FILED 12/13/2022 02:16 PM DEBORAH A. MYERS CLERK OF COURTS ASHLAND, OHIO
Case: 22-CIV-188

IN THE ASHLAND COUNTY COURT OF COMMON PLEAS
GENERAL DIVISION

LEON ALLEN, on behalf of himself and all others similarly situated,

208 Rae Court, Apt 15
Willard, OH 44890

Plaintiff,

v.

WENCO MANAGEMENT, LLC,

400 Claremont Ave, Ashland, OH 44805,

Defendant.

Case No.

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

INTRODUCTION

1. This case arises from a data breach. *See* Notice of Data Breach (Exhibit 1). Defendant Wenco Management, LLC is a franchisee of the Wendy's fast food chain. Wenco collects substantial amounts of personally identifying information (PII) regarding its employees, who have no choice but to trust Defendant to keep their PII secure.

2. In a story that has become all too familiar, an unauthorized third-party obtained access to Wenco's computer systems and stole PII belonging to its employees. Employees' data is now in the hands of criminals, leaving them vulnerable to identity theft. None of this would have occurred if Wenco had implemented reasonable data security measures.

3. Plaintiff Leon Allen is a victim of the data breach. He brings this action for damages and equitable relief on behalf of himself and all others similarly situated.

4. Allen and the Class are entitled to judgment in an amount exceeding $25,000. *See* CIV. R. 8(A).

PARTIES

5. Plaintiff Leon Allen is an employee of Wenco. He resides at 208 Rae Court, Apt 15, Willard, OH 44890.

6. Defendant Wenco Management, LLC is a private company with its principal place of business located at 400 Claremont Ave, Ashland, Ohio 44805.

JURISDICTION AND VENUE

7. Wenco is subject to this Court's personal jurisdiction because its principal place of business is (and at all relevant times was) located in Ashland, Ohio. The claims in this action arise directly from Wenco's decisions regarding data security, which were made from its Ohio headquarters. Those decisions resulted in the injuries sustained by Plaintiff and the Class. The exercise of jurisdiction over Wenco in Ohio would be fair and reasonable, and this Court and Ohio have a strong interest in adjudicating the claims here.

8. This Court has subject-matter jurisdiction under R.C. 2305.03 because this is a civil case in which the amount-in-controversy exceeds $15,000.

9. Venue is proper in the Scioto County Court of Common Pleas because the Defendant's principal place of business is located in this county and, on information and belief, Defendant's relevant acts and omissions occurred at its principal place of business. *See* CIV. R. 3(C)(2)–(3)

FACTUAL ALLEGATIONS

A. Wenco allowed criminals to steal class members' PII.

10. Wenco operates Wendy's restaurants in Michigan, Indiana, and Ohio.

11. Wenco collects substantial amounts of PII about its employees, including their names, social security numbers, and health plan information.

12. Hackers gained unauthorized access to Wenco's systems on August 21, 2022.

13. The hackers accessed Plaintiff's and the Class's PII, including their names, social security numbers, and even their health plan information.

14. Wenco claims that it is "enhancing existing security measures" in order "[t]o help prevent something like this from happening again." Exhibit 1. But a reasonable company would have implemented those enhancements in the first place. Wenco's failure to do so was negligent.

15. Wenco offered credit monitoring services to victims of the breach, thereby acknowledging that the victims are at an imminent and substantial risk of identity theft.

B. The data breach was highly foreseeable, yet Wenco failed to take reasonable precautions.

16. Given the type of data that Wenco collects and stores, it was highly foreseeable that bad actors would attempt to access the information.

17. "[H]ackers are likely to be drawn to databases containing information which has a high value on secondary black markets," such as "identifying and financial data." Mark Verstraete & Tal Zarsky, *Optimizing Breach Notification*, 2021 U. ILL. L. REV. 803, 854–55 (2021). Consequently, "relevant and rational firms should engage in greater security investment and reduced collection—all steps to limit the prospects of a potential breach and subsequent notification." *Id.* at 855.

18. 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.

19. Because Wenco collected and stored identifying and financial information that is very valuable to criminals, it was highly foreseeable that a bad actor would attempt to access that data.

20. Wenco collects and stores personally identifying and financial information. Therefore, the burden of implementing reasonable data security practices is minimal in comparison to the substantial and highly foreseeable risk of harm.

21. Criminals were only able to commit this data breach because Wenco failed to exercise reasonable care.

22. On information and belief, Wenco failed to adequately train its employees on basic cybersecurity protocols, including:

a. Effective password management and encryption protocols, including, but not limited to, the use of multi-factor authentication for all users;

b. Locking, encrypting and limiting access to computers and files containing sensitive information;

c. Implementing guidelines for maintaining and communicating sensitive data;

d. Protecting sensitive information, including personal and financial information, by implementing protocols on how to request and respond to requests for the transfer of such information and how to securely send such information through a secure file transfer system to only known recipients; and

e. Providing focused cybersecurity awareness training programs for employees.

23. The FTC has noted the need to factor data security into all business decision-making. *See Start With Security, A Guide for Business*, FTC (accessed June

9, 2022), https://bit.ly/3mHCGYz. According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; (5) using industry-tested and accepted methods for securing data; (6) monitoring activity on networks to uncover unapproved activity; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software. *Id.*

24. To that end, the FTC has issued orders against businesses that failed to employ reasonable measures to secure sensitive payment card data. *See In the matter of Lookout Services, Inc.*, No. C-4326, ¶ 7 (June 15, 2011) ("[Defendant] allowed users to bypass authentication procedures" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as employing an intrusion detection system and monitoring system logs."); *In the matter of DSW, Inc.*, No. C-4157, ¶ 7 (Mar. 7, 2006) ("[Defendant] failed to employ sufficient measures to detect unauthorized access."); *In the matter of The TJX Cos., Inc.*, No. C-4227 (Jul. 29, 2008) ("[R]espondent stored . . . personal information obtained to verify checks and process unreceipted returns in clear text on its in-store and corporate networks[,]" "did not require network administrators . . . to use different passwords to access different programs, computers, and networks[,]" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks . . ."); *In the matter of Dave & Buster's Inc.*, No. C-4291 (May 20, 2010) ("[Defendant] failed to monitor and filter outbound traffic from its networks to identify and block export of sensitive personal information without authorization" and "failed to use readily available security measures to limit access between

instore networks . . ."). These orders, which all preceded the data breach, further clarify the measures businesses must take to meet their data security obligations.

25. On information and belief, Defendant failed to adhere to the standard of care articulated by the FTC.

26. On information and belief, Defendant's use of outdated and insecure computer systems and software that are easy to hack, and their 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 thousands of members of the proposed Class to unscrupulous operators, con artists, and outright criminals.

27. Defendant violated its obligation to implement best practices and comply with industry standards concerning computer system security, which allowed class members' data to be accessed and stolen by criminals.

C. Plaintiff's PII was exposed in the data breach, which caused him to suffer legally cognizable injuries.

28. Plaintiff Leon Allen is a current employee of a Wenco Wendy's restaurant. He entrusted Wenco with his personally identifying and financial information as a condition of his employment.

29. Allen received a data breach notification informing him that his personally identifying information was accessed in the breach, including his name and social security number.

30. As a result of the data breach, Plaintiff suffered a loss of time, as he has spent and continues to spend a considerable amount of time on issues related to this Data Breach. In response to the data breach, Plaintiff has spent considerable

time monitoring his accounts and credit score. This is time that was lost and unproductive and took away from other activities and duties.

31. Plaintiff also suffered actual injury in the form of damages to, and diminution in, the value of his PII—a form of intangible property that he entrusted to Defendant—which was compromised in and as a result of the data breach.

32. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the data breach and has anxiety and increased concerns for the loss of his privacy.

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

34. Defendant continues to maintain Plaintiff's and class members' PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure. Plaintiff would not have entrusted his PII to Defendant had he known that it would fail to maintain adequate data security. Plaintiff's PII was compromised and disclosed as a result of the Data Breach.

35. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the data breach. As a result of the data breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

36. Because their personally identifying and financial information has been accessed by criminals, Plaintiff and the Class have suffered concrete and ongoing injuries.

37. Plaintiff and the Class are at an imminent and substantial risk of identity theft.

38. According to experts, one out of four data breach notification recipients become a victim of identity fraud. *Study Shows One in Four Who Receive Data Breach Letter Become Fraud Victims*, THREATPOST.COM (Feb. 21, 2013), https://bit.ly/3zB8Uwv.

39. 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. *See* Brian Stack, *Here's How Much Your Personal Information is Selling for on the Dark Web*, EXPERIAN (Dec. 15, 2017), https://bit.ly/2Ox2SGY.

40. 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.

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

42. One such example of criminals using PII for profit is the development of "Fullz" packages. "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record or more on the dark web. Fullz can be cashed out

(turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records For Sale in Underground Stolen From Texas Life Insurance Firm*, KREBS ON SECURITY (Sep. 18, 2014), https://bit.ly/3Qj2eJd.

43. Cyber-criminals can cross-reference two sources of PII to marry unregulated or partial data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete "Fullz" dossiers on individuals.

44. 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 likely what is already 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 other members of the proposed Class's stolen PII is being misused, and that such misuse is fairly traceable to the data breach.

45. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.

46. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."

47. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

48. In addition to out-of-pocket expenses that can exceed thousands of dollars for the victim of new account identity theft, and the emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by theft of their PII. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

49. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PII. To protect themselves, Plaintiff and the Class will need to be remain vigilant against unauthorized data use for years or even decades to come.

50. Moreover, the breach has diminished the value of Plaintiff and the Class's personal information.

51. The FTC has recognized that consumer data is a new and valuable form of currency. In a FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types

and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency." *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, FTC (Dec. 7, 2009), https://bit.ly/3xKfzmu.

52. Since it was included in the breach, Plaintiff and the Class's information has already been accessed by criminals, which decreases its value in the marketplace.

53. Therefore, the value of Plaintiff and the Class's personal information was reduced by the data breach.

54. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

55. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the damages that would result to Plaintiff and the Class.

56. None of those injuries would have occurred if Defendant had implemented reasonable data security practices.

CLASS ACTION ALLEGATIONS

57. Pursuant to CIV. R. 23, Plaintiff seeks certification of a class defined as follows:

> Every person whose information was compromised in the data breach that affected Wenco Management, LLC's systems on or about August 21, 2022.

58. Excluded from the Class are: (a) Defendant and its officers, directors, legal representatives, successors and wholly or partly owned subsidiaries or affiliated companies; (b) class counsel and their employees; and (c) the judicial officers and their immediate family members and associated court staff assigned to this case.

59. *Ascertainability.* The Class can be readily identified through Defendant's records; indeed, Defendant has already identified the class members and notified them of the breach. *Notice of Data Breach*, Exhibit 1.

60. *Numerosity.* Defendant reported to the United States Department of Health and Human Services that 20,526 individuals were affected by the data breach. Therefore, the Class is so numerous that individual joinder is impracticable.

61. *Typicality.* Plaintiff's claims are typical of the Class he seeks to represent. Like all class members, Plaintiff's personal information was exposed in the data breach as a result of Defendant's failure to implement reasonable data security measures. Thus, Plaintiff's claims arise out of the same conduct and are based on the same legal theories as those of the absent class members.

62. *Adequacy of Class Representative.* Plaintiff will fairly and adequately protect the interests of the Class. He is aware of his duties to absent class members and is determined to faithfully discharge his responsibility. Plaintiff's interests are aligned with (and not antagonistic to) the interests of the Class.

63. *Adequacy of Counsel.* In addition, Plaintiff has retained counsel with considerable experience in class action and other complex litigation, including data breach cases. Plaintiff's counsel have done substantial work in identifying and

investigating potential claims in this action, have knowledge of the applicable law, and will devote the time and financial resources necessary to vigorously prosecute this action. They do not have any interests adverse to the Class.

64. *Commonality and Predominance.* This case presents numerous questions of law and fact with answers common to the Class that predominate over questions affecting only individual class members. Those common questions include:

a. Whether Defendant had a duty to use reasonable care to safeguard Plaintiff and the Class's PII;

b. Whether Defendant breached the duty to use reasonable care to safeguard the Class's PII;

c. Whether Defendant knew or should have known about the inadequacies of its data security policies and system and the dangers associated with storing sensitive PII;

d. Whether Defendant failed to use reasonable care and commercially reasonable methods to safeguard and protect Plaintiff and the Class's PII from unauthorized release and disclosure;

e. Whether the proper data security measures, policies, procedures, and protocols were in place and operational within Defendant's computer systems to safeguard and protect Plaintiff and the Class's PII from unauthorized release and disclosure;

f. Whether the data breach was caused by Defendant's inadequate cybersecurity measures, policies, procedures, and protocols;

g. Whether Defendant took reasonable measures to determine the extent of the data breach after it was discovered;

h. Whether Defendant is liable for negligence, gross negligence, or recklessness;

i. Whether Defendant's conduct, practices, statements, and representations about the data breach of the PII violated applicable state laws;

j. Whether Plaintiff and the Class were injured as a proximate cause or result of the data breach;

k. Whether Plaintiff and the Class were damaged as a proximate cause or result of Defendant's breach of its contract with Plaintiff and the Class;

l. What the proper measure of damages is; and

m. Whether Plaintiff and the Class are entitled to restitutionary, injunctive, declaratory, or other relief.

65. *Superiority and Manageability*. A class action is superior to individual adjudications because joinder of all class members is impracticable, would create a risk of inconsistent or varying adjudications, and would impose an enormous burden on the judicial system. The amount-in-controversy for each individual class member is likely relatively small, which reinforces the superiority of representative litigation. As such, a class action presents far fewer management difficulties than individual adjudications, preserves the resources of the parties and the judiciary, and protects the rights of each class member.

CAUSES OF ACTION

Count 1: Negligence

66. Plaintiff realleges all previous paragraphs as if fully set forth below.

67. Plaintiff and members of the Class entrusted their PII to Defendant. Defendant owed to Plaintiff and other members of the Class a duty to exercise reasonable care in handling and using the PII in its care and custody, including by implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

68. Defendant owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard PII in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PII—just like the data breach that ultimately came

to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and members of the Class's PII by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

69. Defendant owed these duties to Plaintiff and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff's and members of the Class's personal information and PII.

70. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII.

71. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff and members of the Class and the importance of exercising reasonable care in handling it.

72. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII of Plaintiff and members of the Class which actually and proximately caused the Data Breach and Plaintiff's and members of the Class's injury.

73. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and members of the Class have suffered or will

suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

74. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

Count 2: Negligence Per Se

75. Plaintiff incorporates by reference all of the above allegations.

76. 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.

77. 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 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.

78. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect its employees' PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant had

collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to its employees in the event of a breach, which ultimately came to pass.

79. 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.

80. Defendant had a duty to Plaintiff and the members of the Class to implement and maintain reasonable security procedures and practices to safeguard Plaintiff and the Class's PII.

81. Defendant breached its 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.

82. Defendant's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitute negligence per se.

83. As a direct and proximate result of Defendant's negligence, Plaintiff suffered actual losses and damages.

PRAYER FOR RELIEF

84. Plaintiff, individually and on behalf of all others similarly situated, hereby demands:

a. Certification of the proposed Class;

b. Appointment of the undersigned counsel as class counsel;

c. An award of all damages, including attorneys' fees and reimbursement of litigation expenses, recoverable under applicable law and/or equity;

d. Restitution or disgorgement of all ill-gotten gains; and

e. Such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

85. Plaintiff demands a jury trial on all applicable claims.

Respectfully submitted,

By: /s/ *Jared W. Connors*

MEYER WILSON CO., LPA
Matthew R. Wilson (72925)
Email: mwilson@meyerwilson.com
Michael J. Boyle, Jr. (91162)
Email: mboyle@meyerwilson.com
Jared W. Connors (101451)
Email: jconnors@meyerwilson.com
305 W. Nationwide Blvd.
Columbus, Ohio 43215
Telephone: (614) 224-6000
Facsimile: (614) 224-6066

TURKE & STRAUSS LLP
Samuel J. Strauss (*pro hac vice* to be filed)
sam@turkestrauss.com
Raina Borrelli (*pro hac vice* to be filed)
raina@turkestrauss.com
613 Williamson St., #201
Madison, WI 53703
P: (608) 237-1775

Counsel for Plaintiff and the Proposed Class

ClassAction.org