FILED
Circuit Court Whiteside County
Date: 4/16/2024 8:43 AM
Sue Costello Circuit Clerk

IN THE CIRCUIT COURT FOR THE FOURTEENTH JUDICIAL CIRCUIT
WHITESIDE COUNTY, ILLINOIS

MARY BOWSER, as an individual and on behalf of all others similarly situated, Plaintiff, vs. HALO BRANDED SOLUTIONS, INC. Defendant.	CASE NO.: 2024LA18

CLASS ACTION COMPLAINT

Plaintiff Mary Bowser ("Plaintiff") brings this Class Action Complaint against HALO Branded Solutions, Inc. ("HALO" or "Defendant"), as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to her own actions and her counsels' investigation, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendant HALO Branded Solutions, Inc., a Sterling, Illinois based merchandise and uniform company, to seek damages for herself and other similarly situated current and former employees ("employees"), or any other person(s) impacted in the data breach at issue ("Class Members") who she seeks to represent, as well as other equitable relief, including, without limitation, injunctive relief designed to protect the very sensitive information of Plaintiff and other Class Members. This action arises from Defendant's failure to properly secure and safeguard personal identifiable information, including without limitation, unencrypted and unredacted names, dates of birth, and Social Security numbers (collectively, "personal identifiable information" or "PII").

2. Plaintiff alleges HALO failed to provide timely, accurate and adequate notice to Plaintiff and Class Members who were or are employees of HALO. Current and former employees' knowledge about what personal identifiable information HALO lost, as well as precisely what

types of information was unencrypted and in the possession of unknown third parties, was unreasonably delayed by HALO's unreasonable notification delay of approximately eight months after it first learned of the data breach.

3. On or about March 28, 2024, HALO notified state Attorneys General about a widespread data breach involving sensitive PII of 7,305 individuals. HALO explained in its required notice letter that it discovered that "[c]omputer systems within our network were accessed by a sophisticated threat actor using techniques to evade detection by our information security defenses." HALO discovered that files on its network were accessed and acquired by the unknown actor (the "Data Breach").

4. In November 2023, when the Data Breach occurred, HALO chose not to notify affected current or former employees or, upon information and belief, anyone of its data breach instead choosing to address the incident in-house by implementing other safeguards to some aspects of its computer security.

5. Approximately five months later, on March 28, 2024, HALO concluded its investigation and notified Class Members' PII had been impacted and may have been taken from its network.

6. HALO "promptly took these systems offline, notified law enforcement, and engaged cybersecurity experts to investigate" HALO's systems, and determined that Plaintiff's and Class Members' personal identifiable information (including but not limited to full name, dates of birth, and Social Security numbers) was present and stolen by the unauthorized person at the time of the incident.

7. Plaintiff and the Class Members in this action were, upon information and belief, current and former employees of HALO. Upon information and belief, the first that Plaintiff and the Class Members learned of the Data Breach was when they received by U.S. Mail Notice of Data Breach letters sent on March 28, 2024, directly from HALO.

8. In its Notice Letters, sent to Plaintiff and Class Members, HALO failed to explain why it took the company five months (from November 2023, when HALO detected unusual

activity to March 28, 2024) to alert Class Members that their sensitive PII had been exposed. As a result of this delayed response, Plaintiff and Class Members were unaware that their PII had been compromised, and that they were, and continue to be, at significant risk to identity theft and various other forms of personal, social, and financial harm.

9. Plaintiff's and Class Members' unencrypted, unredacted PII was compromised due to HALO's negligent and/or careless acts and omissions, and due to the utter failure to protect Class Members' sensitive data. Hackers obtained their PII because of its value in exploiting and stealing the identities of Plaintiff and similarly situated Class Members. The risks to these persons will remain for their respective lifetimes.

10. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of HALO's failure to: (i) adequately protect Plaintiff and Class Member PII; (ii) warn Plaintiff and Class Members of its inadequate information security practices; and (iii) effectively monitor HALO's network for security vulnerabilities and incidents. HALO's conduct amounts to negligence and violates federal and state statutes.

11. Plaintiff and Class Members have suffered injury as a result of HALO's conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, (iv) the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges; change their usernames and passwords on their accounts; investigate, correct and resolve unauthorized debits; deal with spam messages and e-mails received subsequent to the Data Breach, (v) charges and fees associated with fraudulent charges on their accounts, and (vi) the continued and certainly an increased risk to their PII, which remains in HALO's possession and is subject to further unauthorized disclosures so long as HALO fails to undertake appropriate and adequate measures to protect the PII. These risks will remain for the lifetimes of Plaintiff and Class Members.

12. HALO disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or at the very least negligently failing to take and implement adequate and reasonable measures to ensure that its employee PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As the result, the PII of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

13. Plaintiff Mary Bowser is a resident and citizen of Illinois, residing in Dixon Ms. Bowser received HALO's *Notice of Security Incident*, dated March 28, 2024, by U.S. Mail.

14. Defendant HALO Branded Solutions, Inc. is a merchandise and uniform company headquartered in Sterling, Illinois, which has a principal place of business at 1500 Halo Way, Sterling, Illinois 61081.

15. 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 Plaintiff. Plaintiff 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.

16. All of Plaintiff's claims stated herein are asserted against HALO and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction over this matter pursuant to Ill. Const. 1970, art. VI, § 9.

18. This Court has personal jurisdiction over Defendant for at least the following reasons: (i) Defendant regularly does business or solicits business, engages in other persistent courses of conduct and/or derives substantial revenue from products and/or services provided to

individuals in Whiteside County and in the State of Illinois and (ii) Defendant has purposefully established substantial, systematic and continuous contacts with Whiteside County and the State of Illinois and expects or should reasonably expect to be in court here.

19. In short, Defendant has (more than) sufficient minimum contacts with this County such that this Court's exercise of jurisdiction over Defendant will not offend traditional notions of fair play and substantial justice.

20. Venue is proper in Whiteside County pursuant to 735 ILCS 5/2-101 because Defendant conducts its usual and customary business in this County and because a substantial portion of the events complained of occurred in this County.

IV. FACTUAL ALLEGATIONS

Background

21. Defendant HALO Branded Solutions, Inc. is a merchandise and uniform company headquartered in Sterling, Illinois, which has a principal place of business at 1500 HALO Way, Sterling, Illinois 61081.

22. In its Notice of Security Incident letter to victims of the Data Breach, HALO states, "Please know that we have taken a number of steps to address this situation, and we are committed to doing the right thing for everyone involved."

23. As HALO acknowledges in its Notice Letters, "We have been working with external cybersecurity experts to investigate what happened, to strengthen our computer network, and to monitor the "dark web" for information relating to our company. These efforts are all ongoing. We are notifying you now that we know what information was involved."

24. Plaintiff and the Class Members, as current or former employees of HALO, reasonably relied (directly or indirectly) on this sophisticated company to keep their sensitive PII confidential; to maintain its system security; to use this information for business purposes only; and to make only authorized disclosures of their PII. Current, former, and prospective employees, in general, demand security to safeguard their PII, especially when Social Security numbers and other sensitive PII is involved.

25. HALO had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' PII from involuntary disclosure to third parties.

The Data Breach

26. In March 2024, HALO first began notifying state Attorneys General ("AGs") about a widespread data breach of its computer systems involving the sensitive personal identifiable information of persons. Upon information and belief, the Class Members were not notified until March 28, 2024, even though HALO explained that the Data Breach was detected in November 2023. [1]

27. According to its Notice Letters to Class Members, HALO explained it discovered in November 2023 (approximately five months earlier) that it detected an unauthorized third-party gained access to a portion of its computer systems and files.

28. On or about March 28, 2024, HALO notified state Attorneys General about a widespread data breach involving sensitive PII of 7,305 individuals.

29. In November 2023, HALO chose not to notify affected Class Members, or upon information and belief, anyone, of its data breach instead choosing to address the incident in-house by implementing other safeguards to some aspects of its computer security. It then simply resumed its normal business operations.

30. Approximately five months later, on March 28, 2024, HALO admitted that Class Members' PII had been impacted and taken from its network.

31. HALO hired the "cybersecurity experts" to investigate HALO's systems, and determined that Plaintiff's and Class Members' personal identifiable information (including but not limited to full names, dates of birth, and Social Security numbers) was present and potentially stolen by the unauthorized person at the time of the incident.

---

[1] Office of the Maine Attorney General, *Data Breach Notifications*, available at: https://apps.web.maine.gov/online/aeviewer/ME/40/df7830da-907e-42eb-9e7e-9603e486f319.shtml (last accessed April 12, 2024).

32. Plaintiff and Class Members in this action were, upon information and belief, current and former employees of HALO. The first that Plaintiff and Class Members learned of the Data Breach was when they received by U.S. Mail Notice of Data Breach letters dated March 28, 2024, directly from HALO.

33. The confidential information that was accessed without authorization included persons' full names along with their dates of birth, and Social Security numbers.

34. Upon information and belief, the PII was not encrypted prior to the data breach.

35. Upon information and belief, the cyberattack was targeted at HALO as large employer that collects and maintains valuable personal, health, tax, and financial data from its current and former employees.

36. Upon information and belief, the cyberattack was expressly designed to gain access to private and confidential data, including (among other things) the PII of Plaintiff and the Class Members.

37. Beginning on or about March 28, 2024, HALO sent affected persons (including Plaintiff Bowser) a *Notice of Data Breach*, informing the recipients that their confidential data was involved.

38. HALO admitted in its *Notice of Security Incident* to the affected persons that their systems were subjected to unauthorized access in November 2023. HALO made no indication to either state Attorneys General or the Class Members that the exfiltrated PII was retrieved from the cybercriminals who took it.

39. In response to the Data Breach, HALO claims it has further secured their systems to protect the private information. HALO admits additional security was required, but there is no indication whether these steps are adequate to protect Plaintiff's and Class Members' PII going forward.

40. HALO had obligations created by contract, industry standards, common law, and representations made to its current and former employees to keep the PII of Plaintiff and Class

Members that was entrusted to HALO confidential, and to protect the PII from unauthorized access and disclosure.

41. Plaintiff and Class Members provided their PII to HALO with the reasonable expectation that HALO as a sophisticated company would comply with its duty and obligations and representations to keep such information confidential and secure from unauthorized access.

42. HALO failed to uphold its data security obligations to Plaintiff and Class Members. As a result, Plaintiff and Class Members are significantly harmed and will be at a high risk of identity theft and financial fraud for many years to come.

43. HALO did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining, causing Plaintiff's and Class Members' PII to be exposed.

Securing PII and Preventing Breaches

44. HALO could have prevented this Data Breach by properly encrypting or otherwise protecting their equipment and computer files containing PII.

45. In its notice letters, HALO acknowledged the sensitive and confidential nature of the PII. To be sure, collection, maintaining, and protecting PII is vital to virtually all of HALO's business purposes. HALO acknowledged through its conduct and statements that the misuse or inadvertent disclosure of PII can pose major privacy and financial risks to impacted individuals, and that under state law they may not disclose and must take reasonable steps to protect PII from improper release or disclosure.

The Ransomware Attack and Data Breach were Foreseeable Risks of which Defendant was on Notice

46. It is well known that PII, including Social Security numbers in particular, is an invaluable commodity and a frequent target of hackers.

47. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.[2]

48. Individuals place a high value not only on their PII, but also on the privacy of that data. For the individual, identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.

49. Individuals are particularly concerned with protecting the privacy of their social Security numbers, which are the "secret sauce" that is "as good as your DNA to hackers."

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

51. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack.

52. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite their own acknowledgment of its duties to keep PII private and secure, HALO failed to take appropriate steps to protect the PII of Plaintiff and the proposed Class from being compromised.

At All Relevant Times HALO Had a Duty to Plaintiff and Class Members to Properly Secure their Private Information

53. At all relevant times, HALO had a duty to Plaintiff and Class Members to properly secure their PII, encrypt and maintain such information using industry standard methods, train its employees, utilize available technology to defend its systems from invasion, act reasonably to

[2] https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last accessed April 12, 2024).

prevent foreseeable harm to Plaintiff and Class Members, and to *promptly* notify Plaintiff and Class Members when HALO became aware that their PII may have been compromised.

54. HALO's duty to use reasonable security measures arose as a result of the special relationship that existed between HALO, on the one hand, and Plaintiff and the Class Members, on the other hand. The special relationship arose because Plaintiff and the Members of the Class entrusted HALO with their PII when they were employees of HALO.

55. HALO had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite its obligation to protect such information. Accordingly, HALO breached its common law, statutory, and other duties owed to Plaintiff and Class Members.

56. Security standards commonly accepted among businesses that store PII using the internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;

c. Monitoring for suspicious or irregular traffic to servers;

d. Monitoring for suspicious credentials used to access servers;

e. Monitoring for suspicious or irregular activity by known users;

f. Monitoring for suspicious or unknown users;

g. Monitoring for suspicious or irregular server requests;

h. Monitoring for server requests for PII;

i. Monitoring for server requests from VPNs; and

j. Monitoring for server requests from Tor exit nodes.

57. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[3]

[3] 17 C.F.R. § 248.201 (2013).

The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[4]

58. The ramifications of HALO's failure to keep its Class Members' PII secure are long lasting and severe. Once PII is stolen, particularly dates of birth and Social Security numbers, fraudulent use of that information and damage to victims is likely to continue for years.

The Value of Personal Identifiable Information

59. PII of data breach victims 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.[5]

60. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[6]

61. PII can be used to distinguish, identify, or trace an individual's identity, such as their name and Social Security number. This can be accomplished alone, or in combination with other personal or identifying information that is connected or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.[7]

---

[4] *Id*.

[5] *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 April 12, 2024).

[6] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed April 12, 2024).

[7] *See* OFFICE OF MGMT. & BUDGET, OMB MEMORANDUM M-07-16 n. 1.

62. Given the nature of HALO's Data Breach, as well as the long delay in notification to Class Members, it is foreseeable that the compromised PII has been or will be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Plaintiff's and Class Members' PII may easily obtain Plaintiff's and Class Members' tax returns or open fraudulent credit card accounts in Class Members' names.

63. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, basic credit card information in a retailer data breach, because credit card victims can cancel or close credit and debit card accounts.[8] The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as dates of birth).

64. To date, HALO has offered its Class Members just twelve months of credit and identity protection services, even with the five-month delay from their discovery of the Data Breach to the production of the Notice Letters. The advice and services offered to victims in the Notice Letters is inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

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

HALO Failed to Comply with FTC Guidelines

66. Federal and State governments have established security standards and issued recommendations to lessen the risk of data breaches and the resulting harm to employees and institutions. The Federal Trade Commission ("FTC") has issued numerous guides for business

[8] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, Forbes, Mar 25, 2020, *available at*: https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1 (last accessed April 12, 2024).

highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[9]

67. 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.[10] The guidelines note businesses should protect the personal employee information that they keep, as well as properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.

68. The FTC recommends that companies verify that third-party service providers have implemented reasonable security measures.[11]

69. The FTC recommends that businesses:

a. Identify all connections to the computers where you store sensitive information.

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

c. Do not store sensitive data on any computer with an internet connection unless it is essential for conducting their business.

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

---

[9] Federal Trade Commission, *Start With Security, available at*: https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed April 12, 2024).

[10] Federal Trade Commission, *Protecting Personal Information: A Guide for Business, available at*: https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (last accessed April 12, 2024).

[11] FTC, *Start with Security*, *supra* note 34.

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

70. The FTC has brought enforcement actions against businesses for failing to protect employee data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential 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.

71. Because Class Members entrusted HALO with their PII directly or indirectly through HALO, HALO had, and has, a duty to the Class Members to keep their PII secure.

72. Plaintiff and the other Class Members reasonably expected that when they provide PII to HALO, that HALO would safeguard their PII.

73. HALO was at all times fully aware of its obligation to protect the personal data of its employees, including Plaintiff and members of the Classes. HALO was also aware of the significant repercussions if it failed to do so.

74. HALO's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential data—including Plaintiff's and Class Members' full names, Social Security numbers, and other highly sensitive and confidential information—constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

Plaintiff and Class Members Have Suffered Concrete Injury As A Result Of Defendant's Inadequate Security And The Data Breach It Allowed.

75. Plaintiff and Class Members reasonably expected that Defendant would provide adequate security protections for their PII, and Class Members provided Defendant with sensitive personal information, including their Social Security numbers.

76. Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to pay Defendant for services, Plaintiff and other reasonable Class Members understood and expected that their PII would be protected with data security, when in fact Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received services that were of a lesser value than what they reasonably expected. As such, Plaintiff and the Class Members suffered pecuniary injury.

77. Cybercriminals capture PII to exploit it; the Class Members are now, and for the rest of their lives will be, at a heightened risk of identity theft. Plaintiff has also incurred (and will continue to incur) damages in the form of, *inter alia*, loss of privacy and costs of engaging adequate credit monitoring and identity theft protection services.

78. The cybercriminals who obtained the Class Members' PII may exploit the information they obtained by selling the data in so-called "dark markets." Having obtained these names, contact information, Social Security numbers, and other PII, cybercriminals can pair the data with other available information to commit a broad range of fraud in a Class Member's name, including but not limited to:

a. obtaining employment;

b. obtaining a loan;

c. applying for credit cards or spending money;

d. filing false tax returns;

e. stealing Social Security and other government benefits; and

f. applying for a driver's license, birth certificate, or other public document.

79. In addition, if a Class Member's Private Information is used to create false identification for someone who commits a crime, the Class Member may become entangled in the criminal justice system, impairing the person's ability to gain employment or obtain a loan.

80. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Data Breach, Plaintiff and the other Class Members have been deprived of the value of their PII, for which there is a well-established national and international market.

81. Furthermore, PII has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes time for an information breach to be detected.[12]

82. Accordingly, Defendant's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiff and the other Class Members at an imminent, immediate, and continuing increased risk of identity theft and identity fraud.[13] Indeed, "[t]he level of risk is

[12] *Id.*

[13] *Data Breach Victims More Likely To Suffer Identity Fraud*, INSURANCE INFORMATION INSTITUTE BLOG (February 23, 2012), http://www.iii.org/insuranceindustryblog/?p=267 (last accessed April 12, 2024).

growing for anyone whose information is stolen in a data breach."[14] Javelin Strategy & Research, a leading provider of quantitative and qualitative research, notes that "[t]he theft of SSNs places consumers at a substantial risk of fraud."[15] Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that has not yet been exploited by cybercriminals bears a high risk that the cybercriminals who now possess Class Members' PII will do so at a later date or re-sell it.

83. As a result of the Data Breach, Plaintiff and Class Members have already suffered damages.

84. In its Notice Letter, Defendant represented to the Class Members and AGs that it initially discovered the Data Breach in November 2023, and admitted files were accessed and acquired by the cybercriminals. As EmiSoft, an award-winning malware-protection software company, states "[a]n absence of evidence of exfiltration should not be construed to be evidence of its absence, *especially during the preliminary stages of the investigation*."[16] It is likely that the cybercriminals did steal data and did so undetected.

85. In this case, according to Defendant's notification to the Class Members, cybercriminals had access to Class Members' data at least in November 2023, yet its notice letters about that Data Breach did not go out until March 28, 2024. This is tantamount to cybercriminals having a five-month head start on stealing the identities of Plaintiff and Class Members.

---

[14] Susan Ladika, *Study: Data Breaches Pose A Greater Risk*, CREDITCARDS.COM (July 23, 2014), http://www.creditcards.com/credit-card-news/data-breach-id-theft-risk-increase-study-1282.php (last accessed April 12, 2024).

[15] THE CONSUMER DATA INSECURITY REPORT: EXAMINING THE DATA BREACH- IDENTITY FRAUD PARADIGM IN FOUR MAJOR METROPOLITAN AREAS, (*available at* https://www.it.northwestern.edu/bin/docs/TheConsumerDataInsecurityReport_byNCL.pdf) (last accessed April 12, 2024).

[16] EmiSoft Malware Lab, *The chance of data being stolen in a ransomware attack is greater than one in ten* (EMISOFT BLOG July 13, 2020), https://blog.emsisoft.com/en/36569/the-chance-of-data-being-stolen-in-a-ransomware-attack-is-greater-than-one-in-ten/ (last accessed April 12, 2024, emphasis added)).

86. Accordingly, that Defendant has not found evidence of data being viewed is not an assurance that the data were not accessed, acquired, and stolen. Indeed, the likelihood that cybercriminals stole the data covertly is significant, likely, and concerning.

Plaintiff Bowser's Experience

87. On or about March 28, 2024, Ms. Mary Bowser, a citizen and resident of Dixon, Illinois, received Notice of Data Security Incident Letter by US. Mail.

88. As an employee of HALO, she provided her PII to HALO. She reasonably relied on HALO, to protect the security of her PII.

89. As a result of the Data Breach and the information that she received in the Notice Letter, Ms. Bowser has spent many hours dealing with the consequences of the Data Breach (closing and opening bank accounts, changing banks, changing passwords, and now self-monitoring the new bank and credit accounts), as well as her time spent verifying the legitimacy of the Notice of Data Breach, communicating with HALO representatives, communicating with her bank, exploring credit monitoring and identity theft insurance options, and signing up for the credit monitoring. Her time has been lost forever and cannot be recaptured.

90. As a result of the Data Breach, Ms. Bowser was the targeted victim of various phishing attempts.

91. Ms. Bowser is very careful about sharing her own personal identifying information and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

92. Ms. Bowser stores any and all documents containing PII in a secure location and destroys any documents she receives in the mail that contain any PII or that may contain any information that could otherwise be used to compromise her identity and credit card accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

93. Ms. Bowser suffered actual injury and damages due to HALO's mismanagement of her PII before the Data Breach.

94. Ms. Bowser suffered actual injury in the form of damages and diminution in the value of her PII—a form of intangible property that she entrusted to HALO, which was compromised in and as a result of the Data Breach.

95. Ms. Bowser suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach, and she has suffered extreme anxiety and increased concerns for the theft of her privacy since she received the Notice Letter. She is especially concerned about the theft of her full name paired with her date of birth and Social Security number.

96. Ms. Bowser has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her stolen PII, especially her Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

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

V. CLASS ALLEGATIONS

98. Plaintiff brings this nationwide class action on behalf of herself and on behalf of all others similarly situated.

99. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

> **All persons residing in the United States whose PII was compromised in the November 2023 data breach announced by HALO Branded Solutions, Inc. in March 2024. (the "Nationwide Class").**

100. Excluded from the Classes are the following individuals and/or entities: HALO Branded Solutions, Inc., and HALO's parents, subsidiaries, affiliates, officers and directors, and any entity in which HALO 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.

101. Plaintiff reserves the right to modify or amend the definition of the proposed class and any future subclass before the Court determines whether certification is appropriate.

102. **Numerosity – 735 ILCS 5/2-801(1)**: Member of the Classes are so numerous that joinder of all members is impracticable. HALO has identified and sent notice to over 7,300 persons whose PII may have been improperly accessed in the Data Breach, and the Classes are apparently identifiable within HALO's records.

103. **Commonality and Predominance – 735 ILCS 5/2-801(2)**: 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 HALO had a duty to protect the PII of Plaintiff and Class Members;
b. Whether HALO had respective duties not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;
c. Whether HALO had respective duties not to use the PII of Plaintiff and Class Members for non-business purposes;
d. Whether HALO failed to adequately safeguard the PII of Plaintiff and Class Members;
e. Whether and when HALO actually learned of the Data Breach;
f. Whether HALO adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;
g. Whether HALO violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;
h. Whether HALO failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

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

j. Whether HALO breached express or implied contracts – contracts of which Plaintiff and Class Members were third-party beneficiaries -- by failing to safeguard the PII of Plaintiff and Class Members;

k. Whether Plaintiff and Class Members are entitled to actual damages, nominal damages, and/or punitive damages as a result of HALO's wrongful conduct;

l. Whether Plaintiff and Class Members are entitled to restitution as a result of HALO's wrongful conduct, and;

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

104. Defendant engaged in a common course of conduct giving rise to the legal rights Plaintiff seeks to enforce, on behalf of herself and the other members of the Classes, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale in comparison, in both quality and quantity, to the numerous common questions that dominate this action. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

105. **Policies Generally Applicable to the Class**: This class action is also appropriate for certification because HALO 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 the Class Members, and making final injunctive relief appropriate with respect to the Class as a whole. HALO's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on HALO's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

106. **Adequacy of Representation – 735 ILCS 5/2-801(3):** Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that she has no disabling conflicts of interest that would be antagonistic to that of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages she has suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

107. **Superiority – 735 ILCS 5/2-801(4)**: 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 companies, like HALO. 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.

108. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because HALO would necessarily gain an unconscionable advantage since they 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.

109. The litigation of the claims brought herein is manageable. HALO'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.

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

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

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

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

113. Plaintiff restates and reallege all of the foregoing paragraphs as if fully set forth herein.

114. As a condition of being an employee of HALO, current and former employees are obligated to provide HALO with certain PII, including but not limited to, their name, date of birth, address, Social Security number, state-issued identification numbers, tax identification numbers, military identification numbers, and financial account numbers.

115. Plaintiff and Class Members entrusted their PII to HALO on the premise and with the understanding that HALO would safeguard their information, use their PII for legitimate business purposes only, and/or not disclose their PII to unauthorized third parties.

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

117. HALO knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII involved an unreasonable risk of harm to Plaintiff and Class Members, even if the harm occurred through the criminal acts of a third party.

118. HALO had a duty 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 HALO's security protocols to ensure that Plaintiff's and Class Members' information in HALO's possession was adequately secured and protected.

119. HALO also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's and Class Members' PII.

120. A breach of security, unauthorized access, and resulting injury to Plaintiff and Class Members was reasonably foreseeable, particularly in light of HALO's business as sophisticated, national company, for which the diligent protection of PII is a continuous forefront issue.

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

122. HALO's own conduct created a foreseeable risk of harm to Plaintiff and Class Members. HALO's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. HALO's misconduct also included its decisions not to comply with industry standards for the safekeeping of Plaintiff's and Class Members' PII, including basic encryption techniques freely available to HALO.

123. Plaintiff and Class Members had no ability to protect their PII that was in, and possibly remains in, HALO's possession.

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

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

126. HALO had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and Class Members.

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

128. HALO, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiff and Class Members during the time the PII was within HALO's possession or control.

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

130. These foregoing frameworks are existing and applicable industry standards in the industry, and Defendant failed to comply with these accepted standards thereby opening the door to the cyber incident and causing the data breach.

131. HALO improperly and inadequately safeguarded the PII of Plaintiff and Class Members in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

132. HALO failed to heed industry warnings and alerts to provide adequate safeguards to protect current and former employee PII in the face of increased risk of theft.

133. HALO, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of the PII.

134. HALO, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and Class Members the existence and scope of the Data Breach.

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

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

137. Additionally, 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 HALO, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of HALO's duty in this regard.

138. HALO 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. HALO's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and Class Members.

139. HALO's violation of Section 5 of the FTC Act constitutes negligence *per se*.

140. Plaintiff and Class members are within the class of persons that the FTC Act was intended to protect.

141. 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 Plaintiff and Class.

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

143. As a direct and proximate result of HALO's negligence, 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.

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

COUNT II
Unjust Enrichment
(On Behalf of Plaintiff and the Nationwide Class)

145. Plaintiff re-alleges and incorporate by reference paragraphs above as if fully set forth herein.

146. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including funds made as a result of the labor from Plaintiff and the Class Members.

147. As such, a portion of the revenue made as a result of the labor of Plaintiff and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

148. Plaintiff and Class Members conferred a monetary benefit on Defendant. In exchange, Plaintiff and Class Members should have received adequate data security protecting their Private Information.

149. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

150. Plaintiff and Class Members conferred a benefit on Defendant, a portion of which was to have been used for data security measures to secure Plaintiff's and Class Members' Personal Information, and by providing Defendant with their valuable Personal Information.

151. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid their data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

152. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money that should have been used on data security, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

153. Defendant acquired the monetary benefit and Personal Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

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

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

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

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

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

COUNT III
Breach of Express Contract
(On Behalf of Plaintiff and the Nationwide Class)

159. Plaintiff re-alleges and incorporates by reference the above paragraphs as if fully set forth herein.

160. This count is plead in the alternative to Count II (Unjust Enrichment) above.

161. Plaintiff and Class Members allege that they were the express, foreseeable, and intended beneficiaries of valid and enforceable express contracts between Defendant and its former and current employees, contract(s) that (upon information and belief) include obligations to keep sensitive PII private and secure.

162. Upon information and belief, these contracts included promises made by Defendant that expressed and/or manifested intent that the contracts were made to primarily and directly benefit the Plaintiff and the Class (all employees entering into the contracts), but also safeguarding the PII entrusted to Defendant in the process of providing these services.

163. Upon information and belief, Defendant's representations required Defendant to implement the necessary security measures to protect Plaintiff's and Class Members' PII.

164. Defendant materially breached its contractual obligation to protect the PII of Plaintiff and Class Members when the information was accessed and exfiltrated by unauthorized personnel as part of the Data Breach.

165. The Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

166. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release, disclosure of their PII, the loss of control of their PII, the present risk of suffering additional damages, and out-of-pocket expenses.

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

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

168. Plaintiff re-alleges and incorporates by reference the foregoing paragraphs as if fully set forth herein.

169. This count is plead in the alternative to Count II (Unjust Enrichment) above.

170. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth here.

171. Plaintiff and the Class Members entered into implied contracts with Defendant under which Defendant agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class Members that their information had been breached and compromised.

172. Plaintiff and the Class were required to and delivered their Private Information to Defendant as part of the employment process with Defendant.

173. Defendant solicited, offered, and invited Class Members to provide their PII as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their PII to Defendant.

174. Defendant accepted possession of Plaintiff's and Class Members' PII for the purpose of employing Plaintiff and Class Members.

175. In accepting, Plaintiff and the other Class Members entered into an implied contract with Defendant whereby Defendant became obligated to reasonably safeguard Plaintiff's and the other Class Members' PII.

176. In delivering their PII to Defendant, Plaintiff and Class Members intended and understood that Defendant would adequately safeguard the data as part of their employment.

177. The implied promise of confidentiality includes consideration beyond those pre-existing general duties owed under state of federal regulations. The additional consideration included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

178. The implied promises include but are not limited to: (1) taking steps to ensure that any agents who are granted access to PII also protect the confidentiality of that data; (2) taking steps to ensure that the information that is placed in the control of its agents is restricted and limited to achieve an authorized medical purpose; (3) restricting access to qualified and trained agents; (4) designing and implementing appropriate retention policies to protect the information against criminal data breaches; (5) applying or requiring proper encryption; (6) multifactor authentication for access; and (7) other steps to protect against foreseeable data breaches.

179. Plaintiff and the Class Members would not have entrusted their PII to Defendant in the absence of such an implied contract.

180. Had Defendant disclosed to Plaintiff and the Class that it did not have adequate computer systems and security practices to secure sensitive data, Plaintiff and the other Class Members would not have provided their Sensitive Information to Defendant.

181. Defendant recognized that Plaintiff's and Class Members' PII is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and the other Class Members.

182. Plaintiff and the other Class Members fully performed their obligations under the implied contracts with Defendant.

183. Defendant breached the implied contract with Plaintiff and the other Class Members by failing to take reasonable measures to safeguard their PII as described herein.

184. As a direct and proximate result of Defendant's conduct, Plaintiff and the other Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all Class Members, requests judgment against HALO Branded Solutions, Inc. and that the Court grant the following:

A. For an Order certifying the Nationwide Classes and appointing Plaintiff and her Counsel to represent the certified Nationwide Class;

B. For equitable relief enjoining HALO from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and the Class Members' PII, and from refusing to issue prompt, complete, any accurate disclosures to the Plaintiff and Class;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and the Class, including but not limited to an order:

i. prohibiting HALO from engaging in the wrongful and unlawful acts described herein;

ii. requiring HALO to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring HALO to delete, destroy, and purge the personal identifying information of Plaintiff and Class unless HALO can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and the Class;

iv. requiring HALO to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiff's and Class Members' personal identifying information;

v. prohibiting HALO from maintaining Plaintiff's and Class Members' personal identifying information on a cloud-based database;

vi. requiring HALO to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on HALO's systems on a periodic basis, and ordering HALO to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring HALO to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring HALO to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring HALO to segment data by, among other things, creating firewalls and access controls so that if one area of HALO's network is compromised, hackers cannot gain access to other portions of HALO's systems;

x. requiring HALO to conduct regular database scanning and securing checks;

xi. requiring HALO to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring HALO to conduct internal training and education routinely and continually, and on an annual basis to inform internal security personnel how

to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring HALO to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with HALO's policies, programs, and systems for protecting personal identifying information;

xiv. requiring HALO to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor HALO's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring HALO to meaningfully educate all class members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring HALO to implement logging and monitoring programs sufficient to track traffic to and from HALO's servers; and

xvii. for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate HALO's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment; and

D. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of punitive damages;

F. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

G. For prejudgment interest on all amounts awarded; and

H. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: April 16, 2024

Respectfully Submitted,

/s/ *Gary M. Klinger*
Gary M. Klinger
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878
Fax: (865) 522-0049
gklinger@milberg.com

Terence R. Coates (*pro hac vice* forthcoming)
Jonathan T. Deters (*pro hac vice* forthcoming)
MARKOVITS, STOCK & DEMARCO, LLC
119 E. Court Street, Suite 530
Cincinnati, OH 45202
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
jdeters@msdlegal.com

Attorneys for Plaintiff and the Proposed Class