

**UNITED STATES DISTRICT COURT FOR
THE WESTERN DISTRICT OF PENNSYLVANIA**

VINCIEN CURRIE
1550 Madison Road, Apt 9
Hermitage, PA 45206

Individually and on Behalf of All Others
Similarly Situated,

Plaintiff,

v.

JOY CONE CO.,
3435 Lamor Road
Hermitage, PA 16148

Defendant

CASE NO. 23-764

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Vincien Currie (“Mr. Currie” or “Plaintiff”) brings this action on behalf of himself, and all others similarly situated against Defendant, Joy Cone Co., (“Joy Cone” or “Defendant”), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities, and alleges as follows:

SUMMARY OF THE CASE

1. On February 27, 2023, Defendant Joy Cone, a Pennsylvania corporation that produces “over two billion cones a year” for “over 100 years”¹, lost control over its current and former employees’ highly sensitive personal information in a data breach perpetrated by cybercriminals (“Data Breach”). The number of total breach victims is unknown, but on information and belief, the Data Breach has impacted at least thousands of former and current

¹ Our Company, Joy Cone, <https://joycone.com/our-company/#:~:text=We%20are%20an%20independent%2C%20100.best%20cones%20on%20the%20market>. (last accessed May 5, 2023)

employees.

2. On information and belief, the Data Breach occurred on or around February 27, 2023. Due to Defendant’s purposefully obscure language when announcing the breach, it is unclear how long cybercriminals had unfettered access to Defendant’s network and Plaintiff’s and the Class’s personal information, with Defendant only admitting to being aware of the cybercriminals “recently” in its notice. (“Breach Notice”), an example of which is attached as Exhibit A (notice received by the Plaintiff).

3. On or around March 9, 2022, Defendant’s investigations revealed that cybercriminals gained unauthorized access to current and former employees’ personally identifiable information (“PII”) stored on Defendant’s network.

4. On information and belief, cybercriminals bypassed Defendant’s inadequate security systems to access employees’ PII in its computer systems.

5. On information and belief, the stolen PII included, at minimum, employees’ names, Social Security numbers.

6. On or around April 10, 2023—nearly two months after the Data Breach first occurred—Defendant finally began notifying victims about the breach. Exh. A.

7. Defendant’s Breach Notice obfuscated the nature of the breach and the threat it posed—refusing to tell its employees how many people were impacted, how the breach happened, or why it took the Defendant nearly two months to begin notifying victims that hackers had gained access to highly sensitive employee information.

8. Defendant’s failure to timely detect and report the Data Breach made its current and former employees vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their PII.

9. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII misuse.

10. In failing to adequately protect employees' information, adequately notify them about the breach, and obfuscating the nature of the breach, Defendant violated state and federal law and harmed an unknown number of its affiliates' current and former employees.

11. Plaintiff and members of the proposed Class are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiff and members of the proposed Class trusted Defendant with their PII. But Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

12. Plaintiff Currie is a former Joy Cone employee and Data Breach victim. Mr. Currie worked for Joy Cone from 2017-2022.

13. Accordingly, Plaintiff, on his own behalf and on behalf of a class of similarly situated individuals, brings this lawsuit seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in Defendant's possession.

PARTIES

14. Plaintiff, Vincien Currie, is a natural person and citizen of Pennsylvania, residing in Hermitage, Pennsylvania, where he intends to remain. Mr. Currie is a former Joy Cone employee and Data Breach victim, receiving Defendant's Breach Notice in April 2023.

15. Defendant, Joy Cone, is a Pennsylvania Corporation, with its principal place of business at 3435 Lamor Road, Hermitage, PA 16148.

JURISDICTION & VENUE

16. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of \$5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

17. This Court has personal jurisdiction over Defendant because Joy Cone is headquartered in this District and Joy Cone conducts substantial business in this District.

18. Venue is proper in this District because Joy Cone is headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

BACKGROUND FACTS

Joy Cone

19. Joy Cone is “the largest ice cream cone producer in the United States” producing “two billion cones each year.”² Joy Cone boasts over \$421.9 Million in revenue.³

20. On information and belief, Joy Cone accumulates highly sensitive PII of its employees.

21. On information and belief, Joy Cone maintains former employees' PII for years—even decades—after the employee-employer relationship is terminated.

22. In collecting and maintaining its employees' PII, Defendant agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiff and Class Members themselves took reasonable steps to secure their PII.

² Our Company, Joy Cone, <https://joycone.com/our-company/#:~:text=We%20are%20an%20independent%2C%20100.best%20cones%20on%20the%20market>. (last accessed May 5, 2023).

³ Joy Cone, Zoominfo, <https://www.zoominfo.com/c/joy-cone-co/65538031> (last accessed May 5, 2023).

23. Indeed, Joy Cone promises that it “use[s] reasonable efforts to protect your personal information from unauthorized access, use, or disclosure[.]”⁴

24. Joy Cone touts that it only “retain[s] your personal information for the period necessary to fulfill the purpose outlined in this policy unless a longer retention period is required or permitted by the law.”⁵

25. Despite recognizing its duty to do so, on information and belief, Joy Cone has not implemented reasonable cybersecurity safeguards or policies to protect employee PII or trained its IT or data security employees to prevent, detect, and stop breaches of Joy Cone’s systems. As a result, Joy Cone leaves vulnerabilities in its systems for cybercriminals to exploit and gain access to employee PII.

Joy Cone Fails to Safeguard Employees’ PII

26. Plaintiff is a former employee of Joy Cone.

27. As a condition of employment with Joy Cone, Defendant requires its employees to disclose PII including but not limited to, their names and Social Security numbers. Defendant used that PII to facilitate its employment of Plaintiff, including payroll, and required Plaintiff to provide that PII to obtain employment and payment for that employment.

28. On information and belief, Joy Cone collects and maintains current and former employees’ PII in its computer systems.

29. In collecting and maintaining the PII, Joy Cone implicitly agrees it will safeguard the data using reasonable means according to its internal policies and federal law.

⁴Privacy Policy, Joy Cone, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://joycone.com/wp-content/uploads/2020/11/FINAL_Joy-Cone-Privacy-Policy_CCPA602339972.3_9.18.20-2.pdf (last accessed May 5, 2023).

⁵ Privacy Policy, Joy Cone, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://joycone.com/wp-content/uploads/2020/11/FINAL_Joy-Cone-Privacy-Policy_CCPA602339972.3_9.18.20-2.pdf (last accessed May 5, 2023).

30. According to the April 10, 2023, Breach Notice, Joy Cone first “became aware of suspicious activity affecting certain systems within their network”. Exh. A. Due to the obfuscating nature of Defendant’s Notice, it is unclear when Defendant actually discovered the Data Breach.

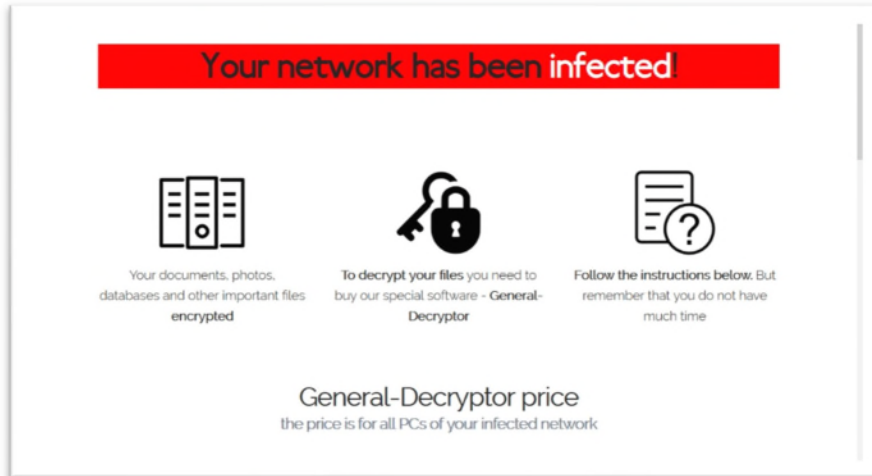
31. On or around March 9, 2023, Defendant’s investigation revealed that its network had been hacked by cybercriminals and that Defendant’s inadequate cyber and data security systems and measures allowed those responsible for the cyberattack to obtain files containing a treasure trove of thousands of Joy Cone employees’ personal, private, and sensitive information, including but not limited to employees’ names, Social Security numbers.

32. Upon information and belief, the notorious Lorenz ransomware gang was responsible for the cyberattack. Known as one of the most notorious and active ransomware actors, Lorenz has perpetrated multiple high-profile breaches in the last year alone.⁶ Joy Cone knew or should have known of the tactics that groups like Lorenz employ.

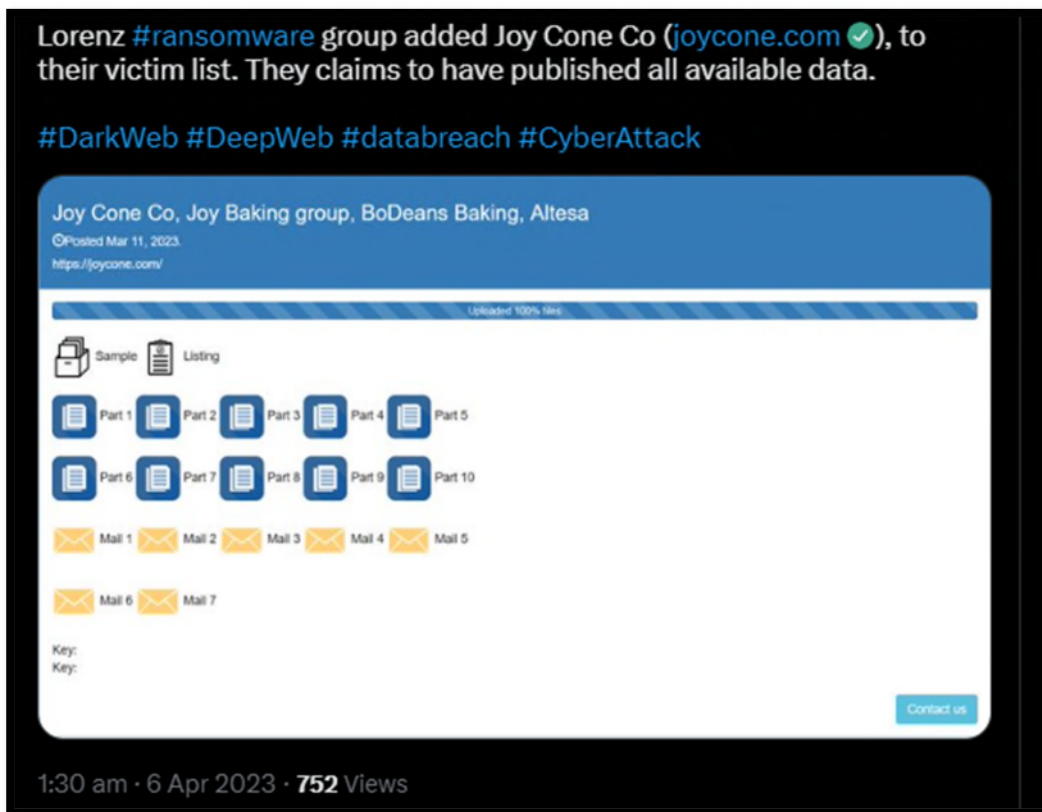
33. Additionally, Defendant admitted that Plaintiff’s and the Class’s PII were actually stolen during the Data Breach, confessing that the information was not just accessed but that the cybercriminals “**may have viewed or taken certain information** stored in those areas”. Exh. A.

34. With the Sensitive Information secured and stolen by Lorenz, the hackers then purportedly issued a ransom demand to Joy Cone. However, Joy Cone has provided no public information on the ransom demand or payment. An example of Lorenz’s standard demand ransom page is displayed below:

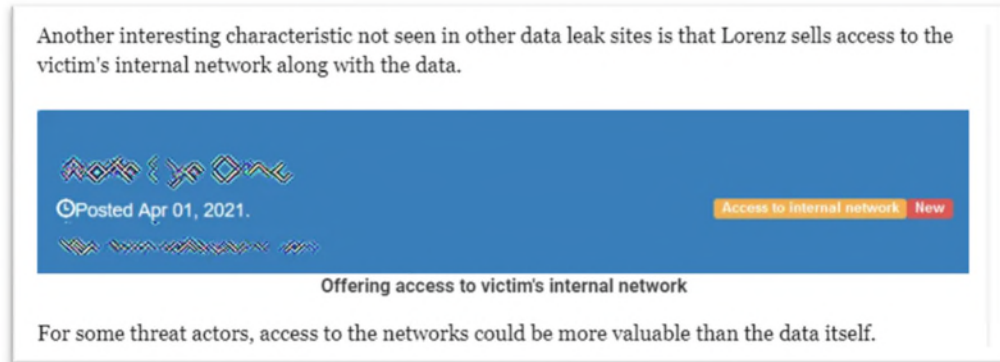
⁶ Meet Lorenz, Bleeping Computer, <https://www.bleepingcomputer.com/news/security/meet-lorenz-a-new-ransomware-gang-targeting-the-enterprise/> (last accessed May 5, 2023).



35. On April 6, 2023, the presumed deadline of Lorenz’s ransom demand, Lorenz released information obtained from the Breach on a data leak page. On information and belief, all stolen information was released onto the data leak page.



36. This is a technique Lorenz is well known for. Unique to Lorenz is their tendency to sell access to the victim's internal network along with the stolen data⁷, putting Plaintiff's and the Class's PII at high risk of a future breach.



37. Employees place value in data privacy and security. These are important considerations when deciding who to work and provide services for. Plaintiff would not have accepted the Defendant's employment offer, nor provided his PII, to Joy Cone had he known that Joy Cone does not take all necessary precautions to secure the PII given to it by its employees.

38. On or about April 10, 2023—almost two months after the Data Breach occurred—Joy Cone finally notified Plaintiff and Class Members about the Data Breach.

39. Despite its duties and alleged commitments to safeguard PII, Joy Cone does not follow industry standard practices in securing employees' PII, as evidenced by the Data Breach and stolen employee PII.

40. In response to the Data Breach, Joy Cone contends that it “reviewing our existing policies and procedures regarding cybersecurity and evaluating additional measures and safeguards to protect against this type of event in the future. We are also implementing additional network security measures to further enhance our network security” Exh. A. Although Joy Cone fails to expand on these alleged “additional measures” and “additional network security” are, such

⁷ *Id.*

steps should have been in place *before* the Data Breach.

41. Through its Breach Notice, Joy Cone also recognized the actual imminent harm and injury that flowed from the Data Breach, so it encouraged breach victims to “remain vigilant against incidents of identity theft and fraud by reviewing [their] account statements and monitoring [their] free credit reports for suspicious activity.” Exh. A.

42. On information and belief, Joy Cone has offered only two years of complimentary credit monitoring services to victims, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the breach involves PII that cannot be changed, such as Social Security numbers. Further, the breach exposed employees’ nonpublic, highly private information, a disturbing harm in and of itself.

43. Even with complimentary credit monitoring services, the risk of identity theft and unauthorized use of Plaintiff’s and Class Members’ PII is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

44. Cybercriminals need not harvest a person’s Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff’s and the Class’s PII. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create “Fullz” packages, which can then be used to commit fraudulent account activity on Plaintiff’s and the Class’s financial accounts.

45. On information and belief, Joy Cone failed to adequately train its IT and data security employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over employee PII. Defendant’s negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing PII. Further, the Breach Notice makes clear that Joy Cone cannot, or will not, determine the full scope of the Data Breach.

Plaintiff's Experience

46. Plaintiff Currie is a former Joy Cone employee.

47. As a condition of employment with Joy Cone, Plaintiff was required to provide his PII, including but not limited to his full name and Social Security number.

48. Plaintiff provided his PII to Joy Cone and trusted that the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law.

49. Plaintiff Currie received a Breach Notice in April 2023, from Defendant, indicating that his PII, including at least his name and Social Security number, may have been compromised in the Data Breach. In addition to the damages detailed herein, the Data Breach has caused Plaintiff Currie, to be at substantial risk for further identity theft.

50. Defendant deprived Plaintiff of the earliest opportunity to guard himself against the Data Breach's effects by failing to notify him about it for over four months after Joy Cone finally discovered the Data Breach.

51. Plaintiff suffered actual injury from the exposure of his PII—which violates his rights to privacy.

52. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

53. As a result of the Data Breach and the recommendations of Defendant's Notice, Plaintiff has spent time and made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, changing his online account passwords, placing a credit freeze through the

three main credit bureaus, and monitoring his credit information as suggested by Defendant.

54. Plaintiff has and will spend considerable time and effort monitoring his accounts to protect himself from identity theft. Plaintiff fears for his personal financial security and uncertainty over what PII was exposed in the Data Breach. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

55. Plaintiff is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third parties. This injury was worsened by Defendant's delay in informing Plaintiff and Class Members about the Data Breach.

56. Plaintiff 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.

Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

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

58. The ramifications of Defendant's failure to keep Plaintiff's and the Class's PII secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, or other nonpublic financial information, without permission, to commit fraud or other crimes.

59. The types of PII compromised and potentially stolen in the Joy Cone Data Breach is highly valuable to identity thieves. The employees' stolen PII can be used to gain access to a

variety of existing accounts and websites to drain assets, bank accounts or open phony credit cards.

60. Identity thieves can also use this data to harm Plaintiff and Class members through embarrassment, blackmail, or harassment in person or online, or to commit other types of fraud including obtaining ID cards or driver's licenses, fraudulently obtaining tax returns and refunds, and obtaining government benefits. A Presidential Report on identity theft from 2008 states that:

In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts, . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.

In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.

61. As a result of Defendant's failure to prevent the Data Breach, Plaintiff and the proposed 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 spent researching how to prevent, detect, contest, and recover from 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 the possession of defendant and is subject to further breaches so long as defendant fails to undertake the appropriate measures to protect the PII in their possession.

62. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to \$1,000.00 depending on the type of information obtained.⁸

63. The value of Plaintiff's and the proposed Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

64. Social Security numbers are particularly attractive targets for hackers because they can easily be used to perpetrate identity theft and other highly profitable types of fraud. Moreover, Social Security numbers are difficult to replace, as victims are unable to obtain a new number until the damage is done.

65. It can take victims years to spot identity or PII theft, giving criminals plenty of time to use that information for cash.

⁸ Here's How Much Your Personal Information Is Selling for on the Dark Web, Experian, <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last visited July 7, 2022).

66. One such example of criminals using PII for profit is the development of “Fullz” packages.

67. 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.⁹

68. The development of “Fullz” packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff’s and the proposed Class’s 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. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff’s and the proposed Class’s stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

69. Defendant disclosed the PII of Plaintiff and the Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiff and members of the proposed 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.

⁹ *Id.*

70. Defendant's use of outdated and insecure computer systems and software that are easy to hack, and its failure to maintain adequate security measures and an up-to-date technology security strategy, demonstrates a willful and conscious disregard for privacy, and has exposed the PII of Plaintiff and members of the proposed Class to unscrupulous operators, con artists, and criminals.

71. Defendant's failure to properly notify Plaintiff and members of the proposed Class of the Data Breach exacerbated Plaintiff's 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.

Joy Cone Failed to Adhere to FTC Guidelines

72. 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.

73. 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 personal customer information that they keep;
- b. properly dispose of personal information 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.

74. 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.

75. 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.

76. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer 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 (“FTCA”), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

77. Defendant’s failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers’ PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Plaintiff and Class Members Suffered Damages

78. The compromised and stolen information of Plaintiff and Class members is private and sensitive in nature and was left inadequately protected by Joy Cone. Defendant did not obtain Plaintiff’s and Class members’ consent to disclose this data to any other person as required by applicable law and industry standards.

79. The data breach was a direct and proximate result of Defendant’s failure to properly safeguard and protect Plaintiff’s and Class members’ PII from unauthorized access, use, and

disclosure, as required by various state and federal regulations, industry practices, and the common law, including the failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class members' sensitive personal information to protect against reasonably foreseeable threats to the security or integrity of such information.

80. Had Joy Cone remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, Joy Cone would have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and the Class Members' PII.

81. As a direct and proximate result of Defendant's wrongful actions and inaction and the resulting data breach, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the data breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports. This time has been lost forever and cannot be recaptured.

82. Defendant's wrongful actions and inaction directly and proximately caused the potential theft and dissemination into the public domain of Plaintiff's and Class members' PII, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

- a. theft of their personal and financial information;

- b. unauthorized charges on their debit and credit card accounts;
- c. the actual, imminent, and certainly impending injury flowing from potential fraud and identity theft posed by their credit/debit card and personal information being placed in the hands of criminals and misused via the sale of Plaintiff's and Class members' information on the Internet's black market;
- d. the untimely and inadequate notification of the data breach;
- e. the improper disclosure of their PII;
- f. loss of privacy;
- g. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the data breach;
- h. ascertainable losses in the form of deprivation of the value of their PII, for which there is a well-established national and international market;
- i. ascertainable losses in the form of the loss of cash back or other benefits as a result of their inability to use certain accounts and cards affected by the data breach;
- j. loss of use of, and access to, their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse credit notations; and
- k. the loss of productivity and value of their time spent to address, attempt to ameliorate, mitigate, and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards,

purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the inconvenience, nuisance and annoyance of dealing with all such issues resulting from the Data reach.

Defendant's Offer of Credit Monitoring is Inadequate

83. At present, Joy Cone has offered two years of free credit monitoring provided by Experian to breach victims.

84. As previously alleged, Plaintiff's and the Class Members' PII may exist on the Dark Web and in the public domain for months, or even years, before it is used for ill gains and actions. With only two years of monitoring, Plaintiff and Class Members remain unprotected from the real and long-term threats against their personal, sensitive, and private data.

85. Therefore, the "monitoring" services offered by Joy Cone are inadequate, and Plaintiff and Class Members have a real and cognizable interest in obtaining equitable relief, in addition to the monetary relief requested herein.

CLASS ACTION ALLEGATIONS

86. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23 on behalf of himself and all members of the proposed class (the "Class"), defined as follows:

Class: All individuals residing in the United States whose PII was compromised in the Joy Cone Data Breach, including all those who received notice of the breach.

87. The following people are excluded from the Class: (1) any judge or magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which the Defendant or its parent has a controlling interest, and their current or former officers and directors; (3) persons who

properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

88. Plaintiff reserves the right to amend the Class definition or add a Class if further information and discovery indicate that other classes should be added and if the definition of the Class should be narrowed, expanded, or otherwise modified.

89. Plaintiff and members of the Class satisfy the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23:

a. **Numerosity**. The exact number of Class members is unknown but is estimated to be up to thousands of former and current Joy Cone employees at this time, and individual joinder in this case is impracticable. Class Members can be easily identified through Defendant's records and objective criteria permitting self-identification in response to notice, and notice can be provided through techniques similar to those customarily used in other data breach, employee breach of contract, unlawful trade practices, and class action controversies;

b. **Typicality**: Plaintiff's claims are typical of the claims of other Class members in that Plaintiff, and the Class Members sustained damages arising out of Defendant's Data Breach, wrongful conduct and misrepresentations, false statements, concealment, and unlawful practices, and Plaintiff and the Class Members sustained similar injuries and damages, as a result of Defendant's uniform illegal conduct;

c. **Adequacy**: Plaintiff will fairly and adequately represent and protect the interests of the Class and has retained counsel competent and experienced in complex class

actions to vigorously prosecute this action on behalf of the Class. Plaintiff has no interests that conflict with, or are antagonistic to those of, the Class, and Defendant has no defenses unique to Plaintiff.

d. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiff and the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include, but are not necessarily limited to the following:

- i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII;
- ii. 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;
- iii. Whether Defendant was negligent in maintaining, protecting, and securing PII;
- iv. Whether Defendant breached contract promises to safeguard Plaintiff's and the Class's PII;
- v. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;
- vi. Whether Defendant's Breach Notice was reasonable;
- vii. Whether the Data Breach caused Plaintiff and the Class injuries;
- viii. What the proper damages measure is; and
- ix. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

e. **Superiority:** This case is also appropriate for class certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy as joinder of all parties is impracticable. The damages suffered by the individual members of the Class will likely be relatively small, especially given the burden and expense of individual prosecution of the complex litigation necessitated by Defendant's actions. Thus, it would be virtually impossible for the individual members of the Class to obtain effective relief from Defendant's misconduct. Even if members of the Class could sustain such individual litigation, it would still not be preferable to a class action, because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Economies of time, effort and expense will be fostered, and uniformity of decisions ensured.

CLAIMS ALLEGED ON BEHALF OF PLAINTIFF AND THE CLASS

First Claim for Relief
Negligence
(On Behalf of Plaintiff and the Class)

90. Plaintiff and the members of the Class incorporate the above allegations as if fully set forth herein.

91. Plaintiff and members of the Class entrusted their PII to Joy Cone. Defendant owed a duty to Plaintiff and the Class to exercise reasonable care in safeguarding and protecting their PII and keeping it from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties. This duty included, among other things, designing, maintaining, and testing Defendant's

security systems to ensure the PII of Plaintiff and the Class was adequately secured and protected, including using encryption technologies. Defendant further had a duty to implement processes that would detect a breach of its security system in a timely manner.

92. Joy Cone was under a basic duty to act with reasonable care when it undertook to collect, create, and store Plaintiff's and the Class's sensitive data on its computer system, fully aware—as any reasonable entity of its size would be—of the prevalence of data breaches and the resulting harm such a breach would cause. The recognition of Defendant's duty to act reasonably in this context is consistent with, *inter alia*, the Restatement (Second) of Torts § 302B (1965), which recounts a basic principle: an act or omission may be negligent if the actor realizes or should realize it involves an unreasonable risk of harm to another, even if the harm occurs through the criminal acts of a third party.

93. Defendant knew that the PII of Plaintiff and the Class was personal and sensitive information that is valuable to identity thieves and other criminals. Defendant also knew of the serious harm that could happen if the PII of Plaintiff and the Class was wrongfully disclosed.

94. By being entrusted by Plaintiff and the Class to safeguard their PII, Defendant had a special relationship with Plaintiff and the Class. Plaintiff and the Class agreed to provide their PII with the understanding that Defendant would take appropriate measures to protect it and would inform Plaintiff and the Class of any security concerns that might call for action by Plaintiff and the Class.

95. Defendant breached its duty to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class members' PII by failing to adopt, implement, and maintain adequate security measures to safeguard that information, despite failures and intrusions, and allowing unauthorized access to Plaintiff' and the other Class member's PII.

96. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and the Class, their PII would not have been compromised, stolen, and viewed by unauthorized persons. Defendant's negligence was a direct and legal cause of the theft of the personal data of Plaintiff and the Class and all resulting damages.

97. The injury and harm suffered by Plaintiff and the Class members was the reasonably foreseeable result of Defendant's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the other Class members' PII. Defendant knew its systems and technologies for processing and securing the PII of Plaintiff and the Class had numerous security vulnerabilities.

98. As a result of this misconduct by Defendant, the PII of Plaintiff and the Class were compromised, placing them at a greater risk of identity theft and subjecting them to identity theft, and their PII was disclosed to third parties without their consent. Plaintiff and Class members also suffered diminution in value of their PII in that it is now easily available to hackers on the Dark Web. Plaintiff and the Class have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

Second Claim for Relief
Negligence Per Se
(On Behalf of Plaintiff and the Class)

99. Plaintiff and the members of the Class incorporate the above allegations as if fully set forth herein.

100. 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's and members of the Class's PII.

101. 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 customers or, in this case, employees’ PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant’s duty to protect Plaintiff’s and the members of the Class’s sensitive PII.

102. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein.

103. Defendant’s violation of Section 5 of the FTC Act constitutes negligence *per se*.

104. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

105. Defendant breached its respective duties to Plaintiff and members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff’s and members of the Class’s PII.

106. But for Defendant’s wrongful and negligent breach of its duties owed to Plaintiff and members of the Class, Plaintiff and members of the Class would not have been injured.

107. The injury and harm suffered by Plaintiff and members of the Class were the reasonably foreseeable result of Defendant’s breach of its duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

108. Had Plaintiff and members of the Class known that Defendant did not adequately protect their PII, Plaintiff and members of the Class would not have entrusted Defendant with their

PII.

109. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and members of the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of PII; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen personal information, entitling them to damages in an amount to be proven at trial.

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

Third Claim for Relief
Breach of Confidence
(On Behalf of Plaintiff and the Class)

111. Plaintiff and the members of the Class incorporate the above allegations as if fully set forth herein.

112. At all times during Plaintiff's and Class Members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' PII that Plaintiff and Class Members were provided to Defendant in exchange for employment.

113. As alleged herein and above, Defendant's relationship with Plaintiff and Class Members was governed by expectations that Plaintiff's and Class Members' PII would be

collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

114. Plaintiff and Class Members provided their respective PII to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the PII to be disseminated to any unauthorized parties.

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

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

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

118. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and Class Members have suffered damages.

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

120. The injury and harm Plaintiff and Class Members suffered was the reasonably

foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and Class Members' PII. Defendant knew its computer systems and technologies for accepting and securing Plaintiff's and Class Members' PII had numerous security vulnerabilities because Defendant failed to observe industry standard information security practices.

121. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and the Class have suffered, and continue to suffer, injuries and damages arising from identity theft; damages from lost time and effort to mitigate the actual and potential impact of the data breach on their lives, including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports, and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

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

Fourth Claim for Relief
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

123. Plaintiff and the members of the Class incorporate the above allegations as if fully set forth herein.

124. Plaintiff and Class Members were required to provide their PII Defendant as a condition of receiving employment from Defendant. Plaintiff and Class Members provided their PII to Defendant in exchange for Defendant's employment.

125. Plaintiff and Class Members reasonably understood that a portion of the funds from their employment would be by Defendant used to pay for adequate cybersecurity and protection of their PII.

126. Plaintiff and the Class Members accepted Defendant's offers by disclosing their PII to Defendant in exchange for employment.

127. In turn, and through internal policies, Defendant agreed to protect and not disclose the PII to unauthorized persons.

128. In its Privacy Policy, Defendant represented that they had a legal duty to protect Plaintiff's and Class Member's PII.

129. Implicit in the parties' agreement was that Defendant would provide Plaintiff and Class Members with prompt and adequate notice of all unauthorized access and/or theft of their PII.

130. After all, Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of such an agreement with Defendant.

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

132. The covenant of good faith and fair dealing is an element of every contract. Thus, parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—and not merely the letter—of the bargain. In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

133. Subterfuge and evasion violate the duty of good faith in performance even when an

actor believes their conduct to be justified. Bad faith may be overt or consist of inaction. And fair dealing may require more than honesty.

134. Defendant materially breached the contracts it entered with Plaintiff and Class Members by:

- a. failing to safeguard their information;
- b. failing to notify them promptly of the intrusion into its computer systems that compromised such information.
- c. failing to comply with industry standards;
- d. failing to comply with the legal obligations necessarily incorporated into the agreements; and
- e. failing to ensure the confidentiality and integrity of the electronic PII that Defendant created, receive and maintained.

135. In these and other ways, Defendant violated its duty of good faith and fair dealing.

136. Defendant's material breaches were the direct and proximate cause of Plaintiff's and Class Members' injuries (as detailed *supra*).

137. Plaintiff and Class Members performed as required under the relevant agreements, or such performance was waived by Defendant's conduct.

Fifth Claim for Relief
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

138. Plaintiff and the members of the Class incorporate the above allegations as if fully set forth herein.

139. This claim is pleaded in the alternative to the breach of implied contract claim.

140. Plaintiff and Class Members conferred a benefit upon Defendant. After all,

Defendant benefitted from using their PII to facilitate its business.

141. Defendant appreciated or had knowledge of the benefits it received from Plaintiff and Class Members. And Defendant benefited from receiving Plaintiff's and Class Members' PII, as this was used to facilitate its business.

142. Plaintiff and Class Members reasonably understood that a portion of the funds from their employment would be by Defendant used to pay for adequate cybersecurity and protection of their PII.

143. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII.

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

145. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and Class Members' services because Defendant failed to adequately protect their PII.

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

147. Defendant should be compelled to disgorge into a common fund—for the benefit of Plaintiff and Class Members—all unlawful or inequitable proceeds that it received because of its misconduct.

Sixth Claim for Relief
Publicity Given to Private Life
(On Behalf of Plaintiff and the Class)

148. Plaintiff and the members of the Class incorporate the above allegations as if fully set forth herein.

149. One who gives publicity to matters concerning the private life of another, of a kind highly offensive to a reasonable man, is subject to liability to the other for invasion of his privacy.

150. As a condition of receiving Defendant's employment, Plaintiff and the Class provided Defendant with sensitive personal information, including names and Social Security numbers.

151. Defendant failed to employ adequate and reasonable security measures to prevent public disclosure of Plaintiff's and the Class's PII.

152. Defendant failed to timely and reasonably notify Plaintiff and the Class about the Data Breach, which made Plaintiff and the Class vulnerable to identity theft.

153. As a result of the disclosure of Plaintiff's and the Class's PII, Plaintiff have suffered a *de facto* injury, which entitles them to general damages.

Seventh Claim for Relief
Declaratory Judgment
(On Behalf of Plaintiff and the Class)

154. Plaintiff and the members of the Class incorporate the above allegations as if fully set forth herein.

155. 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 to grant further necessary relief. The Court has broad authority to restrain acts, such as those alleged herein, which are tortious and unlawful.

156. In the fallout of the Data Breach, an actual controversy has arisen about Defendant's various duties to use reasonable data security. On information and belief, Plaintiff alleges that Defendant's actions were—and *still* are—inadequate and unreasonable. And Plaintiff and Class Members continue to suffer injury from the ongoing threat of fraud and identity theft.

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

- a. Defendant owed—and continues to owe—a legal duty to use reasonable data security to secure the data entrusted to it;
- b. Defendant has a duty to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;
- c. Defendant breached, and continues to breach, its duties by failing to use reasonable measures to the data entrusted to it; and
- d. Defendant breaches of its duties caused—and continues to cause—injuries to Plaintiff and Class Members.

158. The Court should also issue corresponding injunctive relief requiring Defendant to use adequate security consistent with industry standards to protect the data entrusted to it.

159. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy if Defendant experiences a second data breach.

160. And if a second breach occurs, Plaintiff and the Class will lack an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages—while warranted for out-of-pocket damages and other legally quantifiable and provable damages—cannot cover the full extent of Plaintiff's and Class Members' injuries.

161. If an injunction is not issued, the resulting hardship to Plaintiff and Class Members far exceeds the minimal hardship that Defendant could experience if an injunction is issued.

162. An injunction would benefit the public by preventing another data breach—thus preventing further injuries to Plaintiff, Class Members, and the public at large.

PRAYER FOR RELIEF

Plaintiff and members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

- A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing their counsel to represent the Class;
- B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;
- C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;
- D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;
- E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;
- F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;
- G. Awarding attorneys' fees and costs, as allowed by law;
- H. Awarding prejudgment and post-judgment interest, as provided by law;

- I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and
- J. Granting such other or further relief as may be appropriate under the circumstances.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

DATE: May 9, 2023

BY: /s/ Elizabeth A. Bailey

Elizabeth A. Bailey (PA ID #316689)

Patrick Howard* (PA ID #88572)

SALTZ, MONGELUZZI, & BENDESKY, P.C.

1650 Market Street, 52nd Floor

Philadelphia, PA 19103

Tel: (215) 496-8282

Fax: (215) 496-0999

ebailey@smbb.com

phoward@smbb.com

Samuel J. Strauss*

am@turkestrauss.com

Raina C. Borrelli*

raina@turkestrauss.com

TURKE & STRAUSS LLP

613 Williamson St., Suite 201

Madison, WI 53703

Telephone (608) 237-1775

Facsimile: (608) 509-4423

**Pro Hac Vice to be submitted*

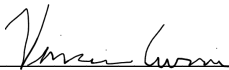
Attorneys for Plaintiff and the proposed Class

VERIFICATION

I, Vincien Currie, hereby certify that I have read the foregoing and that the following is correct:

The facts set forth in the foregoing document are based upon information which I have furnished to counsel, as well as upon information which has been gathered by counsel and or/others acting on my behalf in this matter. The language of the document is that of counsel and not my own. I have read the document, and to the extent it is based upon information which I have given counsel, it is true and correct to the best of my knowledge, information and belief. To the extent the content of the document is that of counsel, I have relied upon such counsel in making this Verification. I hereby acknowledge that the facts set forth in the aforesaid document are made subject to the penalties of 18 Pa. C.S.A. §4904 relating to unsworn falsification to authorities.

05 / 08 / 2023
Date


Vincien Currie