IN THE UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF OKLAHOMA

Wyteria Trimble, Stefanie Garcia, and Olivia Georgiady, individually and on behalf of all others similarly situated, Plaintiffs, v. Paycom Payroll, LLC, Defendant.	Case No.: CIV-24-154-D **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Wyteria Trimble, Stefanie Garcia, and Olivia Georgiady, individually and on behalf of all others similarly situated, for their Class Action Complaint, bring this action against Defendant Paycom Payroll, LLC ("Paycom") based on personal knowledge and the investigation of counsel and allege as follows:

I. INTRODUCTION

1. As early as April 2023, unknown actor(s) gained access to Defendant's inadequately protected computer systems, found their way to Paycom's consumers' accounts, and stole thousands of dollars from Paycom's customers by re-routing consumers' direct deposits to unknown accounts. As a result, Plaintiffs and the Class Members (as further defined below) have had their personal identifiable information ("PII")[1] exposed and direct deposit paychecks stolen (the "Data Breach"). Upon information and belief, these unknown persons still have access to Paycom's network.

[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 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. Paycom is an online payroll and human resource technology company servicing thousands of employers throughout the United States.

3. Plaintiffs and members of the Class are persons who received payroll or human resource services through Paycom or otherwise had a Paycom account whereby they received direct deposits from their respective employers.

4. In carrying out its business, Defendant obtains, collects, uses, and derives a benefit from the PII of Plaintiffs and the Class including their names, Social Security numbers, addresses, email addresses, dates of birth, telephone numbers, account passwords, direct deposit information, and bank account information. Defendant also obtains a benefit from providing direct deposit services to employers and their employees. As such, Defendant assumed the legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

5. In May 2023, or earlier, Defendant began receiving reports from individuals informing Defendant that unknown persons were gaining access to their personal Paycom accounts and re-routing their direct deposits to accounts of the unknown persons. *See* Paycom Email, attached as **Exhibit 1**.

6. The unknown persons gained access to Paycom's consumers' accounts, stole thousands of dollars from Paycom's consumers by re-routing consumers' direct deposits, and accessed the PII stored on the consumers' accounts.

7. Despite this, Paycom has failed to notify Plaintiffs and the Class Members of the Data Breach.

8. Rather, Plaintiffs and the Class Members didn't discover the breach until it was too late and unknown persons had already stolen their hard-earned paychecks.

9. Due to Defendant's negligence, cybercriminals obtained everything they need to commit identity theft and continue wreaking havoc on the financial and personal lives of thousands of individuals.

10. This class action seeks to redress Defendant's unlawful, willful and wanton failure to protect the personal identifiable information of likely thousands of individuals that was exposed in a major data breach of Defendant's network and its failure to safeguard Plaintiffs and the Class Members' direct deposits, in violation of its legal obligations.

11. As a result of Defendant's failure to adequately protect its network and consumers' accounts, unknown persons have stolen thousands of dollars from Plaintiffs and the Class Members.

12. 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.

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

14. Plaintiffs bring 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

15. Plaintiff Wyteria Trimble is a resident of Birmingham, AL.

16. Plaintiff Stephanie Garcia is a resident of Corpus Christi, Texas.

17. Plaintiff Olivia Georgiady is a resident of Lebanon, Ohio.

18. Paycom Payroll, LLC is a Delaware limited liability company registered in the State of Oklahoma with the Oklahoma Secretary of State. Paycom's corporate headquarters are located at 7501 W. Memorial Road, Oklahoma City, OK 73142.

19. 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.

20. 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

21. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs; there are more than 100 members in the proposed class; and at least one Class Member, including Plaintiff, is a citizen of a state different from Defendant to establish minimal diversity.

22. Defendant is a citizen of Oklahoma because its principal place of business is in Oklahoma City, Oklahoma.

23. The Western District of Oklahoma has personal jurisdiction over Defendant because it conducts substantial business in Oklahoma and in this District and collected and/or stored the PII of Plaintiff and the Class Members in this District.

24. Venue is in this District under 28 U.S.C. § 1391(b) because Defendant operates in this District and a substantial part of the events or omissions giving rise to Plaintiffs and the Class Members' claims occurred in this District, including Defendant collecting and/or storing the PII of Plaintiffs and the Class Members.

IV. FACTUAL ALLEGATIONS

Background

25. Defendant required that Plaintiffs and Class Members provide their PII and set up an online accessible account on Paycom's system in order to receive payroll and human resource services, including direct deposit services.

26. Plaintiffs and Class Members relied on this sophisticated Defendant to keep their PII and personal online accounts 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 and direct deposits.

27. Defendant had a duty to adopt reasonable measures to protect the PII, personal online accounts, and direct deposits of Plaintiffs and the Class Members from involuntary disclosure to third parties.

The Data Breach

28. As early as April 2023, due to Defendant's failure to maintain an adequate security system, an unknown hacker gained access to Defendant's systems and acquired access to Plaintiffs

and the Class Members personal online accounts, including access to their PII, direct deposits, and financial account information.

29. Upon information and belief, the unknown person still has access to Defendant's network and continues to steal thousands of dollars from Paycom's consumers.

30. This Data Breach has gone beyond an unknown user merely gaining access to someone's username and password. Possibly hundreds of persons have had unknown users gain access to their online Paycom accounts and re-route direct deposits to unknown accounts. These users have never knowingly shared their account information with anyone, nor have they been victims of prior data breaches. Rather, the unknown users have gained access to Plaintiffs and the Class Members accounts by first gaining access to Paycom's network.

31. Despite being notified of the unknown hacker as early as May 2023, Defendant has failed to notify Plaintiffs and the Class Members of the Data Breach.

32. 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.

33. As a result, unknown persons have gained access to Plaintiffs and the Class Members' online Paycom accounts, exposed their PII, and re-routed direct deposits from Plaintiffs' and the Class Members' accounts to unknown accounts, stealing thousands of dollars from Plaintiffs and the Class.

34. In addition to the already thousands of dollars stolen, 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.

35. 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 Plaintiffs' and Class Members' PII and theft of thousands of dollars from re-routed direct deposits.

The Data Breach was Foreseeable

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

37. 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.

38. 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."[2]

39. 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

[2] FBI, High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations (Oct. 2, 2019) (emphasis added), *available at* https://www.ic3.gov/Media/Y2019/PSA191002 (last visited Jan. 25, 2022).

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."[3]

40. 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."[4]

41. In 2018, the Internal Revenue Service ("IRS") published warnings for professionals of a significant increase that involved payroll direct deposit and wire transfer scams.[5]

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

43. Considering the information was readily available and accessible on the internet before the Data Breach, Defendant, having elected to store the unencrypted PII of Plaintiff and

[3] ZDNet, Ransomware mentioned in 1,000+ SEC filings over the past year (Apr. 30, 2020) (emphasis added), available at https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/ (last visited Jan. 25, 2022).

[4] U.S. CISA, Ransomware Guide – September 2020, available at https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf (last visited Jan. 25, 2022).

[5] IRS, Security Summit Partners Warn Tax Professionals of Fake Payroll Direct Deposit and Wire Transfer Emails, IRS, (Dec. 17, 2018) https://www.irs.gov/newsroom/irs-security-summit-partners-warn-tax-professionals-of-fake-payroll-direct-deposit-and-wire-transfer-emails.

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.

44. 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.

45. Prior to the Data Breach, Defendant knew or should have known that its systems would be the target of a cyberattack. Defendant also knew that it had a duty to protect Plaintiffs' and the Class Members' PII and direct deposits.

46. Prior to the Data Breach, Defendant knew or should have known that there was a foreseeable risk that Plaintiffs' and the Class Members' direct deposits could be accessed, re-routed, and stolen as the result of a cyberattack.

47. Prior to the Data Breach, Defendant knew or should have known that it should have secured Plaintiffs' and the Class Members' direct deposits from a cyberattack by adding additional security measures, such as additional re-routing verifications.

48. On May 23, 2023, Defendant sent an email stating that it would implement an additional re-routing verification process, requiring an employer's human resource team to verify a re-routing request. However, Defendant failed to implement this verification requirement throughout the Class.

49. Defendant also should have required employees to verify re-routing requests.

50. 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.

Securing PII and Preventing Breaches

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

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

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

54. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII and ensure that they are receiving their hard-earned direct deposits. Plaintiffs and the Class Members 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. Plaintiffs and the Class Members relied on Defendant to keep their direct deposit information correct and accurate and prevent unauthorized users from gaining access to their personal Paycom accounts.

55. 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]

56. 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

[6] See 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 July 17, 2023).

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.

- 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]

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

57. 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). . . .

- **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]

58. 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

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]

---

[8] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://www.cisa.gov/news-events/news/protecting-against-ransomware (last visited July 17, 2023).

[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 July 17, 2023).

59. To prevent unauthorized persons from gaining access to Plaintiffs and the Class Members' personal Paycom accounts, Paycom should have implemented additional security measures such as multi-factor authentication or required multiple persons to confirm account changes, such as changes to direct deposit information.

60. Given that Defendant was storing the PII of other individuals and was responsible for maintaining Plaintiffs and the Class Members direct deposit information, Defendant could and should have implemented all of the above measures to prevent and detect ransomware attacks.

61. 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 and theft of thousands of dollars in direct deposits.

62. 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.

63. Defendant could have prevented the theft of thousands of dollars of direct deposits by requiring as multi-factor authentication or required multiple persons to confirm account changes, such as changes to direct deposit information.

64. 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.

65. 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.

66. 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 and failed to ensure that Plaintiffs' and the Class Members' direct deposits were sent to the appropriate persons.

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 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

68. Defendant was negligent and failed to inform Plaintiffs and the Class Members of the Data Breach so that they can protect themselves from identity theft and theft of their hard-earned direct deposits.

69. Defendant learned of the Data Breach and re-routing of direct deposits as early as May 2023. Yet, Defendant has failed to notify Plaintiffs and the Class Members.

70. Defendant did not send out warnings or otherwise adequately inform Plaintiffs and the Class Members that their direct deposits were at risk.

71. As result, Plaintiffs and the Class Members lost the opportunity to protect themselves from wage theft or the theft of their direct deposits.

72. As such, the cybercriminals continue to exploit the Plaintiffs' and the Class Members' PII and re-route their direct deposits.

73. Despite learning of the Data Breach and re-routing of direct deposits as early as May 2023, Defendant has failed to take additional steps and add additional security measures to ensure that Plaintiffs and the Class Members' PII is secure and that the direct deposits are not being fraudulently re-routed to unknown accounts.

Value of PII

74. 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 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]

75. 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.

76. 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]

---

[10] *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 July 17, 2023).

[11] *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 July17, 2023).

[12] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed July 17, 2023).

[13] Time 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 July 17, 2023).

77. 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.

78. One such example of criminals using PII for profit is the development of "Fullz" packages.

79. 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.

80. 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.

81. 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.

Plaintiff Trimble's Experience

82. Plaintiff Trimble's employer used Paycom's payroll services in employing and rendering payment to Plaintiff.

83. In order to receive employment benefits from Paycom, Paycom required that Plaintiff Trimble provide her PII and set up an online account on Paycom's system. Paycom also required that Plaintiff Trimble set up direct deposit information on her online account.

84. On or around April 30, 2023, an unknown user gained access to Plaintiff Trimble's online Paycom account and changed her direct deposit information, resulting in Plaintiff Trimble's April 2023 paycheck direct deposit being sent to an unknown account.

85. After she did not receive her April 2023 direct deposit, Plaintiff Trimble changed her Paycom account password.

86. Despite this, the unknown user gained access to Plaintiff Trimble's online Paycom account again on or around May 25th, June 5th, and June 18th and, again, changed Plaintiff Trimble's direct deposit information.

87. In addition to stealing Plaintiff Trimble's paychecks, the unknown user gained access to Plaintiff Trimble's PII on Paycom's network.

88. Since the Data Breach, Plaintiff Trimble's email account has been subscribed to hundreds of newsletters and subscriptions, for which she herself did not subscribe.

89. To her knowledge, Plaintiff Trimble's PII has never been involved in any other prior data breach.

90. As a result of the Data Breach, Plaintiff Trimble had $1,354.23 of her hard-earned money stolen.

91. As a result of the Data Breach, Plaintiff Trimble's sensitive PII may have been accessed and/or acquired by an unauthorized actor. The confidentiality of Plaintiff Trimble's sensitive information has been irreparably harmed. For the rests of her life, Plaintiff Trimble will

have to worry about when and how her sensitive information may be shared or used to her detriment.

92. As a result of the Data Breach, Plaintiff Trimble 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 her accounts. This time has been lost forever and cannot be recaptured.

93. Additionally, Plaintiff Trimble is very careful about not sharing her sensitive PII. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

94. Plaintiff stores any documents containing her sensitive PII in safe and secure locations or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

95. Plaintiff Trimble 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 her privacy.

96. Plaintiff Trimble has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of unauthorized third parties and possibly criminals.

97. Plaintiff Trimble has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Georgiady's Experience

98. Plaintiff Georgiady's employer used Paycom's payroll services in employing and rendering payment to Plaintiff.

99. In order to receive employment benefits from Paycom, Paycom required that Plaintiff Georgiady provide her PII and set up an online account on Paycom's system. Paycom also required that Plaintiff Georgiady set up direct deposit information on her online account.

100. On or around May 28, 2023, an unknown user gained access to Plaintiff Georgiady's online Paycom account and changed her direct deposit information, resulting in 90% of Plaintiff Georgiady's May and June 2023 paychecks direct deposit being sent to an unknown account.

101. Plaintiff Georgiady did not learn about the breach until June 24, 2023 when she saw that a large sum of her direct deposits were never deposited into her account.

102. Defendant never notified Plaintiff Georgiady that her account and PII had been breached.

103. In addition to stealing Plaintiff Georgiady's paychecks, the unknown user gained access to Plaintiff Georgiady's PII on Paycom's network.

104. To her knowledge, Plaintiff Georgiady's PII has never been involved in any other prior data breach.

105. As a result of the Data Breach, Plaintiff Georgiady had $1,394.07 of her hard-earned money stolen.

106. As a result of the Data Breach, Plaintiff Georgiady's sensitive PII may have been accessed and/or acquired by an unauthorized actor. The confidentiality of Plaintiff Georgiady's sensitive information has been irreparably harmed. For the rests of her life, Plaintiff Georgiady

will have to worry about when and how her sensitive information may be shared or used to her detriment.

107. As a result of the Data Breach, Plaintiff Georgiady 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 her accounts. This time has been lost forever and cannot be recaptured.

108. To date, Ms. Georgiady has never been contacted by Defendant regarding the Data Breach.

109. Additionally, Plaintiff Georgiady is very careful about not sharing her sensitive PII. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

110. Plaintiff stores any documents containing her sensitive PII in safe and secure locations or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

111. Plaintiff Georgiady 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 her privacy.

112. Plaintiff Georgiady has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of unauthorized third parties and possibly criminals.

113. Plaintiff Georgiady has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Garcia's Experience

114. Plaintiff Garcia's employer used Paycom's payroll services in employing and rendering payment to Plaintiff.

115. In order to receive employment benefits from Paycom, Paycom required that Plaintiff Garcia provide her PII and set up an online account on Paycom's system. Paycom also required that Plaintiff Garcia set up direct deposit information on her online account.

116. On or around May 17, 2023, approximately two days prior to the date Plaintiff Garcia was supposed to receive her direct deposit, an unknown person gained access to Plaintiff Garcia's Paycom account and changed her routing information, resulting in Plaintiff Garcia's direct deposit routing to an unknown account.

117. As a result, Plaintiff Garcia never received her May 19, 2023 paycheck.

118. Defendant never notified Plaintiff Garcia that her account and PII had been breached.

119. In addition to stealing Plaintiff Garcia's direct deposits, the unknown user gained access to Plaintiff Garcia's PII on Paycom's network.

120. To her knowledge, Plaintiff Garcia's PII has never been involved in any other prior data breach.

121. As a result of the Data Breach, Plaintiff Garcia had $1,534.06 of her hard-earned money stolen.

122. As a result of the Data Breach, Plaintiff Garcia's sensitive PII may have been accessed and/or acquired by an unauthorized actor. The confidentiality of Plaintiff Garcia's sensitive information has been irreparably harmed. For the rests of her life, Plaintiff Garcia will

have to worry about when and how her sensitive information may be shared or used to her detriment.

123. As a result of the Data Breach, Plaintiff Garcia 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 her accounts. This time has been lost forever and cannot be recaptured.

124. Additionally, Plaintiff Garcia is very careful about not sharing her sensitive PII. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

125. Plaintiff stores any documents containing her sensitive PII in safe and secure locations or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

126. Plaintiff Garcia 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 her privacy.

127. Plaintiff Garcia has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of unauthorized third parties and possibly criminals.

128. Plaintiff Garcia has a continuing interest in ensuring that her 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 Theft

129. Plaintiffs and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant, including unknown persons gaining access to their online Paycom accounts and redirecting their direct deposits to unknown accounts.

130. In allowing unknown users access to Plaintiffs' and the Class Members' online accounts, 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.

131. As a result of Defendant's negligence and failure to prevent the Data Breach and protect Plaintiffs' and the Class Members' online Paycom accounts, 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.

132. In addition to the already stolen direct deposits, further fraudulent activity resulting from this Data Breach may not come to light for years.

133. There may be a time lag between when additional harm and misuse of their PII 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]

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

135. 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.

[14] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last accessed July 17, 2023).

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

137. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members and their direct deposit information, 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.

138. 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

139. 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.

140. 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 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,

[15] 17 C.F.R. § 248.201 (2013).

alien registration number, government passport number, employer or taxpayer identification number."[16]

141. 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.

142. 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.

143. 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 implemented reasonable security measures.

144. 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.

145. Defendant's negligence and failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff 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

146. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rule 23(b)(2), (b)(3), and (c)(4) of the Federal Rules of Civil Procedure.

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

> All individuals whose Paycom accounts were accessed by unauthorized third parties between April 2023 to present (the "Class").

148. 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.

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

150. **Numerosity:** The Class is so numerous that joinder of all members is impracticable. It's estimated that hundreds of persons have had their PII exposed and their direct deposits re-routed.

151. **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 and to what extent Defendant had a duty to prevent unauthorized access to Plaintiffs and the Class Members online Paycom accounts;

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

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

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

f. When Defendant actually learned of the Data Breach;

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

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

i. 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;

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

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

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

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

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

152. **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.

153. **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.

154. **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 seek 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 have retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

155. **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.

156. 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 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.

157. 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.

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

159. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII and direct deposit information of the 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.

160. 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.

161. 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)

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

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

164. 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.

165. Defendant solicited, gathered, and stored the direct deposit information Plaintiffs and the Class as part of the operation of its business.

166. Upon accepting, storing, monitoring, and providing services around Plaintiffs' and the Class Members' direct deposit information, 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.

167. Defendant had full knowledge of the sensitivity of the PII and the direct deposits, the types of harm that Plaintiffs and Class Members could and would suffer if the PII was wrongfully disclosed or if the direct deposit information was impermissibly altered, and the importance of adequate security.

168. 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. Plaintiffs and the Class Members had limited to no ability to ensure that their direct deposit information remained accurate and untouched by cyber criminals. As such, a special relationship existed between Defendant and Plaintiffs and the Class.

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

170. 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.

171. 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.

172. Defendant had duties to protect and safeguard the PII and direct deposits of Plaintiffs and the Class from being vulnerable to cyberattacks by taking common-sense precautions when dealing with sensitive PII and direct deposits. 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 protect and secure Plaintiffs' and the Class Members' direct deposits by ensuring that the direct deposit and routing information is correct and accurate at all times;

d. To protect and secure Plaintiffs' and the Class Members' direct deposits by ensuring that all changes to direct deposit and routing information are verified and authorized;

e. To protect and secure Plaintiffs' and the Class Members' direct deposits by implementing reasonable measures to prevent unauthorized changes to direct deposit and routing information;

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

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

173. Defendant was the only one who could ensure that its systems and protocols were sufficient to protect the PII and direct deposits that Plaintiffs and the Class had entrusted to it.

174. Defendant breached its duties of care by failing to adequately protect Plaintiffs' and Class Members' PII and direct deposits. 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 exercise reasonable care in obtaining, securing, safeguarding, and protecting Plaintiffs' and the Class Members' direct deposits that were transferred through Defendant's system;

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

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

e. Failing to adequately train its employees to stop or otherwise detect direct deposit fraud or fraud on customers' accounts;

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

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

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

176. 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.

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

178. 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.

179. As a result of the Data Breach, Plaintiffs and the Class Members have had their hard-earned money stolen.

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

181. 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)

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

183. 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.

184. 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 Plaintiff and Class Members' PII.

185. 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.

186. 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.

187. 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.

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

189. 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.

190. 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.

191. 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.

192. 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 – BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Class)

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

194. By requiring Plaintiffs and the Class Members to provide their PII and obtain their direct deposits through Defendant's network, 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 and direct deposits. In return, Defendant provided goods to Plaintiffs and the Class.

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

196. Plaintiffs and Class members would not have provided their PII or direct deposit information to Defendant had they known that Defendant would not safeguard their PII or direct deposits, as promised.

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

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

199. 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 and direct deposits 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 direct deposits; and (iii) failing to disclose to Plaintiffs and the Class at the time they provided their PII and direct deposit information that Defendant's data security system and protocols failed to meet applicable legal and industry standards.

200. 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 IV – UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class)

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

202. This count is plead in the alternative to Count IV (Breach of Implied Contract).

203. Plaintiffs and the Class Members conferred a monetary benefit on Defendant by providing Defendant with their PII and direct deposit information.

204. Defendant enriched itself by saving the costs it reasonably should have expended on data and account security measures to secure Plaintiffs' and the Class Members' PII and direct deposits.

205. Defendant intentionally failed to inform Plaintiffs and the Class Members of the Data Breach known direct deposit fraud, thereby denying Plaintiffs and the Class Members an opportunity to protect themselves. Instead, Defendant enriched itself by saving the costs it reasonably should have expended by notifying Plaintiffs and the Class Members of the Data Breach and known fraudulent transactions.

206. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid its data and account security obligations at the expense of Plaintiffs and the Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and the Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

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

208. Defendant acquired the monetary benefit, PII, and direct deposit information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

209. If Plaintiffs and the Class Members knew that Defendant had not secured their PII and direct deposit information, they would not have agreed to provide their PII and direct deposit information to Defendant.

210. Plaintiffs and the Class Members have no adequate remedy at law.

211. As a direct and proximate result of Defendant's conduct, Plaintiffs and the Class Members have suffered and will suffer injury, including but not limited to: (i) wage theft; (ii) identity theft; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery of wage theft and identity theft; (iv) continued risk of their PII and direct deposits, which remain in Defendant's possession unprotected; (v) diminished value of their PII; and (vi) 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.

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

213. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and the Class Members, proceeds that they unjustly received from Plaintiffs, the Class Members, or their respective employers. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs, the Class Members, and their respective employers overpaid for Defendant's services.

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

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

215. 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 and direct deposits.

Defendant accepted this duty and obligation when it received Plaintiffs and the Class Members' PII and direct deposits.

216. 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.

217. Plaintiffs and the Class Members entrusted their direct deposits and direct deposit information to Defendant on the premise and with the understanding that Defendant would safeguard their information, ensure that the direct deposits when to the correct accounts, refrain from disclosing direct deposit information to unauthorized third parties, and prevent unauthorized changes of Plaintiffs' and the Class Members' direct deposit and routing information.

218. Defendant knew or should have known that the failure to exercise due care in the collecting, storing, and using of individual's PII and direct deposits 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.

219. 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.

220. 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 and direct deposits. 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 and direct deposits.

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

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

223. 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.

224. 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 VII – DECLARTORY JUDGMENT
(On Behalf of Plaintiffs and the Class)

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

226. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, 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.

227. 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 and direct deposits. Plaintiffs allege that Defendant's data security measures remain inadequate. Defendant publicly denies these allegations. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their PII and direct deposits and remain at imminent risk that further compromises of their PII and direct deposits will occur in the future. It is unknown what specific measures and changes Defendant has undertaken in response to the Data Breach.

228. 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 while storing it in an Internet-accessible environment, (ii) Defendant's failure to delete PII it has no reasonable need to maintain in an Internet-accessible environment, and (iii) Defendant's failure to ensure all changes to Plaintiffs' and the Class Members' direct deposit and routing information are verified, approved, and accurate.

229. 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 and direct deposits of Plaintiffs and the Class;

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

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

230. 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 and direct deposits. 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.

231. 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.

232. 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.

233. 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 Plaintiff 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 Fed. R. Civ. P. 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 appropriate monetary relief, including actual and statutory damages, punitive damages, attorney 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 implement reasonable and reliable security measures to require that all requested changes to direct deposit or routing information are verified, accurate, and approved;

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

viii. 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: February 6, 2024

Respectfully submitted,

/s/ William B. Federman

William B. Federman, OBA #2853
Jessica A. Wilkes, OBA #34823
Federman & Sherwood
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
Telephone: (405)235-1560
wbf@federmanlaw.com