54. Data thieves regularly target companies like Defendant's due to the highly sensitive information that they custody. Defendant knew and understood that unprotected PII is valuable and highly sought after by criminal parties who seek to illegally monetize that PII through unauthorized access.

55. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.¹¹

56. The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.¹²

57. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one

¹⁰ <https://nucor.com/privacy> (last accessed Aug. 9, 2023).

¹¹ See 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at <https://notified.idtheftcenter.org/s/>), at 6.

¹² *Id.*

report explained, smaller entities that store PII are “attractive to ransomware criminals...because they often have lesser IT defenses and a high incentive to regain access to their data quickly.”¹³

58. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that the PII that they collected and maintained would be targeted by cybercriminals.

59. As a custodian of PII, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to it by Plaintiff and Class members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiff and Class Members as a result of a breach.

60. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

61. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

¹³ https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection (last accessed Aug. 9, 2023).

62. Additionally, as companies became more dependent on computer systems to run their business,¹⁴ *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of Things (“IoT”), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.¹⁵

63. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to potentially over one million individuals’ detailed PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

64. In the Notice Letter, Defendant offers to cover credit monitoring services for a period of 24 months. This is wholly inadequate to compensate Plaintiff and Class Members as it fails to provide for the fact victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiff and Class Members’ PII. Moreover, once this service expires, Plaintiff and Class Members will be forced to pay out of pocket for necessary identity and/or credit monitoring services.

65. Defendant's offer of credit and identity monitoring establishes that Plaintiff's and Class Members’ sensitive PII *was* in fact affected, accessed, compromised, and exfiltrated from Defendant's computer systems.

66. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of

¹⁴ <https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html> (last accessed Aug. 9, 2023).

¹⁵ <https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022> (last accessed Aug. 9, 2023).

Plaintiff and Class Members.

67. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen—particularly bank account and routing numbers—fraudulent use of that information and damage to victims may continue for years.

68. As a company in possession of its current and former employees' PII, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to them by Plaintiff and Class Members and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiff and Class Members as a result of a breach. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

Value Of Personally Identifiable Information

69. The Federal Trade Commission (“FTC”) defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.”¹⁶ The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, Social Security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.”¹⁷

70. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen

¹⁶ 17 C.F.R. § 248.201 (2013).

¹⁷ *Id.*

identity credentials.¹⁸

71. For example, PII can be sold at a price ranging from \$40 to \$200.¹⁹ Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.²⁰

72. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change—bank account and routing numbers.

73. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black market.”²¹

74. Among other forms of fraud, identity thieves may obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police.

75. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability

¹⁸ *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last accessed Aug. 9, 2023).

¹⁹ *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last accessed Aug. 9, 2023).

²⁰ *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last visited Aug. 9, 2023).

²¹ Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last accessed Aug. 9, 2023).

Office (“GAO”), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.²²

NUCOR Failed to Comply with FTC Guidelines

76. The Federal Trade Commission (“FTC”) has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company’s failure to maintain reasonable and appropriate data security for consumers’ sensitive personal information is an “unfair practice” in violation of Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

77. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network’s vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

²² *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <https://www.gao.gov/assets/gao-07-737.pdf> (last accessed Aug. 9, 2022).

78. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

79. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

80. These FTC enforcement actions include actions against insurance companies, like Defendant.

81. As evidenced by the Data Breach, NUCOR failed to properly implement basic data security practices and failed to audit, monitor, or ensure the integrity of its vendor's data security practices. NUCOR's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

82. NUCOR was at all times fully aware of its obligation to protect the PII of its employees yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

NUCOR Failed to Comply with Industry Standards

83. As noted above, experts studying cybersecurity routinely identify companies like Defendant as being particularly vulnerable to cyberattacks because of the value of the PII which

they collect and maintain.

84. Some industry best practices that should be implemented by companies dealing with sensitive PII, like NUCOR, include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all of these industry best practices.

85. Other best cybersecurity practices that are standard include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

86. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

87. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

NUCOR Breached its Duty to Safeguard Plaintiff's and Class Members' PII

88. In addition to its obligations under federal and state laws, NUCOR owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing,

safeguarding, deleting, and protecting the PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. NUCOR owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the PII of Class Members

89. NUCOR breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data and failed to audit, monitor, or ensure the integrity of its vendor's data security practices. NUCOR's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;
- b. Failing to adequately protect employees' PII;
- c. Failing to properly monitor its own data security systems for existing intrusions;
- d. Failing to audit, monitor, or ensure the integrity of its vendor's data security practices;
- e. Failing to sufficiently train its employees and vendors regarding the proper handling of its employees' PII;
- f. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;
- g. Failing to adhere to the industry standards for cybersecurity as discussed above; and
- h. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' PII.

90. NUCOR negligently and unlawfully failed to safeguard Plaintiff's and Class Members' PII by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted PII.

91. Had NUCOR remedied the deficiencies in its information storage and security systems or those of its vendors and affiliates, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential PII.

Common Injuries & Damages

92. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their PII; (e) invasion of privacy; and (f) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII.

The Data Breach Increases Victims' Risk Of Identity Theft

93. Plaintiff and Class Members are at a heightened risk of identity theft for years to come.

94. The unencrypted PII of Class Members will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted PII may fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII of Plaintiff and

Class Members.

95. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

96. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity--or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

97. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victim.

98. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.²³

²³ "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to \$100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule

99. With “Fullz” packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

100. The development of “Fullz” packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiffs’ and Class Members’ phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

101. The existence and prevalence of “Fullz” packages means that the PII stolen from the data breach can easily be linked to the unregulated data (like driver's license numbers) of Plaintiff and the other Class Members.

102. Thus, even if certain information (such as driver's license numbers) was not stolen in the data breach, criminals can still easily create a comprehensive “Fullz” package.

103. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

Loss Of Time To Mitigate Risk Of Identity Theft And Fraud

104. As a result of the recognized risk of identity theft, when a Data Breach occurs,

account” (an account that will accept a fraudulent money transfer from a compromised account) without the victim’s knowledge. *See, e.g.,* Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), <https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-/>(<https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/>) (last accessed on Aug. 9, 2023).

and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

105. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class Members must, as Defendant’s Notice Letter instructs,²⁴ "remain vigilant" and monitor their financial accounts for many years to mitigate the risk of identity theft.

106. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience as a result of the Data Breach, such as researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter.

107. These efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches (“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”²⁵

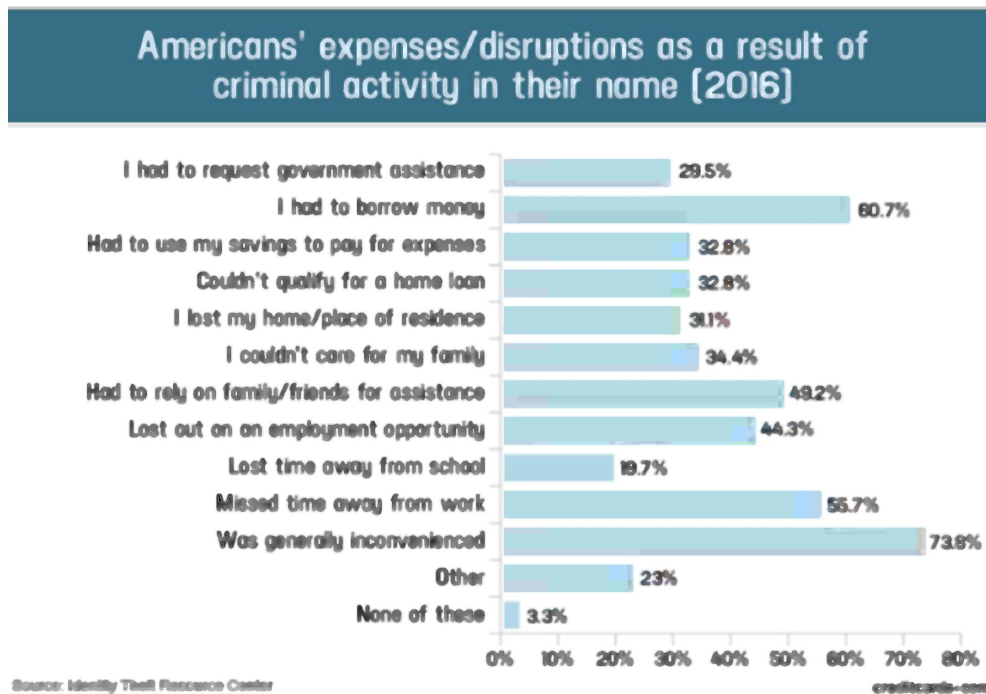
108. These efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit

²⁴ Notice Letter.

²⁵ See United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), <https://www.gao.gov/new.items/d07737.pdf>.

reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.²⁶

109. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:²⁷



110. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches (“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”²⁸

²⁶ See Federal Trade Commission, *Identity Theft.gov*, <https://www.identitytheft.gov/Steps> (last visited Aug. 9, 2023).

²⁷ Credit Card and ID Theft Statistics” by Jason Steele, 10/24/2017, at: <https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php> (last visited Sep 13, 2022).

²⁸ See “Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,” p. 2, U.S. Government Accountability Office, June 2007, <https://www.gao.gov/new.items/d07737.pdf> (last accessed Aug. 9, 2023) (“GAO Report”).

Diminution Value Of PII

111. PII is a valuable property right.²⁹ Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

112. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly \$200 billion.³⁰

113. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.^{31,32}

114. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to \$50.00 a year.³³

115. Conversely sensitive PII can sell for as much as \$363 per record on the dark web according to the Infosec Institute.³⁴

116. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an

²⁹ See, e.g., Randall T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

³⁰ <https://www.latimes.com/business/story/2019-11-05/column-data-brokers> (last accessed Aug. 9, 2023).

³¹ <https://datacoup.com/> (last accessed Aug. 9, 2023).

³² <https://worlddataexchange.com/about> (last accessed Aug. 9, 2023).

³³ Nielsen Computer & Mobile Panel, *Frequently Asked Questions*, available at <https://computermobilepanel.nielsen.com/ui/US/en/faqen.html> (last accessed Aug. 9, 2023).

³⁴ See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/> (last accessed Aug. 9, 2023).

inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

117. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change.

118. Among other forms of fraud, identity thieves may obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police.

119. The fraudulent activity resulting from the Data Breach may not come to light for years.

120. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, and of the foreseeable consequences that would occur if Defendant’s data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

121. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant’s network, amounting to over one million individuals’ detailed personal information, upon information and belief, and thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

122. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary

123. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII involved, and the volume of data obtained in the Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes –e.g., opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

124. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or his Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

125. Consequently, Plaintiff and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

126. The retail cost of credit monitoring and identity theft monitoring can cost around \$200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard their PII.

Loss Of The Benefit Of The Bargain

127. Furthermore, Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to pay Defendant and/or its agents for products and/or services, Plaintiff and other reasonable consumers understood and expected that they were, in part, paying for the product and/or service and necessary data security to protect the PII, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received products and/or services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

Plaintiff Experience

128. Plaintiff Christopher Burleson is an employee of NUCOR.

129. As a condition of receiving employment with NUCOR, he was required to provide his PII, directly or indirectly, to Defendant, including his name, bank account number and routing number.

130. At the time of the Data Breach—approximately May 26, 2023, through June 1, 2023—Defendant retained Plaintiff's PII in its system.

131. Plaintiff is very careful about sharing his sensitive PII. Plaintiff stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff would not have entrusted his PII to Defendant had he known of Defendant's lax data security policies.

132. Plaintiff Christopher Burleson received the Notice Letter, by U.S. mail, from Defendant, dated June 30, 2023. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including his name, bank account number and routing number.

133. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter. Plaintiff has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

134. Plaintiff suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) lost or diminished value of PII; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

135. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed his of key details about the Data Breach's occurrence.

136. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

137. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

138. Plaintiff Christopher Burleson has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected

and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

139. Plaintiff brings this action individually and on behalf of all other persons similarly situated. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

All individuals whose PII was impacted as a result of the Data Breach (the “Class”).

140. Excluded from the Class are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

141. Plaintiff reserves the right to modify or amend the definition of the proposed Nationwide Class, as well as add subclasses, before the Court determines whether certification is appropriate.

142. The proposed Class meets the criteria for certification under Rule 23 of the North Carolina Rules of Civil Procedure.

143. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time it is likely hundreds, if not thousands of individuals had their PII compromised in this Data Breach, given the Defendant operates widely throughout the United States. The identities of Class Members are ascertainable through Defendant’s records, Class Members’ records, publication notice, self-identification, and other means.

144. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

- a. Whether NUCOR engaged in the conduct alleged herein;
- b. Whether NUCOR's conduct violated the FTCA;
- c. When NUCOR learned of the Data Breach;
- d. Whether NUCOR's response to the Data Breach was adequate;
- e. Whether NUCOR unlawfully lost or disclosed Plaintiff's and Class Members' PII;
- f. Whether NUCOR failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the PII compromised in the Data Breach;
- g. Whether NUCOR's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- h. Whether NUCOR's data security systems prior to and during the Data Breach were consistent with industry standards;
- i. Whether NUCOR owed a duty to Class Members to safeguard their PII;
- j. Whether NUCOR breached its duty to Class Members to safeguard their PII;
- k. Whether hackers obtained Class Members' PII via the Data Breach;
- l. Whether NUCOR had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and the Class Members;
- m. Whether NUCOR breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;
- n. Whether NUCOR knew or should have known that its data security systems and monitoring processes were deficient;
- o. What damages Plaintiff and Class Members suffered as a result of NUCOR's misconduct;
- p. Whether NUCOR's conduct was negligent;
- q. Whether NUCOR was unjustly enriched;
- r. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages;
- s. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and
- t. Whether Plaintiff and Class Members are entitled to equitable relief, including

injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

145. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of every other Class Member, was compromised in the Data Breach. Plaintiff's claims are typical of those of the other Class Members because, inter alia, all Class Members were injured through the common misconduct of NUCOR. Plaintiff is advancing the same claims and legal theories on behalf of himself and all other Class Members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class Members arise from the same operative facts and are based on the same legal theories.

146. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

147. Predominance. NUCOR has engaged in a common course of conduct toward Plaintiff and Class Members in that all of Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from NUCOR's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

148. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual

Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for NUCOR. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

149. The nature of this action and the nature of laws available to Plaintiff and the Class make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and the Class for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

150. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

151. Adequate notice can be given to Class Members directly using information maintained in Defendant NUCOR's records.

152. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Class Members, may continue to refuse to provide proper notification

to Class Members regarding the Data Breach, and may continue to act unlawfully as set forth in this Complaint.

153. All conditions precedent to bringing this action have been satisfied and/or waived.

154. Finally, all members of the proposed Class are readily ascertainable. NUCOR has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent Notice of the Data Breach by NUCOR.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

155. Plaintiff restates and realleges the preceding factual allegations set forth above as if fully alleged herein.

156. Defendant requires its employees, including Plaintiff and Class Members, to submit non-public PII in the ordinary course of receiving employment.

157. Defendant gathered and stored the PII of Plaintiff and Class Members as part of its business of soliciting employment with Defendant, which solicitations and services affect commerce.

158. Plaintiff and Class Members entrusted Defendant with their PII, directly or indirectly, with the understanding that Defendant would safeguard their information.

159. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

160. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information

from theft. Defendant's duty included a responsibility to exercise due diligence in selecting IT vendors and to audit, monitor, and ensure the integrity of its vendor's systems and practices and to give prompt notice to those affected in the case of a data breach.

161. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

162. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the PII.

163. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant, Plaintiff and Class Members. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII, a necessary part of obtaining employment with Defendant.

164. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII.

165. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

166. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former employees' PII it was no longer required to retain pursuant to regulations.

167. Moreover, Defendant had a duty to promptly and adequately notify Plaintiff and

the Class of the Data Breach.

168. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiff and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

169. Defendant breached its duties, pursuant to the FTC Act and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;
- b. Failing to adequately monitor the security of their networks and systems;
- c. Failing to audit, monitor, or ensure the integrity of its vendor's data security practices;
- d. Allowing unauthorized access to Class Members' PII;
- e. Failing to detect in a timely manner that Class Members' PII had been compromised;
- f. Failing to remove former employees' PII it was no longer required to retain pursuant to regulations,
- g. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and
- h. Failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

170. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained

and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

171. Plaintiff and Class Members were within the class of persons the Federal Trade Commission Act was intended to protect and the type of harm that resulted from the Data Breach was the type of harm these statutes were intended to guard against.

172. Defendant's violation of Section 5 of the FTC Act constitutes negligence.

173. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

174. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

175. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the insurance industry.

176. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed.

177. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.

178. It was therefore foreseeable that the failure to adequately safeguard Class Members'

PII would result in one or more types of injuries to Class Members.

179. Plaintiff and the Class had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

180. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

181. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

182. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

183. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the PII of Plaintiff and the Class would not have been compromised.

184. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The PII of Plaintiff and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

185. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of PII; (iii) lost time and opportunity costs associated with attempting to

mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

186. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

187. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

188. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

189. Defendant's negligent conduct is ongoing, in that it still holds the PII of Plaintiff and Class Members in an unsafe and insecure manner.

190. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

191. Plaintiff restates and realleges all of the allegations stated above as if fully set forth herein.

192. Plaintiff and the Class entrusted their PII to Defendant as a condition of obtaining employment and receiving services from Defendant. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen. These implied contracts may be composed, in part, of the written policies posted on Defendant's website, including its Privacy Policy and Terms of Use, and its HIPAA Notice of Privacy Practices.

193. At the time Defendant acquired the PII of Plaintiffs and the Class, there was a meeting of the minds and a mutual understanding that Defendant would safeguard the PII and not take unjustified risks when storing the PII.

194. Implicit in the agreements between Plaintiff and Class Members and Defendant to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses, and (f) retain the PII only under conditions that kept such information secure and confidential.

195. Plaintiff and the Class would not have entrusted their PII to Defendant had they known that Defendant would make the PII internet-accessible, not encrypt sensitive data elements

such as bank account and routing numbers, and not delete the PII that Defendant no longer had a reasonable need to maintain it.

196. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

197. Defendant breached the implied contracts they made with Plaintiff and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiff and the Class once the relationship ended, and by failing to provide timely and accurate notice to them that personal information was compromised because of the Data Breach.

198. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

199. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages to be determined at trial.

COUNT III
Breach Of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

200. Plaintiff restates and realleges all of the allegations stated above as if fully set forth

herein.

201. In providing their PII, directly or indirectly, to Defendant, Plaintiff and Class members justifiably placed a special confidence in Defendant to act in good faith and with due regard to interests of Plaintiff and class members to safeguard and keep confidential that PII.

202. Defendant accepted the special confidence Plaintiff and Class members placed in it, as evidenced by its assertion that it is committed to protecting the privacy of Plaintiff's and Class Members' personal information as detailed in its Privacy Policy.

203. In light of the special relationship between Defendant and Plaintiff and Class members, whereby Defendant became a guardian of Plaintiff's and Class members' PII, Defendant became a fiduciary by its undertaking and guardianship of the PII, to act primarily for the benefit of its employees, including Plaintiff and Class members, for the safeguarding of Plaintiff and Class member's PII.

204. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of its relationship with Defendants' employees, in particular, to keep secure the PII of its employees.

205. Defendant breached its fiduciary duties to Plaintiff and Class members by failing to protect the integrity of the systems containing Plaintiff's and Class member's PII.

206. Defendant breached its fiduciary duties to Plaintiff and class members by otherwise failing to safeguard Plaintiff's and Class members' PII.

207. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and class members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of PII; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of

benefit of the bargain; and (v) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

208. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT IV
Breach Of Confidence
(On Behalf of Plaintiff and the Class)

209. Plaintiff restates and realleges all of the allegations stated above as if fully set forth herein.

210. At all times during Plaintiff and Class members' interactions with Defendant, Defendant was fully aware of the confidential, novel, and sensitive nature of Plaintiff's and the Class members' PII that Plaintiff and Class members provided to Defendant.

211. As alleged herein and above, Defendant's relationship with Plaintiff and Class members was governed by expectations that Plaintiff and Class members' PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

212. Plaintiffs and Class members provided their respective PII to Defendant, directly or indirectly, with the explicit and implicit understandings that Defendant would protect and not permit the PII to be disseminated to any unauthorized parties.

213. Plaintiffs and Class members also provided their respective PII to Defendant with the explicit understanding that Defendant would take precautions to protect that PII from unauthorized disclosure, such as following basic principles of information security practices.

214. Defendant voluntarily received in confidence Plaintiff and Class members' PII with the understanding that the PII would not be disclosed or disseminated to the public or any unauthorized third parties.

215. Due to Defendant's failure to prevent, detect, and/or avoid the Data Breach from occurring by, *inter alia*, failing to follow best information security practices to secure Plaintiffs' and Class members' PII, Plaintiffs' and Class members' PII was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs' and Class members' confidence, and without their express permission.

216. But for Defendant's disclosure of Plaintiffs' and Class members' PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiffs' and Class members' PII, as well as the resulting damages.

217. The injury and harm Plaintiffs and Class members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiffs' and Class members' PII. Defendant knew or should have known their security systems were insufficient to protect the PII that is coveted by thieves worldwide. Defendant also failed to observe industry standard information security practices.

218. As a direct and proximate cause of Defendant's conduct, Plaintiffs and Class members suffered damages as alleged above.

COUNT V
Unjust Enrichment / Quasi Contract
(On Behalf of Plaintiff and the Class)

219. Plaintiff restates and realleges all of the allegations stated above as if fully set forth herein.

220. Plaintiff and Class Members conferred a monetary benefit on Defendant, by providing Defendant with their valuable PII. In conferring this benefit, Plaintiff and Class Members understood that part of the benefit Defendant derived from the PII would be applied to data security efforts to safeguard the PII.

221. Defendant appreciated that Plaintiff and Class Members were conferring a benefit upon it and accepted that monetary benefit.

222. Acceptance of the benefit under the facts and circumstances described herein make it inequitable for Defendant to retain that benefit without payment of the value thereof. Specifically, Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid their data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

223. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

224. Defendant acquired the monetary benefit and PII through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

225. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

226. Plaintiff and Class Members have no adequate remedy at law.

227. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII in their continued possession and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

228. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

229. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them.

COUNT VI
Declaratory Judgment
(On Behalf of Plaintiff and the Class)

230. Plaintiff restates and realleges all of the allegations stated above as if fully set forth herein.

231. This cause of action is brought under N.C. Gen. Stat. § 1-253. This Court is

authorized to declare rights, status, and other legal relations, and such declarations shall have the force and effect of a final judgment or decree. Furthermore, the Court has broad authority to restrain acts, such as those here, that are tortious as described in this Complaint.

232. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' PII and whether Defendant are currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their PII. Plaintiff alleges that Defendant's data security measures remain inadequate, contrary to its assertion that it has confirmed the security of its network and its systems.

233. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of PII, and there is a present and continuing risk that further compromises will occur in the future.

234. This Court should enter a judgment declaring, among other things, the following:

- a. Defendant owes a legal duty to secure PII and to timely notify those affected of the Data Breach; and
- b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure PII.

235. This Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect PII.

236. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach. The risk of another such breach is real, immediate, and substantial. If another breach occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

237. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Plaintiff will likely be subjected to substantial

identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures and communicating those measures to the Class is relatively minimal, and it has a pre-existing legal obligation to employ such measures.

238. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the additional injuries that would result to Plaintiff and to those whose PII would be further compromised.

239. Plaintiff and the Class, therefore, seek a declaration (1) that Defendant's existing security measures do not comply with their contractual obligations and duties of care to provide adequate security, and (2) that to comply with their obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to, the following:

- a. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
- b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;
- c. Ordering that Defendant audit, test, and train their security personnel regarding any new or modified procedures;
- d. Ordering that Defendant segment PII data by, among other things, creating firewalls and access controls so that if one area of Defendant's system is compromised, hackers cannot gain access to other portions of Defendant's systems;
- e. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner all data not necessary for its provisions of services;
- f. Ordering that Defendant conduct regular computer system scanning and security checks;
- g. Ordering that Defendant routinely and continually conduct internal training and

education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

- h. Ordering Defendant to meaningfully educate employees and members about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

- A. For an Order certifying this action as a class action and appointing Plaintiff and his counsel to represent the Class;
- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;
- C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Data Breach;
- D. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:
 - i. Prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
 - ii. Requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

- iii. Requiring Defendant to delete, destroy, and purge the PII of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;
- iv. Requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;
- v. Prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;
- vi. Requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
- vii. Requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;
- viii. Requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;
- ix. Requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

- x. Requiring Defendant to conduct regular database scanning and securing checks;
- xi. Requiring Defendant to establish an information security training program that includes at least annual information security training for all patients, with additional training to be provided as appropriate based upon the patients' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;
- xii. Requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
- xiii. Requiring Defendant to implement a system of tests to assess its respective patients' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing patients' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;
- xiv. Requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

- xv. Requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves; and
 - xvi. Requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and
 - xvii. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the Class, and to report any deficiencies with compliance of the Court's final judgment.
- E. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;
 - F. Ordering Defendant to pay for not less than ten years of credit monitoring services for Plaintiff and the Class;
 - G. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;
 - H. For an award of punitive damages, as allowable by law;
 - I. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;
 - J. Pre- and post-judgment interest on any amounts awarded; and
 - K. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: April 17, 2024

Respectfully submitted,

/s/ Scott Harris

Scott Harris
N.C. Bar No.: 35328
**MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC**
900 W. Morgan Street
Raleigh, North Carolina 27603
Tel.: 919-600-5003
Fax: 919-600-5035
sharris@milberg.com

Gary M. Klinger*
**MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN LLC**
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (866) 252-0878
gklinger@milberg.com

Andrew J. Shamis*
SHAMIS & GENTILE P.A.
14 NE 1st Ave., Suite 705
Miami, Florida 33132
Tel: (305) 479-2299
ashamis@shamisgentile.com

**KOPELOWITZ OSTROW
FERGUSON WEISELBERG GILBERT**
Jeff Ostrow*
Ken Grunfeld
Kristen Lake Cardoso*
Steven Sukert*
One West Las Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Tel: (954) 525-4100
ostrow@kolawyers.com
grunfeld@kolawyers.com
cardoso@kolawyers.com
sukert@kolawyers.com

*Attorney for Plaintiff and
the Proposed Class*

**Pro Hac Vice* application forthcoming

Exhibit A




Nucor Corporation
1915 Rexford Road
Charlotte, NC 28211



June 30, 2023

005007

Christopher Burleson


RE: Notice of Data Breach

Dear Christopher,

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.

Step 4

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 **331745690537** 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.

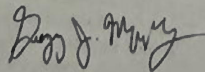
What You Can Do. In addition to enrolling in Equifax's Complete™ Premier service, we recommend that you:

- 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 1-844-568-3083 weekdays 9 am to 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

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Nucor Corporation Settlement Resolves Lawsuit Over 2023 Cyberattack](#)
