UNITED STATES DISTRICT COURT FOR SOUTHERN DISTRICT OF INDIANA INDIANAPOLIS DIVISION

CYNTHIA CASTANEDA, individually and on behalf of all others similarly situated, Plaintiff, v. ARDAGH GLASS, INC., Defendant	)	Case No. 1:23-cv-02214 JURY TRIAL DEMANDED

AMENDED CLASS ACTION COMPLAINT

Plaintiff Cynthia Castaneda ("Plaintiff") brings this action on behalf of herself, and all others similarly situated against Defendant, Ardagh Glass, Inc., ("Ardagh" or "Defendant"), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities, and alleges as follows:

SUMMARY OF THE CASE

1. Between April 23, 2021, and May 19, 2021, Ardagh, a subsidiary to a worldwide container manufacturing corporation, lost control over its current and former employees' highly sensitive personal information in a data breach perpetrated by cybercriminals ("Data Breach").

2. On information and belief, the Data Breach was not discovered by Defendant until May 2, 2021, and appallingly, even after discovery of the Breach, Defendant continued allowing cybercriminals unfettered access to its network and Plaintiff's and the Class's personal information for another seventeen days.

3. Following an internal investigation, Defendant learned cybercriminals had gained unauthorized access to employees' personally identifiable information ("PII") including but not limited to their names, driver's license, Social Security number, and financial account information.

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

5. Despite learning as early as October 2021 that cybercriminals had posted Plaintiff's and the Class's PII onto the dark web for theft and sale by other cybercriminals, Defendant would not notify Class Members about the Data Breach ("Breach Notice") until July 5, 2022, an appalling fourteen months after the Data Breach first began. An example of the Breach Notice is attached as **Exhibit A.**

6. Defendant's Breach Notice obfuscated the nature of the breach and the threat it posed—refusing to tell its employees how many people were impacted, how the breach happened, or why it took the Defendant over a year to begin notifying victims that hackers not only had gained access to highly sensitive employee information but had also posted this information for sale on the dark web.

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

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

9. In failing to adequately protect employees' information, adequately notify them about the breach, and obfuscating the nature of the breach, Defendant violated state and federal law and harmed 5,600 of its current and former employees.

10. Plaintiff and members of the proposed Class are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiff and members of the proposed Class

trusted Defendant with their PII. But Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

11. Plaintiff Castaneda is a former Ardagh employee and Data Breach victim. Ms. Castaneda worked for Ardagh from approximately January 2014 -November 2022.

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

PARTIES

13. Plaintiff, Cynthia Castaneda, is a natural person and citizen of California, residing in Madera, California, where she intends to remain. Ms. Castaneda is a former Ardagh employee and Data Breach victim.

14. Defendant, Ardagh, is a Delaware corporation with its principal place of business in Indianapolis, Indiana. Its United States headquarters are located at 10194 Crosspoint Boulevard, Indianapolis, Indiana. Ardagh's United States headquarters in Indianapolis is completely office based, with no manufacturing elements, and serves as the center of direction, control, and coordination of all North American related business for Ardagh.

JURISDICTION & VENUE

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

16. This Court has personal jurisdiction over Defendant because Ardagh is

headquartered in this District and Ardagh conducts substantial business in this District.

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

BACKGROUND FACTS

Ardagh

18. Ardagh is a packaging manufacturer and subsidiary to Ardagh Group S.A., a worldwide manufacturer of packaging containers. Ardagh maintains commercial offices and manufacturing facilities throughout Indiana.

19. On information and belief, Ardagh accumulates highly sensitive PII of its employees.

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

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

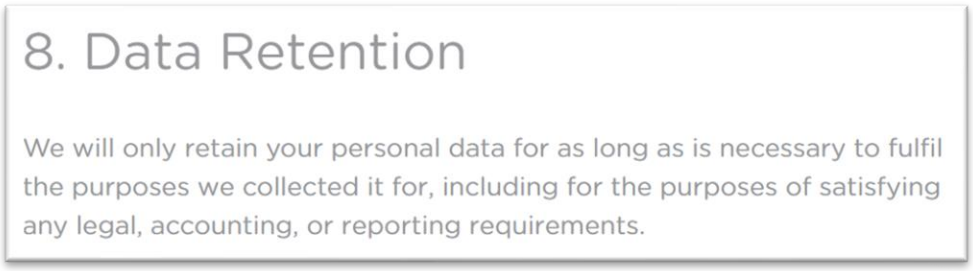
22. Indeed, Ardagh promises that it implements "appropriate security measures" and assures that it will notify breach victims when "legally required to do so":

7. Data Security

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

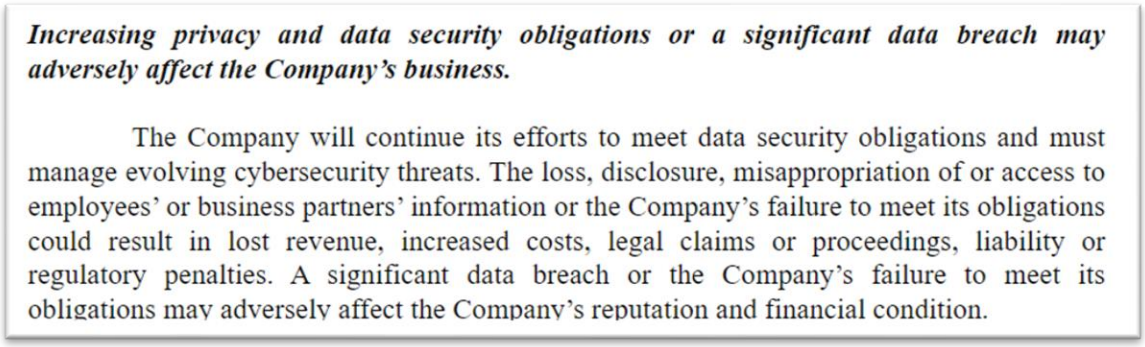
23. Ardagh also promises to delete data when it no longer needs it:



8. Data Retention

We will only retain your personal data for as long as is necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

24. Further, in its 2021 Annual Report filing, Ardagh acknowledged to the SEC and its investors that Ardagh "must" manage cybersecurity threats by meeting its data security obligations: [1]



Increasing privacy and data security obligations or a significant data breach may adversely affect the Company's business.

The Company will continue its efforts to meet data security obligations and must manage evolving cybersecurity threats. The loss, disclosure, misappropriation of or access to employees' or business partners' information or the Company's failure to meet its obligations could result in lost revenue, increased costs, legal claims or proceedings, liability or regulatory penalties. A significant data breach or the Company's failure to meet its obligations may adversely affect the Company's reputation and financial condition.

25. To that end, Ardagh claims to operate "a cyber and information risk management program including operating a global information security function, which partners with global leaders in the security industry to deliver an integrated information and cyber risk management service using state-of-the-art technologies in areas including antivirus & anti-malware, email and web security platforms, firewalls, intrusion detection systems, cyber threat intelligence services and advanced persistent threat detection."[2]

26. Despite clearly recognizing its duty to do so, on information and belief, Ardagh has not implemented reasonable cybersecurity safeguards or policies to protect employee PII or trained

[1] *See* Ardagh Group S.A.'s 2021 Annual Report to investor's at https://otp.investis.com/clients/us/ardagh_group/SEC/secshow.aspx?Type=html&FilingId=14782761&Cik=0001689662 (last visited Sept. 8, 2022).

[2] *Id.*

its IT or data security employees to prevent, detect, and stop breaches of Ardagh's systems. As a result, Ardagh leaves vulnerabilities in its systems for cybercriminals to exploit and gain access to employee PII.

Ardagh Fails to Safeguard Employees' PII

27. Plaintiff is a former employee of Ardagh.

28. As a condition of employment with Ardagh, Defendant requires its employees to disclose PII including but not limited to, their names, Social Security numbers, driver's license, and financial information. Defendant used that PII to facilitate its employment of Plaintiff, including payroll, and required Plaintiff to provide that PII to obtain employment and payment for that employment.

29. On information and belief, Ardagh collects and maintains current and former employees' PII in its computer systems.

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

31. According to its Breach Notice, "on May 2, 2021, Ardagh discovered that criminal actors encrypted portions of [its] network environment in Europe and the United States in a ransomware attack." Ex. A. However, despite discovering the Breach, Ardagh could not stop cybercriminals from continuing the Data Breach. As a result, cybercriminals could access and pilfer the PII belonging to over 5,600 Ardagh employees until May 19—three weeks after the breach started and seventeen days after Ardagh first discovered the Breach.

32. In other words, Ardagh investigation revealed that cyber and data security systems and measures were so inadequate that not only did Ardagh not discover the Breach until the cybercriminals encrypted portions of its system, but that even after discovery, Ardagh was unable

to stop cybercriminals from continuing the breach and obtaining files containing a treasure trove of thousands of Ardagh employees' personal, private, and sensitive information.

33. Additionally, Defendant admitted that Plaintiff's and the Class's PII were actually stolen during the Data Breach, confessing that the information was not just accessed but that "in October 2021 [,] a ransomware group posted links to data that it claimed to have stolen from Ardagh systems on a dark web site" and that "on June 22, 2022, we determined that your personal information was contained within the data files posted on the dark website." Ex. A.

34. Through its inadequate security practices, Defendant exposed Plaintiff's and the Class's PII for theft and sale on the dark web.

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

36. Upon information and belief, the notorious PYSA ransomware gang was responsible for the cyberattack. Known as one of the most active ransomware actors that attacks high value targets, PYSA has perpetrated multiple high-profile breaches in the last year alone.[3] Defendant knew or should have known of the tactics that groups like PYSA employ.

37. With the PII secured and stolen by PYSA, the hackers then purportedly issued a ransom demand to Ardagh. However, Ardagh has provided no public information on the ransom demand or payment.

[3] PYSA Ransomware Group, https://resources.prodaft.com/pysa-ransomware-group-report (last visited February, 20 2024).

38. On information or belief, PYSA released all stolen information onto the dark web for access, sale, and download on October 4, 2021, following the deadline of the ransom demand to Defendant.

39. On or about July 5, 2022–an appalling fourteen months after the Data Breach occurred– Ardagh finally notified some Class Members about the Data Breach. However, Defendant's notification to victims is ongoing, with Plaintiff still waiting for a Breach Notice that identifies which PII was compromised and stolen in the Data Breach.

40. Even so, Ardagh immediately notified its investors and customers about the breach to reassure them the Data Breach would not affect the company's operations or "financial results" that year.[4]

41. Ardagh recognized this effective response was only possible given the "dedication and commitment of [its] employees"—the same employees whose PII Ardagh lost in the Data Breach.[5]

42. Despite its duties and alleged commitments to safeguard PII, Ardagh does not follow industry standard practices in securing employees' PII, as evidenced by the Data Breach

[4] *See* Ardagh's "Cyber Security Incident" website article at https://www.ardaghgroup.com/news-centre/cyber-security-incident (last visited Sept. 8, 2022).
[5] *Id.*

and stolen employee PII.

43. In response to the Data Breach, Ardagh contends that it "continues to enhance its security controls where appropriate and trains its workforce regarding cybersecurity issues." Ex. A. Although Ardagh fails to expand on these alleged "enhancement" and "training" are, such enhancements and training should have been in place *before* the Data Breach.

44. In its Breach Notice, Ardagh attempted to downplay the threat the Data Breach posed, and misrepresented the Breach's risk in four ways:

45. First, Ardagh claims that the dark web website that hosted employees stolen PII is no longer online, claiming their data is "no longer available for download and may remain so." This is baseless, as Ardagh cannot know for certain whether or how cybercriminals are distributing employees' PII over the internet, even if the original dark web site hosting their data is no longer operating.

46. Second, Ardagh says that when employees PII was online, the servers hosting it were "unreliable or slow." Yet, Ardagh does not explain why this should reassure its employees, nor does it disclose that there is nothing preventing cybercriminals from reposting the data on more reliable and faster servers in the future.

47. Third, Ardagh says that employees' data was "posted in an area of the internet that can only be accessed with specialized knowledge and software, making it unlikely that any personal data relating to [them] was readily accessible by the general public." But, again, Ardagh does not explain why this should comfort employees, as their information is *already in the hands of cybercriminals*, who intended to steal their data and misuse it.

48. And fourth, Ardagh says "very limited amounts of personal information were interspersed throughout the data set posted online, making the personal information difficult to

locate even with Ardagh's knowledge of the dataset and powerful technological search tools." This, coming from the same company whose "technological tools" did not detect the Data Breach for eight days and could not stop it after three weeks.

49. Further, these misrepresentations are in direct contradiction to the rest of its Breach Notice, where Ardagh, recognizing the actual imminent harm and injury that flowed from the Data Breach, warned and encouraged breach victims to "remain vigilant against incidents of identity theft and fraud [,to] review your account statements, and to monitor your credit reports for suspicious activity." Ex. A.

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

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

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

53. On information and belief, Ardagh failed to adequately train its IT and data security employees on reasonable cybersecurity protocols or implement reasonable security measures,

causing it to lose control over employee PII. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing PII. Further, the Breach Notice makes clear that Ardagh cannot, or will not, determine the full scope of the Data Breach.

Plaintiff's Experience

54. Plaintiff is a former Ardagh employee.

55. As a condition of employment with Ardagh, Plaintiff was required to provide her PII, including but not limited to her full name, driver's license, financial information (including bank account information), and Social Security number.

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

57. Plaintiff does not recall ever learning that her PII was compromised in a data breach incident, other than the breach at issue in this case.

58. Plaintiff was notified by Ardagh in May 2021 via email of the incident. However, Ardagh completely failed to notify and inform Plaintiff via a Breach Notice that her PII, including at least her name, driver's license, financial information, and Social Security number, may have been compromised in the Data Breach. In addition to the damages detailed herein, the Data Breach has caused Plaintiff to be at substantial risk for further identity theft.

59. Defendant deprived Plaintiff of the earliest opportunity to guard herself against the Data Breach's effects by failing to ever formally notify her after Ardagh finally discovered the Data Breach.

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

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

62. As a result of the Data Breach, Plaintiff has spent time and made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, changing her online account passwords, placing a credit freeze through the three main credit bureaus, and monitoring her credit information. Indeed, these are precisely the actions suggested by Defendant in its Breach Notice.

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

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

65. Indeed, shortly after the Data Breach, Plaintiff's mobile banking service notified her of several out-of-state fraudulent charges that she did not recognize nor authorize, including several charges culminating to over $500 from Walmart. At least one of these Walmart charges occurred on June 17, 2021, and involved a Roku Smart TV pickup order in Yorktown, Virginia, identifying Plaintiff through her first and last name, as well as her email address on the fraudulent

order. As a result of these fraudulent charges, Plaintiff has been forced to work with her banking services for reimbursement and change bank accounts.

66. Once an individual's PII is stolen for sale and access on the dark web, as Plaintiff's PII is here as a result of the Breach, cybercriminals are able to use the stolen and compromised to gain access into other secure accounts.[6] On information and belief, Plaintiff's banking information, including credit and debit card information, was compromised as a result of the Data Breach.

67. Additionally, following the Data Breach, Plaintiff has also begun receiving spam texts and calls, further suggesting that Plaintiff's information has been stolen and placed in the hands of cybercriminals.

68. Once an individual's PII is for sale and access on the dark web, as Plaintiff's PII is here as a result of the Breach, cybercriminals are able to use the stolen and compromised to gather and steal even more information.[7] On information and belief, Plaintiff's phone number and email address were compromised as a result of the Data Breach.

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

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

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

71. The ramifications of Defendant's failure to keep Plaintiff's and the Class's PII

[6] *See* What is Data Theft and How to Prevent it, Kaspersky, https://usa.kaspersky.com/resource-center/threats/datatheft (last visited May 24, 2023); see also https://nordvpn.com/blog/data-theft/; https://www.csoonline.com/article/570759/how-cybercriminals-turn-harmless-stolen-or-leaked-data-intodollars.html

[7] What do Hackers do with Stolen Information, Aura, https://www.aura.com/learn/what-do-hackers-do-with-stolen-information (last visited January 9, 2024).

secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, or other nonpublic financial information, without permission, to commit fraud or other crimes.

72. The types of PII compromised and potentially stolen in the Ardagh Data Breach is highly valuable to identity thieves. The employees' stolen PII can be used to gain access to a variety of existing accounts and websites to drain assets, bank accounts or open phony credit cards.

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

> In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts, . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.

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

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

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

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

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

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

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

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

76. 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.

77. Social Security numbers are particularly attractive targets for hackers because they

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

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.

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

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

80. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.[9]

81. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and the proposed Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

82. Defendant disclosed the PII of Plaintiff and the Class for criminals to use in the

[9] *Id.*

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.

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

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

Ardagh Failed to Adhere to FTC Guidelines

85. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII.

86. 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.

87. 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.

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

89. 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.

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

TOLLING, CONCEALMENT, AND ESTOPPEL

91. The applicable statutes of limitation have been tolled as a result of Ardagh's knowing and active concealment and denial of the facts alleged herein.

92. Ardagh failed to provide Plaintiff with notice of the Data Breach that specifically informed Plaintiff her PII was compromised in the Data Breach.

93. Ardagh knew Plaintiff's and Class Member's PII was affected by the Data Breach, yet it failed to provide notice of the Data Breach to Plaintiff which would have informed her she was affected by the Data Breach.

94. Even while exercising due diligence, Plaintiff could not have discovered the full scope of the Data Breach's effect on her PII because only Ardagh knew 1) whether Plaintiff's PII was compromised in the Data Breach and 2) which data points of Plaintiff's PII had been compromised in the Data Breach.

95. All applicable statutes of limitation have also been tolled by operation of the discovery rule and the doctrine of continuing tort. Ardagh's failure to inform Plaintiff that her specific PII was compromised by the Data Breach has continued unabated through the present.. Ardagh is therefore, is estopped from relying on any statute of limitations defenses.

CLASS ACTION ALLEGATIONS

96. Plaintiff sues on behalf of herself and the proposed nationwide class ("Class") and state subclass ("Subclass"), defined as follows, pursuant to Federal Rule of Civil Procedure 23(b)(2) and (b)(3):

> **Nationwide Class:** All individuals residing in the United States whose PII was compromised in the Ardagh Data Breach, including all those who received notice of the breach.
>
> **California Subclass:** All individuals residing in California whose PII was compromised in the Ardagh Data Breach, including all those who received notice of the breach.

97. The following people are excluded from the Class: (1) any judge or magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries,

parents, successors, predecessors, affiliated entities, and any entity in which the Defendant or its parent has a controlling interest, and their current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

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

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

a. **Numerosity**. Ardagh reports that the Data Breach compromised the PII of more than 5,600 individuals. Therefore, the members of the Class are so numerous that joinder of all members is impractical;

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

c. **Adequacy**: Plaintiff will fairly and adequately represent and protect the interests of the Class and has retained counsel competent and experienced in complex class actions to vigorously prosecute this action on behalf of the Class. Plaintiff has no interests

that conflict with, or are antagonistic to those of, the Class, and Defendant has no defenses unique to Plaintiff.

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

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

ii. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

iii. Whether Defendant was negligent in maintaining, protecting, and securing PII;

iv. Whether Defendant breached contract promises to safeguard Plaintiff's and the Class's PII;

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

vi. Whether Defendant's Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiff and the Class injuries;

viii. What the proper damages measure is; and

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

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

CLAIMS ALLEGED ON BEHALF OF PLAINTIFF AND THE CLASS

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

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

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

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

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

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

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

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

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

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

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

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

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

110. 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.

111. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers or, in this case, employees' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and the members of the Class's sensitive PII.

112. 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.

113. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se.*

114. 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.

115. 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.

116. 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.

117. 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.

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

PII.

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

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

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

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

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

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

124. Plaintiff and the Class Members accepted Defendant's offers by disclosing their PII

to Defendant in exchange for employment.

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

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

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

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

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

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

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

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

a. failing to safeguard their information;

b. failing to notify them promptly of the intrusion into its computer systems that compromised such information.

c. failing to comply with industry standards;

d. failing to comply with the legal obligations necessarily incorporated into the agreements; and

e. failing to ensure the confidentiality and integrity of the electronic PII that Defendant created, receive and maintained.

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

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

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

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

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

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

138. Plaintiff and Class Members conferred a benefit upon Defendant. After all, Defendant benefitted from using their PII to facilitate its business.

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

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

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

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

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

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

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

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

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

147. Plaintiff, the Class Members, and Defendants contemplated a mutual benefit bailment when the Plaintiff and putative members of the Class transmitted their PII to Defendants

solely for the purpose of obtaining employment.

148. Plaintiff and the Class entrusted their PII to Defendants for a specific purpose—to obtain employment—with an implied contract that the trust was to be faithfully executed, and the PII was to be accounted for when the special purpose was accomplished.

149. Defendants accepted the Plaintiff's and the Class's PII for the specific purpose of employment.

150. Defendants were duty bound under the law to exercise ordinary care and diligence in safeguarding Plaintiff's and the Class's PII.

151. Plaintiff's and the Class's PII was used for a different purpose than the Plaintiff and the Class intended, for a longer time period and/or in a different manner or place than Plaintiff and the Class intended.

152. As set forth in the preceding paragraphs, Plaintiff and the Class Members were damaged thereby.

Sixth Claim for Relief
Violation of California's Unfair Competition Law ("UCL")
Unlawful Business Practice
(Cal Bus. & Prof. Code § 17200, *et seq*.)
(On Behalf of Plaintiff and the Nationwide Class or, alternatively, the California Subclass)

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

154. Plaintiff brings this Count on her own behalf and on behalf of the California Class (the "Class" for the purposes of this Count).

155. Defendant engaged in unlawful and unfair business practices in violation of Cal. Bus. & Prof. Code § 17200, *et seq*. which prohibits unlawful, unfair, or fraudulent business acts or practices ("UCL").

156. Defendant's conduct is unlawful because it violates the California Consumer Privacy Act of 2018, Civ. Code § 1798.100, *et seq*. (the "CCPA"), and other state data security laws.

157. Defendant stored the PII of Plaintiff and the Class in its computer systems and knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied with applicable regulations and that would have kept Plaintiff's and the Class's PII secure so as to prevent the loss or misuse of that PII.

158. Defendant failed to disclose to Plaintiff and the Class that their PII was not secure. However, Plaintiff and the Class were entitled to assume, and did assume, that Defendant had secured their PII. At no time were Plaintiff and the Class on notice that their PII was not secure, which Defendant had a duty to disclose.

159. Defendant also violated California Civil Code § 1798.150 by failing to implement and maintain reasonable security procedures and practices, resulting in an unauthorized access and exfiltration, theft, or disclosure of Plaintiff's and the Class's nonencrypted and nonredacted PII.

160. Had Defendant complied with these requirements, Plaintiff and the Class would not have suffered the damages related to the data breach.

161. Defendant's conduct was unlawful, in that it violated the CCPA.

162. Defendant's acts, omissions, and misrepresentations as alleged herein were unlawful and in violation of, *inter alia*, Section 5(a) of the Federal Trade Commission Act.

163. Defendant's conduct was also unfair, in that it violated a clear legislative policy in favor of protecting consumers from data breaches.

164. Defendant's conduct is an unfair business practice under the UCL because it was immoral, unethical, oppressive, and unscrupulous and caused substantial harm. This conduct

includes employing unreasonable and inadequate data security despite its business model of actively collecting PII.

165. Defendant also engaged in unfair business practices under the "tethering test." Its actions and omissions, as described above, violated fundamental public policies expressed by the California Legislature. *See, e.g.*, Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern."). Defendant's acts and omissions thus amount to a violation of the law.

166. Instead, Defendant made the PII of Plaintiff and the Class accessible to scammers, identity thieves, and other malicious actors, subjecting Plaintiff and the Class to an impending risk of identity theft. Additionally, Defendant's conduct was unfair under the UCL because it violated the policies underlying the laws set out in the prior paragraph.

167. As a result of those unlawful and unfair business practices, Plaintiff and the Class suffered an injury-in-fact and have lost money or property.

168. The injuries to Plaintiff and the Class greatly outweigh any alleged countervailing benefit to consumers or competition under all of the circumstances.

169. There were reasonably available alternatives to further Defendant's legitimate business interests, other than the misconduct alleged in this complaint.

170. Therefore, Plaintiff and the Class are entitled to equitable relief, including

restitution of all monies paid to or received by Defendant; disgorgement of all profits accruing to Defendant because of its unfair and improper business practices; a permanent injunction enjoining Defendant's unlawful and unfair business activities; and any other equitable relief the Court deems proper.

Seventh Claim for Relief
Violation of the California Consumer Records Act
Cal. Civ. Code § 1798.80, *et seq*.
(On Behalf of Plaintiff and the California Subclass)

171. Plaintiff restates and realleges all proceeding allegations above and hereafter as if fully set forth herein.

172. Plaintiff brings this Count on her own behalf and on behalf of the California Class (the "Class" for the purposes of this Count).

173. Under California law, any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" must "disclose any breach of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." (Cal. Civ. Code § 1798.82.) The disclosure must "be made in the most expedient time possible and without unreasonable delay" (Id.), but "immediately following discovery [of the breach], if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." (Cal. Civ. Code § 1798.82, subdiv. b.)

174. The Data Breach constitutes a "breach of the security system" of Defendant.

175. An unauthorized person acquired the personal, unencrypted information of Plaintiff and the Class.

176. Defendant knew that an unauthorized person had acquired the personal,

unencrypted information of Plaintiff and the Class, but waited approximately fourteen months to notify them. Fourteen months was an unreasonable delay under the circumstances.

177. Defendant's unreasonable delay prevented Plaintiff and the Class from taking appropriate measures from protecting themselves against harm.

178. Because Plaintiff and the Class were unable to protect themselves, they suffered incrementally increased damages that they would not have suffered with timelier notice.

179. Plaintiff and the Class are entitled to equitable relief and damages in an amount to be determined at trial.

Eighth Claim for Relief
Violation of the California Consumer Privacy Act
Cal. Civ. Code § 1798.150
(On Behalf of Plaintiff and the California Subclass)

180. Plaintiff restates and realleges all proceeding allegations above and hereafter as if fully set forth herein.

181. Plaintiff brings this Count on her own behalf and on behalf of the California Class (the "Class" for the purposes of this Count).

182. Defendant violated California Civil Code § 1798.150 of the CCPA by failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the nonencrypted PII of Plaintiff and the Class. As a direct and proximate result, Plaintiff's, and the Class's nonencrypted and nonredacted PII was subject to unauthorized access and exfiltration, theft, or disclosure.

183. Defendant is a business organized for the profit and financial benefit of its owners according to California Civil Code § 1798.140, that collects the personal information of its customers, and whose annual gross revenues exceed the threshold established by California Civil Code § 1798.140(d).

184. Plaintiff and Class Members seek injunctive or other equitable relief to ensure Defendant hereinafter adequately safeguards PII by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold PII, including Plaintiff's and Class members' PII. Plaintiff and Class members have an interest in ensuring that their PII is reasonably protected, and Defendant has demonstrated a pattern of failing to adequately safeguard this information.

185. Pursuant to California Civil Code § 1798.150(b), Plaintiff mailed a CCPA notice letter on February 20, 2024 to Defendant's registered service agents, detailing the specific provisions of the CCPA that Defendant has violated and continues to violate. If Defendant cannot cure within 30 days—and Plaintiff believes such cure is not possible under these facts and circumstances—then Plaintiff intends to promptly amend this Complaint to seek statutory damages as permitted by the CCPA.

186. As described herein, an actual controversy has arisen and now exists as to whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of the information so as to protect the personal information under the CCPA.

187. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by Defendant.

PRAYER FOR RELIEF

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

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

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

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

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

E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

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

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

H. Awarding prejudgment and post-judgment interest, as provided by law;

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

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

JURY TRIAL DEMANDED

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

Dated: February 26, 2024

Respectfully submitted,

/s/ Lynn A. Toops

Lynn A. Toops (No. 26386-49)
Amina A. Thomas (No. 34451-49)
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, Indiana 46204
(317) 636-6481
ltoops@cohenandmalad.com

athomas@cohenandmalad.com

J. Gerard Stranch, IV (*Pro Hac Vice* forthcoming)
Andrew E. Mize (*Pro Hac Vice* forthcoming)
STRANCH, JENNINGS & GARVEY, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
(615) 254-8801
(615) 255-5419 (facsimile)
gstranch@stranchlaw.com
amize@stranchlaw.com

Samuel J. Strauss (*Pro Hac Vice* forthcoming)
Raina Borelli (*Pro Hac Vice* forthcoming)
TURKE & STRAUSS, LLP
613 Williamson St., Suite 201
Madison, Wisconsin 53703
(608) 237-1775
(608) 509-4423 (facsimile)
sam@turkestrauss.com
raina@turkestrauss.com

Counsel for Plaintiff and the Proposed Class

EXHIBIT A

ArdaghGroup
Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

July 5, 2022

i0488-L01-0000001 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01
APT ABC
123 ANY STREET
ANYTOWN, FC 1A2 B3C
COUNTRY

qppssppprsppppqpqsprssqrrqqprsrppppsrsqrqqsqrsrpqsqqppssppsssqrsqp

RE: Notice of Data [Extra1]

Dear Sample A. Sample:

We write to share important information with you about a data security incident that may have impacted your personal information. In an abundance of caution, we are providing you with this notice so that you know what we are doing and the steps you can take to protect your information should you feel it is appropriate to do so. We regret that this incident occurred and take the security of your personal information seriously.

What Happened? We have conducted an investigation, with the assistance of leading cybersecurity experts, into a criminal cyberattack that targeted our systems. On May 2, 2021, Ardagh discovered that criminal actors encrypted portions of our network environment in Europe and the United States in a ransomware attack. Based on our investigation, we understand that the potential unauthorized activity occurred between April 23, 2021 and May 19, 2021.

In October 2021, we learned that a ransomware group posted links to data that it claimed to have stolen from Ardagh systems on a dark web site, which appears on a portion of the Internet that is only accessible by means of special software and knowledge. In the ensuing time period, Ardagh has worked with outside cybersecurity experts to obtain copies of the posted data and to analyze its contents, specifically with the aim of identifying whether personal information was impacted.

On June 22, 2022, we determined that your personal information was contained within the data files posted on the dark web site. Aside from the act of posting the data on the dark web site, our investigation has not revealed any evidence that your data has been otherwise misused. We are undertaking ongoing monitoring of the dark web to identify if such attempts are made.

There are some additional facts that we can provide to help you assess any risk to your information. First, the servers used to post the data on the dark web have been offline since on or about November 16, 2021. Thus, at this time, the files containing Ardagh data are no longer available for download and may remain so. Second, when the servers were online, they were unreliable and slow, which prolonged Ardagh's efforts to obtain a copy of the data even with the assistance of cybersecurity experts. Third, this dark web site was posted in an area of the internet that can only be accessed with specialized knowledge and software, making it unlikely that any personal data relating to you was readily accessible by the general public. Finally, very limited amounts of personal information were interspersed throughout the data set posted online, making the personal information difficult to locate even with Ardagh's knowledge of the dataset and powerful technological search tools.

Nonetheless, Ardagh takes this matter extremely seriously and wants to ensure that any risk to your information is being properly addressed.

What Information Was Involved? For most individuals, their names and Social Security Numbers were involved. For a small subset of individuals, the types of affected data varied by individual, but may have included one or more of the following data types: name, Social Security Number, driver's license number, passport number, other governmental identification number, birth certificate, financial account number, or work-related injury information.

What We Are Doing. Ardagh regularly reviews and updates the measures it takes to protect your personal information. We strive to continually improve our data security and maintain a secure environment for confidential and personal information.

In response to this incident, Ardagh immediately launched an investigation with the assistance of leading cybersecurity experts to secure each impacted system and has continued to monitor for suspicious activity. Ardagh also continues to enhance its security controls where appropriate and trains its workforce regarding cybersecurity issues. We are also regularly monitoring the dark web to identify any data taken from or relating to Ardagh.

As an added precaution, we are providing you with access to a complimentary ##-month membership of Experian's® IdentityWorksSM. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: **September 30, 2022** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/credit
- Provide your **activation code**: **ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-877-890-9332 by September 30, 2022. Be prepared to provide engagement number **ENGAGE#** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR Coverage_Length-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 1-877-890-9332. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for Coverage_Length months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

We sincerely apologize for this incident and regret any inconvenience it may cause you. Should you have questions or concerns regarding this matter, please do not hesitate to contact us at 1-833-737-0006.

Sincerely,

Joshua Markus
General Counsel Ardagh North America

Steps You Can Take to Protect Against Identity Theft and Fraud

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. Under federal law, you cannot be charged to place, lift or remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. To find out more on how to place a security freeze, you can use the following contact information:

Equifax	Experian Security Freeze	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094
800-349-9960	888-397-3742	888-909-8872

Websites:
www.equifax.com/personal/credit-report-services/credit-freeze
www.experian.com/freeze/center.html
www.transunion.com/credit-freeze

To request a security freeze, you will need to provide some or all of the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail.:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of Birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill, telephone bill, rental agreement, or deed;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. Social Security Card, pay stub, or W2;
8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based upon the method of your request. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password (or both) that can be used by you to authorize the removal or lifting of the security freeze. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (including name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report. You may also temporarily lift a security freeze for a specified period of time rather than for a specific entity or individual, using the same contact information above. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for request made by mail) after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement, your state Attorney General, or the Federal Trade Commission. This notice has not been delayed by law enforcement.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above.

District of Columbia Residents: You may obtain information about preventing and avoiding identity theft from the Office of the Attorney General for the District of Columbia at:

Office of the Attorney General for the District of Columbia
441 4th Street NW
Suite 1100 South
Washington, D.C. 20001
(202) 727-3400
https://oag.dc.gov/

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: You may obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft at:

Office of the Attorney General of Maryland
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
Telephone: 1-888-743-0023.
www.oag.state.md.us/Consumer

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting

0000001

Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: You may obtain information about security breach response and identity theft prevention and protection from the following New York state agencies:

New York Attorney General
Consumer Frauds & Protection Bureau
120 Broadway, 3rd Floor
New York, NY 10271
(800) 771-7755
www.ag.ny.gov

New York Department of State
Division of Consumer Protection
99 Washington Avenue
Suite 650
Albany, NY 12231
(800) 697-1220
www.dos.ny.gov

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office at:

Office of the Attorney General of North Carolina
9001 Mail Service Center
Raleigh, NC 27699-9001
Telephone: 1-919-716-6400
www.ncdoj.gov

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

ClassAction.org
