**IN THE UNITED STATES DISTRICT COURT**
**FOR THE NORTHERN DISTRICT OF OKLAHOMA**

| | |
|---|---|
| 1. KATHY DEEVERS, individually and on behalf of all others similarly situated,<br><br>Plaintiff,<br><br>v.<br><br>1. WING FINANCIAL SERVICES LLC,<br><br>Defendant. | Case No: 22-cv-00550-CVE-JFJ<br><br>CLASS ACTION<br><br>JURY TRIAL DEMANDED |

# CLASS ACTION COMPLAINT

Plaintiff Kathy Deevers ("Plaintiff"), individually and on behalf of all others similarly situated, brings this Class Action Complaint and alleges the following against Defendant Wing Financial Services LLC ("Wing" or "Defendant"), based upon personal knowledge with respect to Plaintiff and upon information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters:

## NATURE OF THE ACTION

1. This class action arises out of the recent cyberattack and data breach (the "Data Breach") involving Wing, which collected and stored certain personally identifiable information ("PII") of the Plaintiff and the putative Class Members, all

of whom have PII on Wing Financial servers.

2. According to Wing, the PII compromised in the Data Breach "may have" included highly-sensitive information including but not limited to: names, addresses, dates of birth, unique biometric information, Social Security numbers, driver's license numbers or other state identification card numbers, individual tax identification numbers, passport numbers or other government ID, tax identification numbers, financial account numbers with access codes, payment card numbers, health insurance policy numbers, and medical treatment/history.

3. Social Security numbers are particularly valuable to criminals. This information can be sold and traded on the dark web black market. The loss of a Social Security number is particularly troubling because it cannot be easily changed and can be misused in a range of nefarious activities, such as filing fraudulent tax returns to steal tax refund payments, opening new accounts to take out loans, and other forms of identity theft.

4. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect consumers' PII. Inexplicitly, the Defendant has acknowledged that the cybersecurity attack occurred in August of 2022, but it has only recently begun contacting Class Members.

5. According to the Office of the Maine Attorney General, whom

Defendant was required to notice, the Data Breach has affected 240,772 individuals.[1]

6. Plaintiff brings this class action lawsuit on behalf of herself and all those similarly situated to address Defendant's inadequate safeguarding of Class Members' PII that they collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information was unsecured and left open to the unauthorized access of any unknown third party.

## PARTIES

7. Plaintiff Kathy Deevers is an adult individual and citizen of the State of Oklahoma who resides in Duncan, Oklahoma. Plaintiff previously received tax preparation services from Defendant and is one of its customers.

8. On December 1, 2022, Plaintiff was notified by Wing Financial via letter of the Data Breach and of the impact to her PII.

9. As a result of Defendant's conduct, Plaintiff suffered actual damages including, without limitation, time and expenses related to monitoring her financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, the lost value of their personal information, and other economic and non-economic harm. Plaintiff and Class Members will now be forced to expend additional time to review their credit reports and monitor their financial accounts

[1] https://apps.web.maine.gov/online/aeviewer/ME/40/266008e2-e657-41cb-a258-40357b43c24b.shtml (last accessed December 12, 2022).

and medical records for fraud or identify theft – particularly since the compromised information may include Social Security numbers.

10. Defendant Wing Financial is a financial services company with its principal place of business and headquarters at 2301 SE Washington Blvd, Bartlesville, OK 74006.

## JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over this controversy pursuant to 28 U.S.C. § 1332(d). The amount in controversy in this class action exceeds $5,000,000, exclusive of interest and costs, and there are numerous Class members who are citizens of states other than Defendant's state of citizenship.

12. This Court has personal jurisdiction over Defendant because it is authorized to and does conduct substantial business in this District, and is a citizen of this District by virtue of its headquarters and principal place of business being located in this District.

13. Venue is proper under 28 U.S.C. §1391(b) because the cause of action upon which the complaint is based arose in Bartlesville, Oklahoma, which is in the Northern District of Oklahoma.

## COMMON FACTUAL ALLEGATIONS

14. Plaintiff and the proposed Class are consumers of Wing. Wing Financial is a financial services company and is an independently owned and operated franchise of Jackson Hewitt, a tax-preparation service.[2]

15. As noted above, Plaintiff brings this class action against Defendant for Defendant's failure to properly secure and safeguard personally identifiable information, for failing to comply with industry standards to protect and safeguard that information, and for failing to provide timely, accurate, and adequate notice to Plaintiff and other members of the class that such information had been compromised.

### Wing Financial's Unsecure Data Management and Disclosure of Data Breach

16. Plaintiff and Class Members provided their PII to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

[2] https://www.jdsupra.com/legalnews/wing-financial-files-notice-of-data-7155203/ (last accessed December 12, 2022).

17. Plaintiff and Class Members' PII was provided to Defendant in conjunction with the type of work Defendant does within the financial services industry, as a franchise of tax-preparation company Jackson Hewitt.[3]

18. However, Wing Financial failed to secure the PII of the individuals that provided it with this sensitive information.

19. Wing Financial's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches preceding the date they disclosed the incident.

20. According to Wing, "certain client records were accessible to unauthorized parties on the internet" as discovered on August 7, 2022.[4] Wing Financial said that it "immediately limited access to the potentially affected systems and began gathering evidence relating to the incident."[5] In addition, it "communicated with the security and privacy professionals," and "hired independent computer forensic experts" to assist its investigation, and also "changed all of its user's login credentials."[6] Though the breach was discovered on August 7, 2022, Wing Financial reported to the Office of the Maine Attorney General that the breaches actually occurred anywhere from *September 2020 through January 2022*.[7]

---

[3] *See* n. 2.
[4] Exhibit A., "Notice Letter to the Office of the Maine Attorney General, dated December 1, 2022."
[5] *Id.*
[6] *Id.*
[7] *See* n.1.

21. Despite being aware of the breach in August of 2022, Wing Financial was not able to determine that the files exposed included PII until three months later, on November 10, 2022.[8] Wing Financial failed to take any action to notify Plaintiff or other class members of this breach until at least December 1, 2022.

22. Defendant failed to take appropriate or even the most basic steps to protect the PII of Plaintiff and other class members from being disclosed.

**Plaintiff and the Class Have Suffered Injury as a Result of Wing Financial's Data Mismanagement**

23. As a result of Defendant's failure to implement and follow even the most basic security procedures, Plaintiff's and Class Members' PII has been and is now in the hands of unauthorized individuals, which may include thieves, unknown criminals, banks, credit companies, and other potentially hostile individuals. Plaintiff and other Class Members now face an increased risk of identity theft, particularly due to the dissemination of their Social Security Number, and will consequentially have to spend, and will continue to spend, significant time and money to protect themselves due to Defendant's Data Breach.

24. Plaintiff and other class members have had their most personal, sensitive and PII disseminated to the public at large and have experienced and will continue to experience emotional pain and mental anguish and embarrassment.

[8] *See* Ex. A.

25. Plaintiff and Class members face an increased risk of identity theft, phishing attacks, and related cybercrimes because of the Data Breach. Those impacted are under heightened and prolonged anxiety and fear, as they will be at risk for falling victim for cybercrimes for years to come.

26. PII/PHI ("private health information") is a valuable property right.[9] The value of PII/PHI as a commodity is measurable.[10] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[11] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[12] It is so valuable to identity thieves that once PII/PHI has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

---

[9] *See* Marc van Lieshout, *The Value of Personal Data*, 457 IFIP ADVANCES IN INFORMATION AND COMMUNICATION TECHNOLOGY 26 (May 2015), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible...").

[10] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE (Apr. 28, 2014), http://www.medscape.com/viewarticle/824192 (last visited November 30, 2022).

[11] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD 4 (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[12] *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

27. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, Social Security numbers, PII/PHI, and other sensitive information directly on various Internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

28. Personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[13] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[14] All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[15] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[16] According to a report released by the

[13] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited November 30, 2022).
[14] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited November 30, 2022).
[15] Adam Greenberg, *Health insurance credentials fetch high prices in the online black market*, SC MAGAZINE (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market (last visited November 30, 2022).
[16] *In the Dark*, VPNOverview.com, 2019, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed on Nov. 30, 2022).

Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[17]

29. Criminals can use stolen PII/PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[18] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion . . . . By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[19]

30. Consumers place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[20]

---

[17] *See Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI CYBER DIVISION (Apr. 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.
[18] *See* n.8, *supra*.
[19] *Id.*
[20] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011), https://www.jstor.org/stable/23015560?seq=1.

31. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII/PHI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

32. Indeed, cyberattacks against the healthcare industry have been common for over ten years with the Federal Bureau of Investigation ("FBI") warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[21]

33. 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 prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals… because they often have lesser IT defenses and a high incentive to regain access to their data quickly.[22]

[21] Gordon M. Snow, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector (last visited November 30, 2022).

[22] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited November 30, 2022).

34. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[23]

35. Wing was on notice that the FBI has recently been concerned about data security regarding entities that store certain amounts of PHI, as Wing Financial does. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[24]

36. Plaintiff and members of the Class, as a whole, must immediately devote time, energy, and money to: 1) closely monitor their medical statements, bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing

[23] *See* Maria Henriquez, *Iowa City Hospital Suffers PIIshing Attack*, SECURITY MAGAZINE (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-PIIshing-attack (last visited November 30, 2022).

[24] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820 (last visited November 30, 2022).

attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

37. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff and Class members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of Wing Financial's conduct. Further, the value of Plaintiff's and Class members' PII has been diminished by its exposure in the Data Breach.

38. As a result of Wing Financial's failures, Plaintiff and Class Members are at substantial risk of suffering identity theft and fraud or misuse of their PII.

39. Plaintiff and the Class suffered actual injury from having PII compromised as a result of Wing Financial's negligent data management and resulting Data Breach including, but not limited to (a) damage to and diminution in the value of their PII, a form of property that Defendant obtained from Plaintiff; (b) violation of their privacy rights; and (c) present and increased risk arising from the identity theft and fraud.

40. For the reasons mentioned above, Wing Financial's conduct, which allowed the Data Breach to occur, caused Plaintiff and members of the Class these significant injuries and harm.

41. Plaintiff brings this class action against Defendant for Defendant's failure to properly secure and safeguard PII and for failing to provide timely, accurate, and adequate notice to Plaintiff and other class members that their PII had been compromised.

42. Plaintiff, individually and on behalf of all other similarly situated individuals, alleges claims in negligence, negligence per se, breach of implied contract, breach of fiduciary duty, unjust enrichment, and violation of the Oklahoma Consumer Protection Act. Do we also need to plead federal violation?

## CLASS ACTION ALLEGATIONS

43. Plaintiff brings this action on behalf of herself and on behalf of all other persons similarly situated pursuant to Rule 23(b)(2), (b)(3) and (c)(4) of the Federal Rules of Civil Procedure.

44. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> All persons in the United States whose PII was compromised in the Data Breach as disclosed by Wing Financial in or around December 1, 2022 (the "Nationwide Class").

45. Plaintiff proposes the following Subclass definition, subject to amendment as appropriate:

> All persons in the State of Oklahoma whose PII was compromised in the Data Breach as disclosed by Wing Financial

on December 1, 2022 (the "Oklahoma Subclass").

46. Excluded from the Classes are Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Classes are Members of the judiciary to whom this case is assigned, their families and Members of their staff.

47. Plaintiff hereby reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery. The proposed Classes meet the criteria for certification under Rule 23(a), 23(b)(2), 23(b)(3), and 23(c)(4).

48. Numerosity. The Members of the Classes are so numerous that joinder of all of them is impracticable. As noted above, there are at least 240,772 Members.

49. Commonality. There are questions of law and fact common to the Classes, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope

of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their PII;

f. Whether Defendant breached its duty to Class Members to safeguard their PII;

g. Whether computer hackers obtained Class Members' PII in the Data Breach;

h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Defendant's conduct was negligent;

j. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

k. Whether Defendant's acts breaching an implied contract they formed with Plaintiff and the Class Members;

l. Whether Defendant violated the Federal Trade Commission Act ("FTC

Act");

m. Whether Defendant violated the Health Insurance Portability and Accountability Act ("HIPAA");

n. Whether Defendant was unjustly enriched to the detriment of Plaintiff and the Class;

o. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and

p. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

50. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of every other Class Member, was compromised in the Data Breach.

51. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions, including data privacy litigation of this kind.

52. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, 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. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

53. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

54. Defendant has acted on grounds that apply generally to the Classes as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

55. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties'

interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and the Classes to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendant's data security practices were reasonable in light of best practices recommended by data security experts;

c. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

d. Whether Defendant failed to take commercially reasonable steps to safeguard consumer PII; and

e. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

56. Finally, all members of the proposed Classes are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. At least some Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

## CAUSES OF ACTION(

### COUNT I
### NEGLIGENCE

71. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

72. Wing Financial owed a duty to Plaintiff and all other Class members to exercise reasonable care in safeguarding and protecting their PII in its possession, custody, or control.

73. Wing Financial knew, or should have known, the risks of collecting and storing Plaintiff's and all other Class members' PII and the importance of maintaining secure systems. Wing Financial knew, or should have known, of the vast uptick in data breaches in recent years. Add Wing had a duty to protect PII.

74. Given the nature of Wing Financial's business, the sensitivity and value of the PII it maintains, and the resources at its disposal, Wing Financial should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring. Had a duty to prevent.

75. Wing breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and

hardware systems to safeguard and protect PII entrusted to it—including Plaintiff's and Class members' PII.

76. It was reasonably foreseeable to Wing Financial that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class members' PII to unauthorized individuals.

77. But for Wing Financial's negligent conduct or breach of the above-described duties owed to Plaintiff and Class members, their PII would not have been compromised.

78. As a result of Wing Financial's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and all other Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-

established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vii) actual or attempted fraud.

## COUNT II
## NEGLIGENCE PER SE

79. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

80. Wing Financial's duties arise from, in part due to its storage of certain medical information, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

81. Wing Financial's duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as Wing Financial, of failing to employ reasonable measures to protect and secure PII.

82. Wing Financial's duties further arise from the Health Insurance Portability and Accountability Act of 1996 (HIPAA), 42 U.S.C. § 1302(d), *et seq.*

83. Wing is an entity covered under HIPAA, which sets minimum federal standards for privacy and security of PHI.

84. Wing violated HIPAA Privacy and Security Rules and Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and all other Class members' PII/PHI and not complying with applicable industry standards. Wing Financial's conduct was particularly unreasonable given the nature and amount of PII/PHI it obtains and stores, and the foreseeable consequences of a data breach involving PII/PHI including, specifically, the substantial damages that would result to Plaintiff and the other Class members.

85. Wing Financial's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA constitutes negligence per se.

86. Plaintiff and Class members are within the class of persons that HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to protect.

87. The harm occurring as a result of the Data Breach is the type of harm HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to guard against.

88. It was reasonably foreseeable to Wing Financial that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies,

procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

89. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of Wing Financial's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA. Plaintiffs and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vi) actual or attempted fraud.

## COUNT III
## BREACH OF FIDUCIARY DUTY

90. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

91. Plaintiff and Class members either directly or indirectly gave Wing Financial their PII in confidence, believing that Wing Financial – a financial services

company – would protect that information. Plaintiff and Class members would not have provided Wing Financial with this information had they known it would not be adequately protected. Wing Financial's acceptance and storage of Plaintiff's and Class members' PII created a fiduciary relationship between Wing Financial and Plaintiffs and Class members. In light of this relationship, Wing Financial must act primarily for the benefit of its patients and health plan participants, which includes safeguarding and protecting Plaintiff's and Class members' PII.

92. Wing has a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of their relationship. It breached that duty by failing to properly protect the integrity of the system containing Plaintiff's and Class members' PII, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard the PII/PHI of Plaintiffs and Class members it collected.

93. As a direct and proximate result of Wing Financial's breaches of its fiduciary duties, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued

risk to their PII which remains in Wing Financial's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII compromised as a result of the Data Breach; and (vii) actual or attempted fraud.

## COUNT IV
## UNJUST ENRICHMENT

94. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein. This claim is pled in the alternative to the implied contract claim pursuant to Fed. R. Civ. P. 8(d).

95. Plaintiff and Class Members conferred a monetary benefit upon Wing Financial in the form of monies paid for healthcare services or other services.

96. Wing accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. Wing Financial also benefitted from the receipt of Plaintiff's and Class Members' PII.

97. As a result of Wing Financial's conduct, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiff and Class Members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

98. Wing should not be permitted to retain the money belonging to Plaintiffs and Class Members because Wing Financial failed to adequately

implement the data privacy and security procedures for itself that Plaintiff and Class members paid for and that were otherwise mandated by federal, state, and local laws. and industry standards.

99. Wing should be compelled to provide for the benefit of Plaintiff and Class Members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

## COUNT V
## BREACH OF IMPLIED CONTRACT

100. Plaintiff realleges and incorporates by reference all allegations of the preceding factual allegations as though fully set forth herein.

101. Defendant required Plaintiff and Class Members to provide, or authorize the transfer of, their PII in order for Wing Financial to provide services. In exchange, Defendant entered into implied contracts with Plaintiff and Class Members in which Defendant agreed to comply with its statutory and common law duties to protect Plaintiff's and Class Members' PII and to timely notify them in the event of a data breach.

102. Plaintiff and Class Members would not have provided their PII to Defendant had they known that Defendant would not safeguard their PII, as promised, or provide timely notice of a data breach.

103. Plaintiff and Class Members fully performed their obligations under their implied contracts with Defendant.

104. Defendant breached the implied contracts by failing to safeguard Plaintiff's and Class Members' PII and by failing to provide them with timely and accurate notice of the Data Breach.

105. The losses and damages Plaintiff and Class Members sustained (as described above) were the direct and proximate result of Defendant's breach of its implied contracts with Plaintiffs and Class Members.

## COUNT VI
## VIOLATION OF THE OKLAHOMA CONSUMER PROTECTION ACT
## 15 Okla. Stat. Ann. § 751, *et. seq.*
## (On Behalf of the Oklahoma Subclass)

106. Plaintiff realleges and incorporates by reference all preceding allegations as though fully set forth herein.

107. Plaintiff brings this cause of action individually and on behalf of the members of the Oklahoma Subclass.

108. The Oklahoma Consumer Protection Act was created to protect Oklahoma consumers from unfair methods of competition and unfair or deceptive business practices.

109. Plaintiff and the Oklahoma Subclass contracted with Wing Financial for financial services. As part of their transaction, Wing Financial collected and stored PII/PHI.

110. Wing Financial has its principal place of business and headquarters in Oklahoma, and otherwise engaged in trade or commerce, or conducted business, in Oklahoma.

111. As set forth more fully above, Wing Financial collected consumers' PII/PHI as a part of their doing business. While selling and profiting from its services, Wing Financial failed to adequately maintain safeguards to protect individuals' PII/PHI. Wing Financial concealed this material information from consumers because to do otherwise would have resulted in consumers seeking other businesses or Wing Financial's competitors for the same services by virtue of Wing Financial's data security policies.

112. Wing Financial's conduct constituted, among other things, the following prohibited fraudulent, deceptive, and unfair business practices: (a) misrepresenting that Wing Financial's data security policy has characteristics, ingredients, uses, or benefits, which it does not have; and (b) engaging in fraudulent and deceptive conduct that creates a likelihood of confusion and misunderstanding.

113. Wing Financial's conduct was fraudulent and deceptive because the omissions created a likelihood of confusion and misunderstanding and had the capacity or tendency to deceive and, in fact, did deceive, ordinary consumers, including Oklahoma Plaintiffs. Ordinary consumers, including Oklahoma Plaintiffs, would have found it material to their choice in services to know that Wing

Financial's data security policies were inadequate and that Wing Financial would be collecting PII/PHI that was at serious risk of unauthorized access. Knowledge of those facts would have been a substantial factor in Oklahoma Plaintiffs', as well as Oklahoma Subclass members', decision to contract with Wing Financial.

114. Wing Financial's conduct actually and proximately caused an ascertainable loss of money or property to Oklahoma Plaintiffs (as set forth above) and members of the Oklahoma Subclass. Absent Wing Financial's unfair, deceptive, and/or fraudulent conduct, Oklahoma Plaintiffs and Oklahoma Subclass members would have behaved differently and would not have contracted with Wing Financial. Wing Financial's omissions induced Oklahoma Plaintiffs and Oklahoma Subclass members to contract for services with Wing Financial that they would have otherwise used another entity for.

115. Accordingly, pursuant to the aforementioned statutes, Oklahoma Plaintiffs and Oklahoma Subclass members are entitled to recover their actual damages, which can be calculated with a reasonable degree of certainty using sufficiently definitive and objective evidence. Those damages are: time and expenses related to monitoring their financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, the lost value of their personal information, and other economic and non-economic harm. In addition, given the nature of Wing Financial's conduct, Oklahoma Plaintiffs and Oklahoma

Subclass members are entitled to recover all available statutory, exemplary, treble, and/or punitive damages, costs of suit, and attorneys' fees based on the amount of time reasonable expended and equitable relief necessary, and all such other relief as the Court deems proper.

## PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Classes, pray for judgment as follows:

a. For an Order certifying this action as a class action and appointing Plaintiff and her counsel to represent the Class and Subclass;

b. For equitable relief enjoining Wing Financial from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII;

c. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Data Breach;

d. For an order requiring Defendant to pay for not less than seven years of credit monitoring services for Plaintiff and the Class(es);

e. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

f. For an award of punitive damages, as allowable by law;

g. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

h. Pre and post-judgment interest on any amounts awarded; and

i. Such other and further relief as this court may deem just and proper.

**JURY TRIAL DEMANDED**

Plaintiff demands a trial by jury on all claims so triable.

Dated: December 19, 2022

Respectfully Submitted By:

**FEDERMAN & SHERWOOD**

*/s/ William B. Federman*
William B. Federman
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
T: (405) 235-1560
F: (405) 239-2112
wbf@federmanlaw.com

**SHUB LAW FIRM LLC**

Jonathan Shub*
Benjamin F. Johns*
134 Kings Hwy E., Fl. 2,
Haddonfield, NJ 08033
T: (856) 772-7200
F: (856) 210-9088
jshub@shublawyers.com
bjohns@shublawyers.com

*Attorneys for Plaintiff and the Proposed Class*

**Pro Hac Vice Forthcoming*