IN THE COURT OF COMMON PLEAS
MEDINA COUNTY, OHIO

JAMES FELGER
138 Idelwood Drive
Van Wert, Ohio 45891

and

WILLIAM HUDSON
380 Pinehurst Drive
Marshall TX 75670

individually and on behalf of all others similarly situated,

Plaintiffs,

v.

THE CORNWELL QUALITY TOOLS COMPANY
667 Seville Road
Wadsworth, OH 44281

Defendant.

Case No.: 2025CIV0456

Judge JOYCE V. KIMBLER, JUDGE

CLASS ACTION COMPLAINT

JURY DEMAND ENDORSED HEREON

Plaintiffs James Felger and William Hudson, individually and on behalf of all others similarly situated, bring this action against Defendant The Cornwell Quality Tools Company ("Cornwell") based on personal knowledge and the investigation of counsel, and for their Class Action Complaint allege as follows:

I. INTRODUCTION

1. On September 22, 2022, an unknown actor gained access to Defendant's inadequately-protected computer systems. As a result, Plaintiffs and Class Members (as defined below) have had their personal identifiable information ("PII")[1] exposed (the "Data Breach").

[1] Personal identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal

2. Cornwell manufactures tools for automotive and aviation industries.

3. Plaintiffs and members of the class purchased tools from Cornwell.

4. In carrying out its business, Defendant obtains, collects, uses, and derives a benefit from the PII of Plaintiffs and the Class. As such, Defendant assumed the legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

5. On September 22, 2022, Defendant experienced a network disruption. Defendant launched an investigation into the disruption and, with the help of independent cybersecurity experts, determined that some of Defendant's files containing borrower-related information had been accessed or acquired by the unknown actor. Defendant concluded its investigation on August 23, 2023.

6. According to Defendant, the PII exposed in the Breach included names and Social Security numbers.

7. In late August 2023, Defendant began notifying Plaintiffs and Class Members of the Data Breach.

8. Due to Defendant's negligence, cybercriminals obtained all they need to commit identity theft and wreak havoc on the financial and personal lives of thousands of individuals.

9. This class action seeks to redress Defendant's unlawful, willful and wanton failure to protect the personal identifiable information of approximately 11,884 individuals that was exposed in a major data breach of Defendant's network in violation of its legal obligations.[2]

---

or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

[2] Office of the Me. Atty. Gen., *Data Breach Notifications, Cornwell Quality Tools*, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/03e9b627-f5fd-4940-be00-50e4201a8f26.shtml (last visited May 3, 2025).

10. For the rest of their lives, Plaintiffs and the Class Members will have to deal with the danger of identity thieves possessing and misusing their PII. Plaintiffs and Class Members will have to spend time responding to the Breach and are at an immediate, imminent, and heightened risk of all manners of identity theft as a direct and proximate result of the Data Breach. Plaintiffs and Class Members have incurred and/or will continue to incur damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damaged credit, deprivation of the value of their PII, loss of privacy, and/or additional damages as described below.

11. Defendant betrayed the trust of Plaintiffs and the other Class Members by failing to properly safeguard and protect their personal identifiable information and thereby enabling cybercriminals to steal such valuable and sensitive information.

12. Plaintiffs brings this action individually and on behalf of the Class, seeking remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, injunctive relief, reasonable attorney fees and costs, and all other remedies this Court deems proper.

II. THE PARTIES

13. Plaintiff James Felger is a citizen of Van Wert, Ohio.

14. Plaintiff William Hudson is a citizen of Marshall, Texas.

15. Cornwell is an Ohio corporation with its principal place of business located in Wadsworth, Medina County, Ohio.

16. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiffs. Plaintiffs will seek leave of court to amend this Complaint to reflect the

true names and capacities of such other responsible parties when their identities become known.

17. All of Plaintiffs' claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

18. The Court has subject matter jurisdiction over this action under R.C. 2305.01.

19. This Court has personal jurisdiction over Defendant because it is incorporated under Ohio law, its principal place of business is in Ohio, and the acts and omissions giving rise to Plaintiffs' claims occurred in this State.

20. Venue is proper in Medina County under Civ.R. 3(C)(2) because Defendant's principal place of business is in this county and because Defendant's activities giving rise to this action were conducted in this county.

IV. FACTUAL ALLEGATIONS

Background

21. Defendant required that Plaintiffs and Class Members provide their PII in order to do business with Defendant.

22. Plaintiffs and Class Members relied on this sophisticated Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members demand security to safeguard their PII.

23. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiffs and the Class Members from involuntary disclosure to third parties.

The Data Breach

24. On September 22, 2022, due to Defendant's failure to maintain an adequate security

system, an unknown hacker gained access to Defendant's systems and acquired certain files and information including Plaintiffs and Class Members' PII.

25. Defendant negligently delayed in responding to the notice and did not conclude its review of the attack until August 23, 2023.

26. In late August, Defendant sent Plaintiffs and Class Members a notice of the Data Breach ("Notice of Data Breach"). Attached hereto as Exhibit 1.

27. Defendant admitted in the Notice of Data Breach that an unauthorized actor accessed sensitive information about Plaintiffs and Class Members. *Id.*

28. The details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur have not been shared with regulators or Plaintiffs and Class Members, who retain a vested interest in ensuring that their information remains protected.

29. The unencrypted PII of Plaintiffs and Class Members may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can easily access the PII of Plaintiffs and Class Members.

30. Defendant was negligent and did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiffs and Class Members, causing the exposure of PII for Plaintiffs and Class Members.

31. Because Defendant had a duty to protect Plaintiffs' and Class Members' PII, Defendant should have known through readily available and accessible information about potential threats for the unauthorized exfiltration and misuse of such information.

32. In the years immediately preceding the Data Breach, Defendant knew or should

have known that Defendant's computer systems were a target for cybersecurity attacks because warnings were readily available and accessible via the internet.

33. In October 2019, the Federal Bureau of Investigation published online an article titled "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations" that, among other things, warned that "[a]lthough state and local governments have been particularly visible targets for ransomware attacks, ransomware actors have also targeted health care organizations, industrial companies, and the transportation sector."[3]

34. In April 2020, ZDNet reported, in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year," that "[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize damage, leak corporate information on dark web portals, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay."[4]

35. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that "[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."[5]

36. This readily available and accessible information confirms that, prior to the Data

[3] FBI, *High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations* (Oct. 2, 2019) (emphasis added), https://www.ic3.gov/PSA/2019/PSA191002 (last visited May 3, 2025).

[4] Catalin Cimpanu, *Ransomware mentioned in 1,000+ SEC filings over the past year*, ZDNet (Apr. 30, 2020), https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/ (emphasis added) (last visited May 3, 2025).

[5] U.S. Cybersecurity & Infrastructure Sec. Agency ("CISA"), *Ransomware Guide* (Sept. 2020), https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf (last visited May 3, 2025).

Breach, Defendant knew or should have known that: (i) cybercriminals were targeting big companies such as Defendant, (ii) cybercriminals were ferociously aggressive in their pursuit of companies in possession of significant sensitive information such as Defendant, (iii) cybercriminals were leaking corporate information on dark web portals, and (iv) cybercriminals' tactics included threatening to release stolen data.

37. Considering the information readily available and accessible on the internet before the Data Breach, Defendant, having elected to store the unencrypted PII of Plaintiffs and Class Members in an Internet-accessible environment, had reason to be on guard for the exfiltration of the PII, and Defendant's type of business had cause to be particularly on guard against such an attack.

38. Prior to the Data Breach, Defendant knew or should have known that there was a foreseeable risk that Plaintiffs' and Class Members' PII could be accessed, exfiltrated, and published as the result of a cyberattack.

39. Prior to the Data Breach, Defendant knew or should have known that it should have encrypted the Social Security numbers and other sensitive data elements within the PII to protect against their publication and misuse in the event of a cyberattack.

Defendant Acquires, Collects, and Stores the PII of Plaintiffs and Class Members

40. Defendant acquired, collected, and stored the PII of Plaintiffs and Class Members.

41. Plaintiffs and other Members of the Class entrusted their PII to Defendant.

42. By obtaining, collecting, and storing the PII of Plaintiffs and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII from disclosure.

43. Plaintiffs and Class Members have taken reasonable steps to maintain the

confidentiality of their PII and relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

44. 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."[6]

45. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, 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 (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.

[6] See U.S. Govt., *How to Protect Your Networks from RANSOMWARE*, at 3, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited May 3, 2025).

- 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.[7]

46. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks. . . .

- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net) . . . .

[7] *Id.* at 3-4.

- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it. . . .

- **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic. . . .[8]

47. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, 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 privilege credentials

Thoroughly investigate and remediate alerts
- Prioritize and treat commodity malware infections as potential full comprise

Include IT Pros in security discussions
- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely

[8] *See* CISA, *Protecting Against Ransomware* (Apr. 11, 2019, rev. Sept. 2, 2021), https://www.cisa.gov/news-events/news/protecting-against-ransomware (last visited May 3, 2025).

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]

48. Given that Defendant was storing the PII of other individuals, Defendant could and should have implemented all of the above measures to prevent and detect ransomware attacks.

49. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the PII of Plaintiffs and Class Members.

Securing PII and Preventing Breaches

50. Defendant could have prevented this Data Breach by properly securing and encrypting the folders, files, and or data fields containing the PII of Plaintiffs and Class Members. Alternatively, Defendant could have destroyed the data it no longer had a reasonable need to maintain or only stored data in an Internet-accessible environment when there was a reasonable need to do so.

[9] *See* Microsoft Threat Intelligence, *Human-operated ransomware attacks: A preventable disaster* (Mar. 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited May 3, 2025).

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

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

53. The ramifications of Defendant's failure to keep secure the PII of Plaintiffs and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Defendant's Response to the Data Breach is Inadequate

54. Defendant was negligent and failed to inform Plaintiffs and the Class Members of the Data Breach in time for them to protect themselves from identity theft.

55. Defendant admitted that it learned of the data breach as early as September 22, 2022. Yet, Defendant did not start notifying affected individuals until late August.

56. During these intervals, the cybercriminals have had the opportunity to exploit the Plaintiffs and the Class Member's PII while Defendant was secretly investigating the Data Breach.

Value of PII

57. 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 identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[10] Experian reports that a stolen credit or

[10] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed May 3, 2025).

debit card number can sell for $5 to $110 on the dark web.[11] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[12]

58. 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.

59. 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 and Social Security numbers are worth more than 10x on the black market."[13]

60. 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.

61. One such example of criminals using PII for profit is the development of "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. These dossiers are known as "Fullz" packages.

---

[11] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed May 3, 2025).

[12] VPNOverview, *In the Dark* (2019), https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed May 3, 2025).

[13] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Network World (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed May 3, 2025).

62. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiffs' and the Class' 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 stolen by the cyber-criminals in the Data Breach, criminals can 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.

63. That is exactly what is happening to Plaintiffs and members of the Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs' and the Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

Plaintiffs' Experiences

Plaintiff James Felger

64. Plaintiff Felger was required to provide and did provide his PII to Defendant during the courts of his employment with Defendant. The PII included his name and Social Security number.

65. Plaintiff received a Notice Letter from The Cornwell Quality Tools Company, dated August 29, 2023, on or about that date. The Notice Letter informed Plaintiff that on September 22, 2022, Cornwell Quality Tools identified unusual activity on its network and subsequently learned that certain systems may have been accessed without authorization and Mr. Felger's personal information including his name and Social Security number were involved. The letter further advised that Plaintiff that he could participate in credit monitoring services detecting suspicious activity.

66. To date, Cornwell Quality Tools has done next to nothing to adequately protect Plaintiff Felger and Class Members, or to compensate them for their injuries sustained in this Data Breach.

67. Defendant's data breach notice letter downplays the theft of Plaintiff's and Class Members PII, when the facts demonstrate that the PII was targeted, accessed, and exfiltrated in a criminal cyberattack. The fraud and identity monitoring services offered by Defendant are only for 12 months, and it places the burden squarely on Plaintiff Felger and Class Members by requiring them to expend time signing up for the service and addressing timely issues.

68. Plaintiff Felger and Class Members have been further damaged by the compromise of their PII.

69. Plaintiff Felger PII was compromised in the Data Breach and was likely stolen and in the hands of cybercriminals who illegally accessed Cornwell Quality Tools' network for the specific purpose of targeting the PII.

70. Plaintiff Felger typically takes measures to protect his PII, and is very careful about sharing his PII Felger has never knowingly transmitted unencrypted PII over the internet or other unsecured source.

71. Plaintiff Felger stores any documents containing his PII in a safe and secure location, and he diligently chooses unique usernames and passwords for his online accounts.

72. As a result of the Data Breach, Plaintiff has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to this Data Breach. He monitors accounts and credit scores and has sustained emotional distress. This is time that was lost and unproductive and took away from other activities and duties.

73. Plaintiff also suffered actual injury in the form of damages to and diminution in the

value of his PII—a form of intangible property that he entrusted to Defendant for the purpose of obtaining employment from Defendant, which was compromised in and as a result of the Data Breach.

74. Plaintiff Felger suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

75. Plaintiff Felger has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially his Social Security number, being placed in the hands of criminals.

76. Defendant obtained and continues to maintain Plaintiff's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure. Defendant required the PII from Plaintiff when he began employment with Defendant. Plaintiff, however, would not have entrusted his PII to Defendant had he known that it would fail to maintain adequate data security. Plaintiff Felger's PII was compromised and disclosed as a result of the Data Breach.

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

Plaintiff Hudson

78. Plaintiff Hudson purchased tools from Cornwell. In order to do business with Defendant, Cornwell required that Plaintiff Hudson provide his PII.

79. Plaintiff Hudson received Defendant's Notice of Data Breach dated August 23, 2023. The Notice stated that Plaintiff Hudson's PII, including his Social Security number, was impacted by the Data Breach.

80. As a result of the Data Breach, Plaintiff Hudson's sensitive information may have been accessed and/or acquired by an unauthorized actor. The confidentiality of Plaintiff Hudson's sensitive information has been irreparably harmed. For the rest of his life, Plaintiff Hudson will have to worry about when and how his sensitive information may be shared or used to his detriment

81. As a result of the Data Breach, Plaintiff Hudson spent time dealing with the consequences of the Data Breach, which includes times spent verifying the legitimacy of the Notice of Data Breach and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

82. Additionally, Plaintiff Hudson is very careful about not sharing his sensitive PII. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

83. Plaintiff Hudson stores any documents containing his sensitive PII in safe and secure locations or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

84. Plaintiff Hudson suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and experiences fear and anxiety and increased concern for the loss of his privacy.

85. Plaintiff Hudson has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially his Social Security number, being in the hands of unauthorized third parties and possibly criminals.

86. Plaintiff Hudson 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.

Plaintiffs and the Class Face Significant Risk of Continued Identity Theft

87. Plaintiffs and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

88. Defendant negligently disclosed the PII of Plaintiffs and the Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiffs and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

89. As a result of Defendant's negligence and failure to prevent the Data Breach, Plaintiffs and the Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spend researching how to prevent, detect, contest, and recover form identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII in their possession.

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

91. 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 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.[14]

92. Defendant's negligence and failure to properly notify Plaintiffs and members of the Class of the Data Breach exacerbated Plaintiffs' and the Class's injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach

93. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Classes are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

94. Defendant was, or should have been, fully aware of the unique type and the significant volume of data contained in Defendant's database, amounting to potentially thousands

[14] GAO, *Report to Congressional Requesters*, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf (last accessed May 3, 2025).

of individuals' detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

95. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members, including Social Security numbers, 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 Plaintiffs and Class Members as a result of a breach.

96. To date, Defendant has offered Plaintiffs and some Class Members only twelve (12) months of credit monitoring services. The offered service is inadequate to protect Plaintiffs and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

97. The injuries to Plaintiffs and Class Members are directly and proximately caused by Defendant's negligence and failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

Defendant Failed to Adhere to FTC Guidelines

98. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII.

99. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[15] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other

[15] 17 C.F.R. § 248.201 (2013).

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."[16]

100. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. Protect the sensitive consumer information that they keep;

b. Properly dispose of PII that is no longer needed;

c. Encrypt information stored on computer networks;

d. Understand their network's vulnerabilities; and

e. Implement policies to correct security problems.

101. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

102. The FTC recommends that companies not maintain information 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 for suspicious activity on the network; and verify that third-party service providers have reasonable security measures.

103. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, 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 Section 5 of the Federal Trade Commission Act ("FTC Act"),

[16] *Id.*

15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

104. Defendant's negligence and failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs and the Class's PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

V. CLASS ACTION ALLEGATIONS

105. Plaintiffs bring this nationwide class action on behalf of herself and on behalf of all others similarly situated pursuant to Civ.R. 23.

106. The Class that Plaintiffs seek to represent is defined as follows:

> All individuals whose PII was accessed and/or acquired in the ransomware attack that is the subject of the Notice of Data Breach that Defendant sent to Plaintiffs and Class Members on or around August 23, 2023 (the "Class").

107. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

108. Plaintiffs reserve the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

109. **Numerosity:** The Class is so numerous that joinder of all members is impracticable. Defendant reported to the Maine Attorney General that 11,884 individuals were impacted by the Data Breach.

110. **Commonality:** Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiffs and Class Members;

b. Whether Defendant had duties not to disclose the PII of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendant had duties not to use the PII of Plaintiffs and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the PII of Plaintiffs and Class Members;

e. When Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their PII had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practice by failing to safeguard the PII of Plaintiffs and Class Members;

k. Whether Plaintiffs and Class Members are entitled to actual, consequential,

and/or nominal damages as a result of Defendant's wrongful conduct;

l. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

m. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and ongoing harm faced as a result of the Data Breach.

111. **Typicality:** Plaintiffs' claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendant's misfeasance.

112. **Policies Generally Applicable to the Class:** This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

113. **Adequacy:** Plaintiffs will fairly and adequately represent and protect the interests of Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiffs has retained counsel experienced in complex class action litigation, and Plaintiffs intends to prosecute this action vigorously.

114. **Superiority and Manageability:** The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will

permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

115. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members 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 Plaintiffs 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.

116. 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.

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

118. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

119. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to Class Members as a whole is appropriate.

120. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendant adequately and accurately informed Plaintiffs and Class Members that their PII had been compromised;

e. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

f. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class Members; and,

g. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

VI. CAUSES OF ACTION

COUNT I – NEGLIGENCE
(On Behalf of Plaintiffs and the Class)

121. Plaintiffs incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

122. Defendant solicited, gathered, and stored the PII Plaintiffs and the Class as part of the operation of its business.

123. Upon accepting and storing the PII of Plaintiffs and Class Members, Defendant undertook and owed a duty to Plaintiffs and Class Members to exercise reasonable care to secure and safeguard that information and to use secure methods to do so.

124. Defendant had full knowledge of the sensitivity of the PII, the types of harm that Plaintiffs and Class members could and would suffer if the PII was wrongfully disclosed, and the importance of adequate security.

125. Plaintiffs and Class members were the foreseeable victims of any inadequate safety and security practices. Plaintiffs and the Class members had no ability to protect their PII that was in Defendant's possession. As such, a special relationship existed between Defendant and Plaintiffs and the Class.

126. Defendant was well aware of the fact that cyber criminals routinely target large corporations through cyberattacks in an attempt to steal sensitive PII.

127. Defendant owed Plaintiffs and the Class members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiffs and the Class when

obtaining, storing, using, and managing personal information, including taking action to reasonably safeguard such data.

128. Defendant's duty extended to protecting Plaintiffs 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 also have recognized the existence of a specific duty to reasonably safeguard personal information.

129. Defendant had duties to protect and safeguard the PII of Plaintiffs and the Class from being vulnerable to cyberattacks by taking common-sense precautions when dealing with sensitive PII. Additional duties that Defendant owed Plaintiffs and the Class include:

a. To exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant's networks, systems, protocols, policies, procedures and practices to ensure that Plaintiffs' and Class Members' PII was adequately secured from impermissible access, viewing, release, disclosure, and publication;

b. To protect Plaintiffs' and Class Members' PII in its possession by using reasonable and adequate security procedures and systems;

c. To implement processes to quickly detect a data breach, security incident, or intrusion involving their networks and servers; and

d. To promptly notify Plaintiffs and Class Members of any data breach, security incident, or intrusion that affected or may have affected their PII.

130. Defendant was the only one who could ensure that its systems and protocols were

sufficient to protect the PII that Plaintiffs and the Class had entrusted to it.

131. Defendant breached its duties of care by failing to adequately protect Plaintiffs' and Class Members' PII. Defendant breached its duties by, among other things:

a. Failing to exercise reasonable care in obtaining, retaining securing, safeguarding, deleting, and protecting the PII in its possession;

b. Failing to protect the PII in its possession using reasonable and adequate security procedures and systems;

c. Failing to adequately train its employees to not store PII longer than absolutely necessary;

d. Failing to consistently enforce security policies aimed at protecting Plaintiffs' and the Class's PII; and

e. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions.

132. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

133. As a proximate and foreseeable result of Defendant's negligent and/or grossly negligent conduct, Plaintiffs and the Class have suffered damages and are at imminent risk of additional harms and damages.

134. Through Defendant's acts and omissions described herein, including but not limited to Defendant's failure to protect the PII of Plaintiffs and Class Members from being stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the PII of Plaintiffs and Class Members while it was within Defendant's possession and control.

135. As a result of the Data Breach, Plaintiffs and Class Members have spent time, effort, and money to mitigate the actual and potential impact of the Data Breach on their lives, including but not limited to, closely reviewing and monitoring bank accounts, credit reports, and statements sent from providers and their insurance companies and the payment for credit monitoring and identity theft prevention services.

136. Defendant's wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence.

137. The damages Plaintiffs and the Class have suffered and will suffer were and are the direct and proximate result of Defendant's negligent and/or grossly negligent conduct.

COUNT II – NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs and the Class)

138. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

139. In addition to its duties under common law, Defendant had additional duties imposed by statute and regulations, including the duties the FTC Act. The harms which occurred as a result of Defendant's failure to observe these duties, including the loss of privacy and significant risk of identity theft, are the types of harm that these statutes and their regulations were intended to prevent.

140. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs and Class Members' PII.

141. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders

also form part of the basis of Defendant's duty in this regard.

142. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect consumers 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 a data breach including, specifically, the damages that would result to Plaintiffs and Class Members.

143. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se* as Defendant's violation of the FTC Act establishes the duty and breach elements of negligence.

144. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

145. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. 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 Plaintiffs and the Class.

146. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

147. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet their duties, and that Defendant's breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their PII.

148. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

COUNT III – INVASION OF PRIVACY
(On Behalf of Plaintiffs and the Class)

149. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

150. Plaintiffs and Class Members had a legitimate expectation of privacy regarding their PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

151. Defendant owed a duty to Plaintiffs and Class Member to keep their PII confidential.

152. Defendant affirmatively and recklessly disclosed Plaintiffs and Class Members' PII to unauthorized third parties.

153. The unauthorized disclosure and/or acquisition (i.e., theft) by a third party of Plaintiffs and Class Members' PII is highly offensive to a reasonable person.

154. Defendant's reckless failure to protect Plaintiffs and Class Members' PII constitutes an intentional interference with Plaintiffs and the Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

155. In failing to protect Plaintiffs and Class Members' PII, Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

156. Because Defendant failed to properly safeguard Plaintiffs and Class Members' PII, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and the Class.

157. Defendant knowingly did not notify Plaintiffs and Class Members in a timely fashion about the Data Breach.

158. As a proximate result of Defendant's acts and omissions, Plaintiffs and the Class Members' private and sensitive PII was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class to suffer damages.

159. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their PII are still maintained by Defendant with their inadequate cybersecurity system and policies.

160. Plaintiffs and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard Plaintiffs and the Class's PII.

161. Plaintiffs, on behalf of herself and Class Members, seeks injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiffs and Class Members' PII.

162. Plaintiffs, on behalf of herself and Class Members, seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

COUNT IV – BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Class)

163. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

164. By requiring Plaintiffs and the Class Members PII to do business with and purchases tools from Defendant, Defendant entered into an implied contract in which Defendant agreed to comply with its statutory and common law duties to protect Plaintiffs and Class Members' PII. In return, Defendant provided goods to Plaintiffs and the Class.

165. Based on this implicit understanding, Plaintiffs and the Class accepted Defendant's offers and provided Defendant with their PII.

166. Plaintiffs and Class members would not have provided their PII to Defendant had they known that Defendant would not safeguard their PII, as promised.

167. Plaintiffs and Class members fully performed their obligations under the implied contracts with Defendant.

168. Defendant breached the implied contracts by failing to safeguard Plaintiffs and Class Members' PII.

169. Defendant also breached the implied contracts when it engaged in acts and/or omissions that are declared unfair trade practices by the FTC. These acts and omissions included (i) representing, either expressly or impliedly, that it would maintain adequate data privacy and security practices and procedures to safeguard the PII from unauthorized disclosures, releases, data breaches, and theft; (ii) omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for the Class's PII; and (iii) failing to disclose to Plaintiffs and the Class at the time they provided their PII that Defendant's data security system and protocols failed to meet applicable legal and industry standards.

170. The losses and damages Plaintiffs and Class members sustained were the direct and proximate result of Defendant's breach of the implied contract with Plaintiffs and Class Members.

COUNT V – BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiffs and the Class)

171. Plaintiffs incorporate by reference all preceding factual allegations as though fully alleged herein.

172. A relationship existed between Plaintiffs and Class Members and Defendant in which Plaintiffs and the Class put their trust in Defendant to protect their PII. Defendant accepted this duty and obligation when it received Plaintiffs and the Class Members' PII.

173. Plaintiffs and the Class Members entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and refrain from disclosing their PII to unauthorized third parties.

174. Defendant knew or should have known that the failure to exercise due care in the collecting, storing, and using of individual's PII involved an unreasonable risk of harm to Plaintiffs and the Class, including harm that foreseeably could occur through the criminal acts of a third party.

175. Defendant's fiduciary duty required it to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that Plaintiffs and the Class's information in Defendant's possession was adequately secured and protected.

176. Defendant also had a fiduciary duty to have procedures in place to detect and prevent improper access and misuse of Plaintiffs' and the Class's PII. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiffs and the Class. That special relationship arose because Defendant was entrusted with Plaintiffs and the Class's PII.

177. Defendant breached its fiduciary duty that it owed Plaintiffs and the Class by failing to case in good faith, fairness, and honesty; by failing to act with the highest and finest loyalty; and by failing to protect the PII of Plaintiffs and the Class Members.

178. Defendant's breach of fiduciary duties was a legal cause of damages to Plaintiffs and the Class.

179. But for Defendant's breach of fiduciary duty, the damage to Plaintiffs and the Class would not have occurred, and the Data Breach contributed substantially to producing the damage to Plaintiffs and the Class.

180. As a direct and proximate result of Defendant's breach of fiduciary duty, Plaintiffs and the Class are entitled to actual, consequential, and nominal damages and injunctive relief, with amounts to be determined at trial.

COUNT VI – DECLARTORY JUDGMENT
(On Behalf of Plaintiffs and the Class)

181. Plaintiffs incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

182. Under the Declaratory Judgment Act, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Further, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

183. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and the Class's PII and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and the Class from further data breaches that compromise their PII. Plaintiffs alleges that Defendant's data security measures remain inadequate. Defendant publicly denies these allegations. Furthermore, Plaintiffs continues to suffer injury as a result of the

compromise of her PII and remains at imminent risk that further compromises of their PII will occur in the future. It is unknown what specific measures and changes Defendant has undertaken in response to the Data Breach.

184. Plaintiffs and the Class have an ongoing, actionable dispute arising out of Defendant's inadequate security measures, including (i) Defendant's failure to encrypt Plaintiffs' and the Class's PII, including Social Security numbers, while storing it in an Internet-accessible environment, and (ii) Defendant's failure to delete PII it has no reasonable need to maintain in an Internet-accessible environment, including the Social Security numbers of Plaintiffs and the Class.

185. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owes a legal duty to secure the PII of Plaintiffs and the Class;

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII; and

c. Defendant's ongoing breaches of its legal duty continue to cause Plaintiffs and the Class harm.

186. This Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry and government regulatory standards to protect consumers' PII. Specifically, this injunction should, among other things, direct Defendant to:

a. engage third party auditors, consistent with industry standards, to test its systems for weakness and upgrade any such weakness found;

b. audit, test, and train its data security personnel regarding any new or modified procedures and how to respond to a data breach;

c. regularly test its systems for security vulnerabilities, consistent with industry standards;

d. implement an education and training program for appropriate employees regarding cybersecurity.

187. If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendant. The risk of another such breach is real, immediate, and substantial. If another breach at Defendant occurs, Plaintiffs 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.

188. The hardship to Plaintiffs and Class Members if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiffs 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 is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

189. 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 at Defendant, thus eliminating the additional injuries that would result to Plaintiffs and others whose confidential information would be further compromised.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs and the Class pray for judgment against Defendant as follows:

a. An order certifying this action as a class action under Civ.R. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are a

proper representative of the Class requested herein;

b. A judgment in favor of Plaintiffs and the Class awarding them damages in excess of $25,000, including actual and statutory damages, punitive damages, attorneys' fees, expenses, costs, and such other and further relief as is just and proper;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class and the general public as requested herein, including, but not limited to:

i. 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;

ii. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

iii. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

iv. Ordering that Defendant segment customer data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

v. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner customer data not necessary for their provisions of services;

vi. Ordering that Defendant conduct regular database scanning and securing checks; and

vii. 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.

d. An order requiring Defendant to pay the costs involved in notifying the Class members about the judgment and administering the claims process;

e. A judgment in favor of Plaintiffs and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and

f. An award of such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all issues so triable.

Dated: May 2, 2025

Respectfully submitted,

/s/ Dylan J. Gould

Dylan J. Gould (0097954)
MARKOVITS, STOCK & DE MARCO, LLC
119 East Court Street, Ste. 530
Cincinnati, OH 45202
(513) 651-3700
dgould@msdlegal.com

William B. Federman (*pro hac vice* forthcoming)
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
Telephone: (405)235-1560
wbf@federmanlaw.com

Philip J. Krzeski (0095713)
CHESTNUT CAMBRONNE
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401-2138
Phone: (612) 339-7300
pkrzeski@chestnutcambronne.com

Counsel for Plaintiffs and the Putative Class