☐ YES ☐ NO

EXHIBITS

CASE NO. 22 Ch 6132

DATE: 6-24-22

CASE TYPE: Class Action

PAGE COUNT: 25

CASE NOTE

12-Person Jury

IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
COUNTY DEPARTMENT, CHANCERY DIVISION

MARIA FLORES, individually and on behalf of all others similarly situated, Plaintiff, v. AON CORPORATION, Defendant.	2022CH06132 Case No. CLASS ACTION JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Maria Flores brings this action on behalf of herself, and all others similarly situated against Defendant, Aon Corporation ("Aon" or "Defendant"), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities, and alleges as follows:

INTRODUCTION

1. Starting in late December 2020, global insurance provider Aon, with U.S. headquarters in Chicago, Illinois, lost control over consumers' highly sensitive personal information in a data breach ("Data Breach"), and then failed to start notifying the public about the breach for nearly a year and a half. When Aon finally announced the Data Breach in May of 2022, it deliberately underplayed the breach's severity and misrepresented that it had no evidence cybercriminals had copied, retained, or shared the data, even though Aon knew cybercriminals had accessed its files for an extended period.

2. On information and belief, cybercriminals bypassed Aon's inadequate security systems to access consumers' personally identifiable information ("PII") in its insurance files,

including their names, addresses, dates of birth, Social Security numbers, drivers' license information and, in some cases, benefit-enrollment information. Upon information and belief, the PII of these consumers' beneficiaries were also compromised in the Data Breach.

3. On or around February 25, 2022, Aon's investigation confirmed the unauthorized access to its consumers' PII and that the cybercriminals had such access between December 2020 and late February 2022.

4. Still, Aon did not immediately notify consumers about the breach, nor would it do so for another three months—until May 2022.

5. On information and belief, Aon lacked the security necessary to prevent such a hack or stop it before hackers could steal victims' PII. What's more, Aon neglected to tell consumers about the hack in a timely manner.

6. By letter dated May 27, 2022, Aon finally began informing consumers of the Data Breach, offering only 24 months of free credit-monitoring services to breach victims despite the significant PII that was compromised over a two-year period.

7. Aon publicly announced the data breach stating it did not have "a significant impact" on its own operations. However, the same cannot be said for the victims, whose PII was exposed to cybercriminals.

8. For approximately six years, Plaintiff Flores' employer has used Aon to administer its employee benefits. Plaintiff's PII was thus impacted in the Data Breach.

9. Plaintiff Flores received a copy of the breach notification letter in June 2022.

10. After receiving a copy of the Breach Notice, Plaintiff Flores devoted significant time and resources in dealing with the Data Breach's impact on her.

11. Aon is well-versed in the dangers of cyber-security breaches as it offers cyber insurance policies and related solutions to its customers, including Cyber Risk Financing, Cyber Impact Analysis, Security Testing, Incident Response Retainers and Stroz Friedburg Digital Forensics.

12. Aon's failures to adequately protect consumers' PII and timely notify them about the devastating Data Breach harmed consumers in violation of Illinois law.

PARTIES

13. Plaintiff Maria Flores is a natural person and Illinois citizen, residing in Chicago, Illinois, where she intends to remain. Ms. Flores is a Data Breach victim.

14. Defendant Aon is a publicly traded global corporation that is incorporated in Delaware and maintains its U.S. headquarters at 200 E. Randolph Street, Aon Center floors 3-15, Chicago, IL 60601.

JURISDICTION & VENUE

15. This Court has subject-matter jurisdiction over this action under Ill. Const. art. VI, § 9.

16. This Court has general personal jurisdiction over Aon under 735 ILCS § 5/2-209 because it is incorporated under the laws of Delaware and headquartered in Illinois.

17. Venue is proper in this Court under 735 ILCS § 5/2-101(2) because some part of the transactions out of which the cause of action arose occurred in Cook County. Specifically, Plaintiff Flores' injuries arising out of the Data Breach occurred in, and were felt in, Cook County.

BACKGROUND FACTS

18. Aon is a global insurance company providing commercial risk, health, retirement and reinsurance solutions in over 120 countries.

19. Upon information and belief, Aon manages highly sensitive PII of consumers through its many insurance offerings.

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

21. This is the case despite the fact that Aon's insurance offerings include numerous cybersecurity-related insurance products.

22. In fact, Aon has published articles on its website describing the well-known risks of cyberattacks and counseling business on how to safeguard their data, acknowledging the rising trend in data breaches and the risks they pose to business and consumers.[1]

23. Aon was also aware that "many breaches result from a lack of employee awareness of the IT security risks their actions online, on social media, at work and at home have."[2] However, despite this knowledge, Aon failed to take reasonable actions to prevent the Data Breach and, instead, left Plaintiff's and Class members' PII vulnerable to a lengthy cyberattack that went undetected by Aon for years.

[1] https://www.aon.com/cyber-solutions/thinking/preparing-for-the-expected-cyber-incidents-data-breaches/ (last accessed June 22, 2022).
[2] https://www.aon.com/cyber-solutions/solutions/cyber-awareness-training/ (last accessed June 22, 2022).

Aon Fails to Safeguard Consumers' PII

24. Plaintiff and the proposed Class are consumers whose PII was maintained in Aon's files and systems.

25. Aon collects and maintains PII in its systems for purposes of offering insurance and other products to its customers.

26. In collecting and maintaining consumers' PII, Aon implicitly agrees it will safeguard the data using reasonable means according to its internal policies and state and federal law.

27. Despite its duties to safeguard PII, in late December 2020, cybercriminals bypassed Aon's inadequate security systems undetected and accessed consumer confidential information.

28. However, it was not until February 25, 2022 that Aon finally identified that cybercriminals had breached its systems and accessed consumers' PII.

29. Aon's Breach Notice states that "an unauthorized third party accessed certain Aon systems at various times between December 29, 2020, and February 26, 2022." It also states that "[f]indings from the investigation indicate the unauthorized third party temporarily obtained certain documents containing personal information from Aon systems." Ex. A.

30. Despite the devastating nature of the Data Breach and the admission that documents containing consumers' PII were not only accessed, but "obtained" by cybercriminals, Aon did not immediately inform affected consumers about the breach or otherwise notify them according to Illinois law. Instead, Aon initiated an internal investigation with "leading cybersecurity firms," and it has failed to provide key details about the Data Breach to those impacted.

31. On or around May 27, 2022, Aon finally issued notice of the Data Breach. Ex A.

32. The Breach Notice reveals little about the breach and says Aon has no indication that the third party "further copied, retained, or shared any of the data."

33. On information and belief, Aon failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over consumer PII. Aon's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing PII.

Plaintiff Flores' Experience

34. Plaintiff Flores obtains certain employee-related benefits through her employer. Plaintiff's employer uses Aon to administer these employee benefits. Therefore, by virtue of Plaintiff's participation in employer-offered benefits, Aon maintained Plaintiff's PII in its system.

35. Plaintiff Flores provided her PII to Aon and trusted Aon would use reasonable measures to protect it according to Aon's internal policies, as well as state and federal law.

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

Plaintiff and the Proposed Class Face Significant Risk of Identity Theft

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

38. The ramifications of Aon's failure to keep Plaintiff's and the Class's PII secure are severe. Identity theft occurs when someone uses another's personal and financial information such

as that person's name, account number, Social Security number, driver's license number, date of birth, or other information, without permission, to commit fraud or other crimes.

39. As a result of Aon's failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered, or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost-opportunity costs and lost wages associated with the time and effort expended addressing and trying to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in the possession of Aon and is subject to further breaches so long as Aon fails to undertake the appropriate measures to protect the PII in its possession.

40. 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.[3]

41. 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.

42. It can take victims years to stop identity or PII theft, giving criminals time to sell that information for cash.

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

44. Cybercriminals can cross-reference multiple sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.[4]

45. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff 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 cybercriminals in the Data Breach, criminals can easily create a Fullz package and

---

[3] *See* Here's How Much Your Personal Information Is Selling for on the Dark Web, Experian, https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited June 22, 2022).

[4] *Id.*

sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and other members of the proposed Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

46. Defendant disclosed the PII of Plaintiff and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiff and members of the proposed Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (*i.e.*, identity fraud), all using the stolen PII.

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

48. Defendant's failure to properly notify Plaintiff and members of the proposed Class of the Data Breach exacerbated Plaintiff's and members of the proposed Class's injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

Aon Failed to Adhere to FTC Guidelines

49. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous

guidelines identifying best data security practices that businesses, such as Aon, should employ to protect against the unlawful exposure of Personal Information.

50. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

51. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

52. The FTC recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

53. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

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

CLASS ACTION ALLEGATIONS

55. Plaintiff Flores brings this action individually and on behalf of the following Class: All persons residing in the state of Illinois whose PII was compromised in the Aon Data Breach (the "Class").

56. Excluded from the Class are counsel for any Party, Aon, any entities in which Aon has a controlling interest, any judge to whom this action is assigned, and any member of such judge's staff and immediate family.

57. The Class defined above is identifiable through Aon's business records.

735 ILCS § 5/2-801(1) Numerosity

58. There are thousands of potential Class members.

59. Individual joinder of these persons is impracticable.

60. Plaintiff Flores is a member of the Class.

735 ILCS § 5/2-801(2) Commonality & Predominance

61. There are questions of law and fact common to Plaintiff and to the proposed Class, including but not limited to the following:

a. Whether Aon had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII;

b. Whether Aon 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 Aon was negligent in maintaining, protecting, and securing PII;

d. Whether Aon breached contract promises to safeguard Plaintiff's and the Class's PII;

e. Whether Aon took reasonable measures to determine the extent of the Data Breach after discovering it;

f. Whether Aon's Breach Notice was reasonable;

g. Whether the Data Breach caused Plaintiff and the Class's injuries;

h. What the proper damages measure is;

i. Whether Aon violated the statutes alleged in this Complaint; and

j. Whether Plaintiff and the Class are entitled to damages, treble damages, and/or injunctive relief.

62. Common questions of law and fact predominate over questions affecting only individual class members, and a class action is the superior method for fair and efficient adjudication of the controversy.

63. Plaintiff's claims are typical of the claims of members of the Class.

735 ILCS 5/2-801(3) Adequacy

64. Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the Class, she will fairly and adequately protect the interests of the Class, and she is represented by counsel skilled and experienced in class actions.

735 ILCS 5/2-801(4) Appropriateness

65. The likelihood that individual members of the Class will prosecute separate actions is remote due to the time and expense necessary to prosecute an individual case.

66. Plaintiff is not aware of any litigation concerning this controversy already commenced by others who meet the criteria for class membership described above.

FIRST CLAIM FOR RELIEF
Negligence
(On Behalf of Plaintiff and the Class)

67. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

68. 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, retaining, and using the PII in its care and custody, including 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.

69. Defendant owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard their PII in accordance with state-of-the-art industry standards for 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 allowing access to consumers' PII to unknown third parties and by failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who made that happen.

70. Defendant owed to Plaintiff and members of the Class a duty to notify them within a reasonable time frame of any breach to the security of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and occurrence of the Data Breach. These duties are required and necessary for Plaintiff and members of the Class to take appropriate measures to protect their PII, to be vigilant in the face of an

increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

71. 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 PII for purpose of providing insurance services to its customers. Plaintiff and members of the Class needed to provide their PII to Defendant in order to obtain certain insurance benefits. Defendant negligently maintained this information.

72. The risk that unauthorized persons would try 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 try to access Defendant's databases containing the PII—whether by malware or otherwise.

73. 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.

74. 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. These failures actually and proximately caused the Data Breach and Plaintiff's and members of the Class's injury.

75. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and members of the Class, which actually and proximately caused

and exacerbated the harm from the Data Breach and Plaintiff's and members of the Class's injuries-in-fact.

76. As a direct and traceable result of Defendant's negligence or negligent supervision, Plaintiff and members of the Class have suffered or will suffer damages, including but not limited to monetary damages, loss of privacy, lost time, loss of value of PII, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress, entitling them to damages in an amount to be proven at trial.

77. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff's and members of the Class's 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.

SECOND CLAIM FOR RELIEF
Negligence Per Se
(On Behalf of Plaintiff and the Class)

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

79. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant has a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and members of the Class's PII.

80. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff and the members of the Class's sensitive

PII. 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 consumers' PII.

81. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect its consumers' PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to its customers in the event of a breach, which ultimately came to pass.

82. 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.

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

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

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

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

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

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

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

THIRD CLAIM FOR RELIEF
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

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

91. Defendant provided insurance benefits to Plaintiff and members of the Class on the condition that Plaintiff and members of the Class provide Defendant with their PII.

92. In turn, and through internal policies, Defendant agreed it would not disclose the PII it collects to unauthorized persons.

93. Plaintiff and the members of the Class accepted Defendant's offer by providing PII to Defendant in exchange for insurance-related services.

94. Implicit in the parties' agreement was that Defendant would maintain Plaintiff's and the Class's PII using reasonable security measures and that Defendant would provide Plaintiff and members of the Class with prompt and adequate notice of all unauthorized access and/or theft of their PII.

95. Plaintiff and the members of the Class would not have entrusted their PII to Defendant in the absence of such agreement with Defendant.

96. Defendant materially breached the contracts it had entered with Plaintiff and members of the Class by failing to safeguard such information and failing to notify them promptly of the intrusion into its computer systems that compromised such information. Defendant also breached the implied contracts with Plaintiff and members of the Class by:

a. Failing to properly safeguard and protect Plaintiff's and members of the Class's PII;

b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement; and

c. Failing to ensure the confidentiality and integrity of electronic PII that Defendant created, received, maintained, and transmitted.

97. The damages sustained by Plaintiff and members of the Class as described above were the direct and proximate result of Defendant's material breaches of its agreement(s).

98. Plaintiff and members of the Class have performed under the relevant agreements, or such performance was waived by the conduct of Defendant.

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

100. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

101. Defendant failed to advise Plaintiff and members of the Class of the Data Breach promptly and sufficiently.

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

103. Plaintiff and members of the Class have sustained damages because of Defendant's breaches of its agreement, including breaches of it through violations of the covenant of good faith and fair dealing.

104. Plaintiff, on behalf of themselves and the Class, seek compensatory damages for breach of implied contract, which includes the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

FOURTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of the Plaintiff and the Class)

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

106. This claim is plead in the alternative to the breach of implied contractual duty claim.

107. Plaintiff and members of the Class conferred a benefit upon Defendant in the form of payment of premiums for Defendant's insurance products and services. Defendant also benefited from the receipt of Plaintiff's and members of the Class's PII, including because such PII was used to purchase insurance through Defendant.

108. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiff and members of the Class.

109. Under principals of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and the proposed Class's payments and their PII because Defendant failed to adequately protect their PII. Plaintiff and the proposed Class would not have provided their PII to Aon had they known Aon would not adequately protect their PII.

110. Defendant should be compelled to disgorge into a common fund to benefit Plaintiff and members of the Class all unlawful or inequitable proceeds received by it as a result of the conduct and Data Breach alleged here.

FIFTH CLAIM FOR RELIEF
Violation of Illinois Consumer Fraud and Deceptive Business Practices Act
815 ILCS § 505/1, *et seq.*
(On Behalf of Plaintiff and the Class)

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

112. The Illinois Personal Information Protection Act ("IPIPA"), 815 ILCS § 530/20 provides that a violation of that statute constitutes an unlawful practice under the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS § 505/1, *et seq.* ("ICFA"), which prohibits unfair and deceptive acts or practices in the conduct of trade and commerce.

113. Defendant is a "data collector" under IPIPA. As a data collector, Defendant owns or licenses information concerning Illinois resident.

114. The IPIPA requires a data collector that "maintains or stores . . . records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, . . . use, . . . or disclosure." IPIPA, 815 ILCS § 530/45(a).

115. The IPIPA further requires that data collectors "notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach. The disclosure notification shall be made in the most *expedient* time possible and *without unreasonable delay*, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system." IPIPA, 815 ILCS § 530/10(a) (emphasis added).

116. As alleged above, Defendant violated the IPIPA by failing to implement and maintain reasonable security measures to protect Plaintiff's and the Class's PII. Defendant further violated the IPIPA by failing to give Plaintiff and the Class expedient notice of the Data Breach without unreasonable delay.

117. As a direct and proximate cause of Defendant's failures, Plaintiff and the Class have suffered actual damages.

118. Plaintiff, on behalf of herself and the Class seeks compensatory damages for breach of the IPIPA and the ICFA, which includes the costs of future monitoring of their credit history for identity theft and fraud, plus attorneys' fees, prejudgment interest, and costs.

SIXTH CLAIM FOR RELIEF
Invasion of Privacy
(On Behalf of the Plaintiff and the Class)

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

120. Plaintiff and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

121. Defendant owed a duty to its customers, including Plaintiff and the Class, to keep this information confidential.

122. The unauthorized acquisition (*i.e.*, theft) by a third party of Plaintiff's and Class Members' PII is highly offensive to a reasonable person.

123. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and the Class disclosed their sensitive and confidential information to Defendant as part of their purchase of insurance products and services, but they did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

124. The Data Breach constitutes an intentional interference with Plaintiff's and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

125. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

126. Defendant acted with a knowing state of mind when it failed to notify Plaintiff and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

127. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

128. As a proximate result of Defendant's acts and omissions, the private and sensitive PII of Plaintiff and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages.

129. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class because their PII are still maintained by Defendant with its inadequate cybersecurity system and policies.

130. Plaintiff and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the PII of Plaintiff and the Class.

131. In addition to injunctive relief, Plaintiff, on behalf of themselves and the other members of the Class, also seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

PRAYER FOR RELIEF

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

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing her counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Aon from further deceptive and unfair practices and making untrue statements about the Data Breach and the stolen PII;

E. Awarding Plaintiff and the Class damages that include compensatory, exemplary, punitive damages, and statutory damages, including pre- and post-judgment interest, in an amount to be proven at trial;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

I. Granting such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

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

Dated: June 24, 2022

Respectfully submitted,

By: */s/ Kenneth A. Wexler*

Kenneth A. Wexler
Bethany R. Turke
Eaghan S. Davis
WEXLER BOLEY & ELGERSMA LLP
55 West Monroe St., Suite 3300
Chicago, IL 60603
Telephone:(312) 346-2222

Facsimile:(312) 346-0022
kaw@wbe-llp.com
brt@wbe-llp.com
esd@wbe-llp.com
Firm ID:99616

Samuel J. Strauss
sam@turkestrauss.com
Raina C. Borrelli
raina@turkestrauss.com
Alex Phillips
alexp@turkestrauss.com
TURKE & STRAUSS LLP
613 Williamson St., Suite 201
Madison, WI 53703
Telephone (608) 237-1775
Facsimile: (608) 509-4423

Attorneys for Plaintiff and the Proposed Class

ClassAction.org