IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

IRMA CARRERA AGUALLO, DROR HERTZ, KELVIN HOLMES, MELISSA ANTONIO, MARY MACARONIS and GREGGORY VEECH, individually and on behalf of all others similarly situated, Plaintiffs, v. KEMPER CORPORATION and INFINITY INSURANCE COMPANY, Defendants.	Case No.: 1:21-cv-01883-MMP (YBK) **JURY TRIAL DEMANDED**

THIRD AMENDED CLASS ACTION COMPLAINT

Plaintiffs Irma Carrera Aguallo, Dror Hertz, Kelvin Holmes, Melissa Antonio, Mary Macaronis and Greggory Veech ("Plaintiffs") bring this Class Action Complaint against Defendants Kemper Corporation ("Kemper") and Infinity Insurance Company ("Infinity" and, collectively, "Defendants") as individuals and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Kemper and its wholly-owned subsidiary, Infinity, are insurance companies. Among other types of insurance, Defendants sell automobile insurance.

2. On or about March 16, 2021, Infinity began notifying customers and state Attorneys

General about a data breach that occurred on December 26, 2020 (the "Data Breach").[1] Hackers obtained information from Kemper and its subsidiaries including personally identifiable information ("PII") of thousands of its customers, potential customers, employees and other consumers, including, but not limited to, their names, addresses, Social Security Numbers, driver's license numbers, medical leave information, and workers' compensation claim information.

3. After the initial notification of Data Breach, Infinity discovered an additional potential security incident, and on April 25, 2021, determined that an unauthorized individual potentially accessed the names and driver's license numbers of hundreds of thousands of additional individuals. On or about May 25, 2021, Infinity began notifying the additional individuals of the Data Breach.

4. As Defendant Infinity explains on its website: "Personal data is information that identifies you: your name and surname, your picture, your address, your phone, etc. Your personal data tells your life story: who you are, where you live, what you do, what you like...."[2] And it is this exact personal data that Defendants failed to protect.

5. Not only did hackers steal the PII of Plaintiffs and class members, but, upon information and belief, criminals have already used the PII to attempt to steal certain of Plaintiffs' and class members' identities. Hackers accessed and then either used or offered for sale the unencrypted, unredacted, stolen PII to criminals. This stolen PII has great value to hackers. Because of Defendants' Data Breach, customers' PII is still available and may be for sale on the dark web for criminals to access and abuse. Defendants' customers and employees face a lifetime risk of identity theft.

6. As Defendant Infinity acknowledges on its own website:

> The information they steal allows the modern thief to assume your identity when carrying out criminal acts such as:

---

[1] https://www.doj.nh.gov/consumer/security-breaches/documents/infinity-insurance-20210317.pdf (last visited Aug. 28, 2021).

[2] https://www.infinityauto.com/knowledge-center/daily-life-and-family/how-can-your-identity-be-stolen (last visited Aug. 28, 2021).

- Using your credit history.
- Making financial transactions on your behalf, including opening credit accounts in your name.
- Impersonating you via mail and/or email.
- Impersonating you in cyber forums and social networks.
- Stealing benefits that belong to you.
- Committing illegal acts which, in turn, incriminate you.[3]

7. Infinity also acknowledges that "[w]hen you discover that you've been a victim of online fraud and identity theft, it can be a scary moment."[4]

8. Plaintiffs' and class members' PII was compromised due to Defendants' negligent and/or careless acts and omissions and their failure to protect the PII.

9. Plaintiffs bring this action on behalf of all persons whose PII was compromised as a result of Defendants' failure to: (i) adequately protect consumers' and employees' PII, (ii) warn its customers, potential customers, employees and other consumers of their inadequate information security practices, and (iii) effectively monitor their websites and platforms for security vulnerabilities and incidents. Defendants' conduct amounts to negligence and violates federal and state statutes.

10. Plaintiffs and similarly situated individuals have suffered injury as a result of Defendants' conduct. These injuries include: (i) lost or diminished inherent value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) deprivation of rights they possess under California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq*. (the "UCL"); the California Consumer Privacy Act, Cal. Civ. Code

---

[3] *Id*.

[4] https://www.infinityauto.com/knowledge-center/daily-life-and-family/how-to-get-my-identity-back (last visited Aug. 28, 2021).

§ 1798.100, *et seq*. (the "CCPA"); and California's Consumers Legal Remedies Act, Cal. Civ. Code § 1750, *et seq*. (the "CLRA");; and (v) the continued and certainly an increased risk to their PII, which: (a) remains available on the dark web for individuals to access and abuse; and (b) remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

PARTIES

11. Plaintiff Irma Carrera Aguallo is a citizen of California, residing in the County of Los Angeles, California. Ms. Aguallo received the Notice of Data Breach from Defendants dated March 16, 2021, on or about that date. The Notice advised that the Data Breach had occurred following a "potential security incident," and that Ms. Aguallo's personal data (including her name and driver's license number) was involved.

12. Plaintiff Dror Hertz is a citizen of Florida, residing in Broward County, Florida. Mr. Hertz received the Notice of Data Breach from Defendants dated March 16, 2021, on or about that date. The Notice advised that the Data Breach had occurred following a "potential security incident," and that Mr. Hertz's personal data (including his name and Social Security number) was involved.

13. Plaintiff Kelvin Holmes is a citizen of Georgia residing in Polk County, Georgia. Mr. Holmes received the Notice of Data Breach from Defendants dated March 16, 2021, on or about that date. The Notice advised that the Data Breach had occurred following a "potential security incident," and that Mr. Holmes' personal data (including his name and Social Security number) was involved.

14. Plaintiff Melissa Antonio is a citizen of Florida, residing in Hernando County, Florida. Plaintiff Antonio received the Notice of Data Breach from Defendants dated March 16, 2021, on or about that date. The Notice advised that the Data Breach had occurred following a "potential security incident," and that Ms. Antonio's personal data (including her name and Social Security number) was involved.

15. Plaintiff Mary Macaronis is a citizen of Florida, residing in Orange County, Florida.

Ms. Macaronis received the Notice of Data Breach from Defendants dated March 16, 2021, on or about that date. The Notice advised that the Data Breach had occurred following a "potential security incident," and that Ms. Macaronis' personal data (including her name and Social Security number) was involved.

16. Plaintiff Greggory Veech is a citizen of the State of New York, residing in Broome County, New York. Mr. Veech received the Notice of Data Breach from Defendants dated May 25, 2021, on or about that date. The Notice advised that the Data Breach had occurred following a "potential security incident" that occurred between January 7 and April 4, 2021, and that Mr. Veech's personal data (including his name and driver's license number) was involved.

17. Defendant Kemper Corporation ("Kemper") is a Delaware corporation with its principal place of business at 200 E. Randolph St., Suite 3300, Chicago, Illinois, 60601. Kemper offers insurance for home, auto, life, health, and valuables and has $14.1 billion in assets. According to its website, Kemper services approximately 6.4 million policies, employs over 9,300 "associates," is represented by more than 30,000 agents and brokers, and is licensed to sell insurance in all 50 states and the District of Columbia.[5]

18. Defendant Infinity Insurance Company ("Infinity") is an Indiana corporation with its principal place of business at 2201 4th Avenue North, Birmingham, Alabama, 35203. Infinity is a provider of auto insurance specializing in specialty or difficult-to-insure drivers. They have 2,300 employees and more than 10,000 independent agents. Writing about 1.5 billion premiums annually and generating $998.72 million in sales, the company is one of the largest nonstandard auto insurers in the nation.

19. Infinity is a wholly-owned subsidiary of Kemper.

JURISDICTION AND VENUE

20. 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

[5] https://www.kemper.com/wps/portal/Kemper/Home/AboutKemper (last visited Aug. 28, 2021).

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.

21. This Court has personal jurisdiction over Defendants because Defendant Kemper has its principal place of business within this District, and Defendant Infinity is a wholly-owned subsidiary of Kemper.

22. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to these claims occurred in, were directed to, and/or emanated from this District. Defendant Kemper resides within this judicial district and a substantial part of the events giving rise to the claims alleged herein occurred within this judicial district.

FACTUAL ALLEGATIONS

Background

23. Defendant Kemper Corporation is one of the nation's leading specialized insurers, offering insurance for home, auto, life, health, and valuables, services approximately 6.2 million policies, and has $14.3 billion in assets. Kemper is licensed to sell insurance in all fifty (50) states and the District of Columbia.[6]

24. Defendant Infinity is a provider of auto, business, property, life, and umbrella insurance. Prior to its acquisition by Defendant Kemper in 2018, Infinity was a provider of auto insurance focused on serving the specialty, nonstandard segment. With approximately 2,300 employees, 10,600 independent agents, and $1.4 billion in 2017 direct written premiums, Infinity was one of the largest nonstandard auto insurers in the country.[7]

25. There is a unity of identity between the Defendants because Defendant Infinity is a wholly owned subsidiary of Defendant Kemper.

26. In the ordinary course of doing business with Defendants, customers and

[6] https://www.kemper.com/about-kemper (last visited Aug. 28, 2021).

[7] https://www.businesswire.com/news/home/20180213006637/en/Kemper-to-Acquire-Infinity-in-1.4-Billion-Transaction (last visited Aug. 28, 2021).

prospective customers are required to provide Defendants with sensitive PII such as:

- Name;
- Address;
- Phone number;
- Driver's license number;
- Social Security number;
- Date of birth;
- Email address;
- Gender;
- Marital status;
- Whether or not there is a homeowner on the policy;
- Vehicle information; and
- Other driver information.

27. Defendants also collect and maintain "contractual information," including payment information, method of payment (*i.e.*, credit/debit card number or bank account number), billing information, and the chosen insurance package (including coverage, limits, and premium).

28. In addition to the types of information Defendants collect from consumers listed above, Defendants collect personal information "through directories and other consumer reporting agencies," and track and maintain record of internet usage information and inferences from PII collected.[8]

29. Information collected by Defendants about its customers and prospective customers, including Plaintiffs, includes driving records, claims history with other insurers, and credit history information.

30. In the course of collecting PII from consumers, including Plaintiffs, Defendants make promises to provide confidentiality and security for personal information, including by

[8] https://customer.kemper.com/auto/privacy-policy (last visited Aug. 28, 2021).

promulgating and placing privacy policies on their website.

31. Defendant Kemper promises that it will protect its customers' privacy and remain in compliance with statutory privacy requirements. For example, Defendant Kemper states on its website:

> Kemper promises to keep your personal information safe and confidential. We never ask for information that we don't need, nor do we share your information with any other companies or organizations without your permission. We collect information from you for one reason only: to provide top-notch, on-demand services and accurate insurance quotes.[9]

32. Defendant Kemper also represents on its website: "We keep your information safeguarded and confidential;" "[w]e will share information about you ONLY AS PERMITTED BY LAW;" and "[w]e will NOT share your personal information with any other companies without your consent."[10] The types of information Kemper collects from its customers includes identifiers, personal records, consumer characteristics, commercial information, and professional or employment information, internet usage information and inferences from PII collected.[11]

33. Defendant Infinity similarly promises in its privacy policy: "[W]e will not share your personal information with other Kemper companies for marketing purposes except as allowed by applicable law."[12] Infinity also represents that it "take[s] reasonable steps to protect personal information. These steps vary depending on the type of information we have. These steps include computer equipment and system safeguards and secured files and buildings."[13]

The Data Breach

34. On or about March 16, 2021, Defendant Infinity began notifying consumers and state Attorneys General about a data security incident that occurred on December 26, 2020.

35. According to the Notice of Data Breach letters and letters sent to state Attorneys General, Infinity's security team "detected indications of a potential security incident on December

---

9 https://customer.kemper.com/auto/privacy-policy (last visited Aug. 28, 2021).
10 *Id*.
11 *Id*.
12 https://www.infinityauto.com/privacy-policy (last visited Aug. 28, 2021).
13 *Id*.

26, 2020," and "identified brief, unauthorized access to files on certain company servers in [its] network on two days in December 2020."[14]

36. According to the Notice, Infinity "immediately began to investigate and took measures to address the incident." Infinity's investigation concluded on February 18, 2021. [15]

37. However, despite first learning of the Data Breach in December 2020 and concluding the investigation in February 2021, Defendants did not take any "measures" to notify affected Class Members until March 16, 2021.

38. Subsequently, Infinity's security team detected indications that between January 7 and April 4, 2021, an unauthorized actor entered the names and other information obtained elsewhere of individuals with whom Infinity had no prior relationship into the Infinity application system used by insurance agents and potential customers to obtain online insurance quotes.

39. As a result, the application prefill process populated the individual's driver's license number, giving the unauthorized actor access to individuals' driver's license numbers.

40. Defendants began notifying additional individuals affected by this conduct on or about May 25, 2021.

41. Plaintiffs Antonio, Hertz, Holmes and Macaronis were informed that their names and Social Security Numbers were accessed, and Plaintiff Aguallo was informed that her name and driver's license number were accessed.

42. The Infinity Notices apologized for the "inconvenience" and offered a "complementary one-year membership to Experian IdentityWorks^{SM} credit monitoring service. The Infinity Notices advised the recipients to "remain vigilant by reviewing your financial account statements for any unauthorized activity."

Defendants Were Aware of the Risks of a Data Breach

43. Defendants had obligations created by contract, industry standards, common law,

---

[14] https://www.doj.nh.gov/consumer/security-breaches/documents/infinity-insurance-20210317.pdf (last visited Aug. 28, 2021).

[15] *Id*.

and representations made to Plaintiffs and Class members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

44. Plaintiffs and Class members provided their PII to Defendants with the reasonable expectation and mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

45. Defendants' data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches in the banking/credit/financial services industry preceding the date of the breach.

46. Data breaches, including those perpetrated against the banking/credit/financial sector of the economy, have become widespread. In fact, over 62% of the 164 million sensitive records exposed in data breaches in 2019 were exposed in breaches involving the banking/credit/financial sector. [16]

47. Indeed, data breaches, such as the one experienced by Defendants, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendants' industry, including Defendants.

48. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve.[17] Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank and finance fraud.[18]

---

[16] https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last visited Aug. 31, 2021).

[17] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (Apr. 2013), https://dss.mo.gov/cd/older-youth-program/files/taking-charge-what-to-do-if-identity-is-stolen.pdf (last visited Aug. 28, 2021).

[18] *Id*. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security

49. The PII of Plaintiffs and Class members was taken by hackers to engage in identity theft and/or to sell it to other criminals who will purchase the PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

50. Defendants knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and members of the Classes, including Social Security numbers, driver's license or state identification numbers, and/or dates of birth, and of the foreseeable consequences that would occur if Defendants' data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class members as a result of a breach.

51. Plaintiffs and members of the Classes now face years of constant surveillance and monitoring of their financial and personal records and loss of rights. The Classes are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

52. The injuries to Plaintiffs and members of the Classes were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the PII of Plaintiffs and members of the Classes.

Defendants Fail to Comply with FTC Guidelines

53. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

54. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security

number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id*.

problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

55. The FTC further 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.

56. The FTC has brought enforcement actions against businesses for failing to protect consumer data adequately and reasonably, 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.

57. Defendants failed to properly implement basic data security practices, and their failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

58. Defendants were at all times fully aware of their obligation to protect the PII of customers, prospective customers and employees. Defendants were also aware of the significant repercussions that would result from their failure to do so.

Defendants Fail to Comply with Industry Standards

59. A number of industry and national best practices have been published and should have been used as a go-to resource and authoritative guide when developing Defendants' cybersecurity practices.

60. Best cybersecurity practices that are standard in the financial services industry

include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

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

62. These foregoing frameworks are existing and applicable industry standards in Defendants' industry, and Defendants failed to comply with these accepted standards, thereby opening the door to the Cyber-Attack and causing the Data Breach.

The Value of PII to Cyber Criminals

63. Businesses that store personal information are likely to be targeted by cyber criminals. Credit card and bank account numbers are tempting targets for hackers. However, information such as dates of birth and Social Security numbers are even more attractive to hackers; they are not easily destroyed and can be easily used to perpetrate identity theft and other types of fraud.

64. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[19]

65. Social Security numbers, for example, are among the worst kind of personal

[19] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs (last visited Aug. 28, 2021).

information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration ("SSA") stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[20]

66. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

67. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[21]

68. Furthermore, as the SSA warns:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is

---

[20] SSA, *Identity Theft and Your Social Security Number*, https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Apr. 7, 2021).

[21] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited Apr. 7, 2021).

> especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[22]

69. Here, the unauthorized access left the cyber criminals with the tools to perform the most thorough identity theft—they have obtained all the essential PII to mimic the identity of the user. The personal data of Plaintiffs and members of the Classes stolen in the Data Breach is a dream for hackers and a nightmare for Plaintiffs and the Classes. The stolen personal data of Plaintiffs and members of the Classes represents essentially one-stop shopping for identity thieves.

70. The FTC has released its updated publication on protecting PII for businesses, which includes instructions on protecting PII, properly disposing of PII, understanding network vulnerabilities, implementing policies to correct security problems, using intrusion detection programs, monitoring data traffic, and having in place a response plan.

71. General policy reasons support such an approach. A person whose personal information has been compromised may not see any signs of identity theft for years. According to the United States Government Accountability Office ("GAO") Report to Congressional Requesters:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[23]

72. Companies recognize that PII is a valuable asset. Indeed, PII is a valuable commodity. A "cyber black-market" exists in which criminals openly post stolen Social Security

---

[22] SSA, *Identity Theft and Your Social Security Number*, SSA Publication No. 05-10064 (Jun. 2018), http://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Aug. 28, 2021).

[23] *See* https://www.gao.gov/assets/gao-07-737.pdf (June 2007) at 29 (last visited Aug. 28, 2021).

numbers and other PII on a number of Internet websites. The stolen personal data of Plaintiffs and members of the Classes has a high value on both legitimate and black markets.

73. Identity thieves may commit various types of crimes such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, and/or using the victim's information to obtain a fraudulent tax refund or fraudulent unemployment benefits. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected.

74. As noted above, the disclosure of Social Security numbers in particular poses a significant risk. Criminals can, for example, use Social Security numbers to create false bank accounts or file fraudulent tax returns. Defendants' former and current customers and employees whose Social Security numbers have been compromised now face a real and imminent substantial risk of identity theft and other problems associated with the disclosure of their Social Security number and will need to monitor their credit and tax filings for an indefinite duration.

75. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change — Social Security number, driver's license number or government-issued identification number, name, and date of birth.

76. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[24]

77. Among other forms of fraud, identity thieves may obtain driver's licenses,

[24] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Aug. 28, 2021).

government benefits, medical services, and housing or even give false information to police.

78. According to a recent article in the New York Times, cyberthieves are using driver's licenses obtained via insurance company application prefill processes to submit and fraudulently obtain unemployment benefits.[25] An individual may not know that his or her driver's license was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud, or until the individual attempts to lawfully apply for unemployment and is denied benefits (due to the prior, fraudulent application and award of benefits).

Plaintiffs' and Class Members' Damages

79. To date, Defendants have done absolutely nothing to provide Plaintiffs and Class members with relief for the damages they have suffered as a result of the Data Breach, including, but not limited to, the costs and loss of time they incurred because of the Data Breach. Defendants have only offered twelve months of inadequate credit monitoring services, and it is unclear whether that credit monitoring was only offered to certain affected individuals (based upon the type of data stolen), or to all persons whose data was compromised in the Data Breach.

80. Moreover, the twelve months of credit monitoring offered to persons whose PII was compromised is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud.

81. Defendants entirely fail to provide any compensation for the unauthorized release and disclosure of Plaintiffs' and Class members' PII.

82. Plaintiffs and Class members have been damaged by the compromise of their PII in the Data Breach.

83. Plaintiffs and Class members face substantial risk of out-of-pocket fraud losses

[25] *How Identity Thieves Took My Wife for a Ride*, New York Times, (April 27, 2021) https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html (last visited Aug. 28, 2021)

such as loans opened in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

84. Plaintiffs and Class members have been, and face substantial risk of being targeted in the future, subjected to phishing, data intrusion, and other illegal activities based on their PII as potential fraudsters could use that information to target such schemes more effectively to Plaintiffs and Class members.

85. Plaintiffs and Class members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

86. Plaintiffs and Class members also suffered a loss of value of their PII when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in data breach cases.

87. Plaintiffs and Class members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

88. Plaintiffs and Class members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach

89. Moreover, Plaintiffs and Class members have an interest in ensuring that their PII, which is believed to remain in the possession of Defendants, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password protected.

90. Further, as a result of Defendants' conduct, Plaintiffs and Class members are forced to live with the anxiety that their PII —which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

91. As a direct and proximate result of Defendants' actions and inactions, Plaintiffs and Class members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

The Plaintiffs' Experiences

Plaintiff Irma Carrera Aguallo

92. Plaintiff Irma Carrera Aguallo has purchased automobile insurance through a Kemper insurance company since in or about August 2018. Ms. Aguallo was required to supply Kemper with her PII, including but not limited to her full name, California driver's license number, vehicle identification number, car registration, address, and telephone number. She has paid Kemper using her debit card, including type and full number, CVV code, and debit card expiration date.

93. Ms. Aguallo received the Notice of Data Breach from Defendant Infinity, dated March 16, 2021, on or about that date. The Notice stated that the exposed PII included Ms. Aguallo's full name and driver's license number.

94. As a result of receiving the Data Breach notice, Ms. Aguallo has spent time dealing with the consequences of the Breach, including confirming the legitimacy of the Data Breach, reviewing the information compromised by the Breach, self-monitoring her accounts, exploring credit monitoring and identity theft insurance options, and signing up for the free credit monitoring service offered by Defendants.

95. Ms. Aguallo is not aware of any other data breaches that could have resulted in the theft of her driver's license number. She is very careful about sharing her PII, and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

96. Ms. Aguallo stores any and all documents containing her PII in a safe and secure digital location and destroys any documents she receives in the mail that contain any of her PII or that may contain any information that could otherwise be used to compromise her payment card accounts. Moreover, she uses complex passwords for her online accounts for added security.

97. Ms. Aguallo suffered actual injury in the form of damages to and diminution in the

value of her PII—a form of intangible property that Plaintiff entrusted to Defendants for the purpose of purchasing Defendants' products and which was compromised in and as a result of the Data Breach.

98. Further, a portion of the price Ms. Aguallo paid for any services she purchased from Defendants, like all other revenue Defendants obtained from customers, was or should have been allocated by Defendants to adequately safeguard customers' PII, but it was not. Thus, Ms. Aguallo and Class Members overpaid for Defendants' services and should be entitled to restitution for that overpayment.

99. Ms. Aguallo also suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has serious concerns for the loss of her privacy.

100. Ms. Aguallo has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of criminals.

101. Ms. Aguallo has become worried about this theft of her PII and has a continuing interest in ensuring that Defendants protect and safeguard her PII, which remains in their possession, from future breaches.

Plaintiff Dror Hertz

102. Plaintiff Dror Hertz received the Notice of Data Breach from Defendant Infinity, dated March 16, 2021, on or about that date. The Notice informed him that Infinity lost a file containing, at least, his full name and Social Security number.

103. As a result of receiving the Data Breach notice, Mr. Hertz has spent time dealing with the consequences of the breach, including confirming the legitimacy of the Data Breach, reviewing the account compromised by the breach, traveling to his bank to report the breach, self-monitoring his accounts, exploring credit monitoring and identity theft insurance options, and signing up for the free credit monitoring service offered by Defendants.

104. Mr. Hertz has experienced a dramatic increase in the number of phishing emails he receives since early 2021.

105. Mr. Hertz is not aware of any other data breaches that could have resulted in the theft of his Social Security number. He is very careful about sharing his PII, and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

106. Mr. Hertz stores any and all documents containing his PII in a safe and secure digital location and destroys any documents he receives in the mail that contain any of his PII or that may contain any information that could otherwise be used to compromise his payment card accounts. Moreover, he periodically changes his passwords for his online accounts for added security.

107. Mr. Hertz suffered actual injury in being forced to review phishing emails and in paying money to, or purchasing products from, Defendants during the Data Breach—expenditures which he would not have made had Defendants disclosed that they lacked computer systems and data security practices adequate to safeguard customers' PII from theft.

108. Mr. Hertz suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that Plaintiffs entrusted to Defendants for the purpose of purchasing Defendants' products and which was compromised in and as a result of the Data Breach.

109. Mr. Hertz also suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has serious concerns for the loss of his privacy.

110. Mr. Hertz has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of criminals.

111. Mr. Hertz is worried about the theft of his PII and has a continuing interest in ensuring that Defendants protect and safeguard his PII, which remains in their possession, from future breaches.

Plaintiff Kelvin Holmes

112. Plaintiff Kelvin Holmes has been a client of a Kemper insurance company for his automobile insurance since in or about September 2020. Mr. Holmes was required by Kemper to

supply it with his PII, including his full name, Social Security number, addresses, driver's license number, vehicle identification number, automobile registration, and telephone number. He has paid Kemper using his debit card, including type and full number, CVV code, and debit card expiration date.

113. Mr. Holmes received the Notice of Data Breach from Defendant Infinity, dated March 16, 2021, on or about that date. The Notice informed him that Infinity lost a file containing, at least, his full name and Social Security number.

114. As a result of receiving the Data Breach notice, Mr. Holmes has spent time dealing with the consequences of the breach, including confirming the legitimacy of the Data Breach, reviewing the accounts compromised by the breach, contacting his bank, self-monitoring his accounts, exploring credit monitoring and identity theft insurance options, and signing up for the free credit monitoring service offered by Defendants.

115. Mr. Holmes is not aware of any other data breaches that could have resulted in the theft of his Social Security number. He is very careful about sharing his PII, and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

116. Mr. Holmes stores any and all documents containing his PII in a safe and secure digital location and destroys any documents he receives in the mail that contain any of his PII or that may contain any information that could otherwise be used to compromise his payment card accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts, and periodically changes his passwords for added security.

117. Mr. Holmes suffered actual injury in paying money to, and purchasing products from, Defendants' website during the Data Breach—expenditures which he would not have made had Defendants disclosed that they lacked computer systems and data security practices adequate to safeguard customers' PII from theft.

118. Mr. Holmes suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that Plaintiffs entrusted to Defendants for the purpose of purchasing Defendants' products and which was compromised in and as a result of the

Data Breach.

119. Further, a portion of the price Mr. Holmes paid for the insurance he purchased from Defendants, like all other revenue Defendants obtained from customers, should have been allocated by Defendants to adequately safeguard customers' PII, but it was not. Thus, Mr. Holmes and Class Members overpaid for Defendants' services and should be entitled to restitution for that overpayment.

120. Mr. Holmes also suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has serious concerns for the loss of his privacy.

121. Mr. Holmes has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of criminals.

122. Mr. Holmes has become worried about this theft of his PII and has a continuing interest in ensuring that Defendants protect and safeguard his PII, which remains in their possession, from future breaches.

Plaintiff Melissa Antonio

123. Plaintiff Melissa Antonio previously applied for auto insurance coverage with Defendant Infinity, and believes that occurred in or about 2017. As part of the application process, Ms. Antonio believes that she was required to supply Infinity with her PII, including her full name, Social Security number, addresses, driver's license number, vehicle identification number, automobile registration, and telephone number.

124. Ms. Antonio received the Notice of Data Breach from Defendant Infinity, dated March 16, 2021, on or about that date. The Notice informed her that Infinity lost a file containing, at least, her full name and Social Security number.

125. Ms. Antonio has been placed at the imminent, immediate, and continuing risk of harm through the theft of her name and Social Security number, which are the keys to financial fraud. *See* Ex. A. On or about April 1, 2021, she received a spam phone call from a person purporting to be from the Social Security Administration, seeking to "inform" her of the theft of

her Social Security number, which she attributes to the theft of her PII as a result of the Data Breach.

126. Ms. Antonio has greatly increased anxiety as a result of the theft of her PII. She has spent time checking her financial records and undertaking other activities to mitigate the effects of the Data Breach.

127. Ms. Antonio is not aware of any other data breaches that could have resulted in the theft of her Social Security number. She is very careful about sharing her PII, and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

128. Ms. Antonio stores any and all documents containing her PII in a safe and secure digital location and destroys any documents she receives in the mail that contain any of her PII or that may contain any information that could otherwise be used to compromise his financial accounts.

129. Ms. Antonio suffered actual injury in the form of diminution in the inherent value of her PII—which was in the hands of Defendants and which was compromised in and as a result of the Data Breach.

130. Ms. Antonio has suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has serious concerns for the loss of her privacy.

131. Ms. Antonio has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of criminals.

132. Ms. Antonio is worried about the theft of her PII and has a continuing interest in ensuring that Defendants protect and safeguard her PII, which remains in their possession, from future breaches.

Plaintiff Mary Macaronis

133. Plaintiff Mary Macaronis received the Notice of Data Breach from Defendant Infinity, dated March 16, 2021, on or about that date. The Notice informed her that in December of 2020, Infinity had exposed her PII, including her Social Security number, to third parties as part

of the Data Breach.

134. Plaintiff Mary Macaronis does not recall ever being a customer of Defendants or applying for insurance through Defendants.

135. On or about January 16, 2021, Ms. Macaronis received a phone call, from whom she believed to be an account manager at SunTrust, notifying her of fraudulent activity on her SunTrust bank account. During the phone call, Ms. Macaronis checked her SunTrust account online and discovered a $10,000 withdrawal. The caller was aware of Ms. Macaronis's personal information and had access to her bank account. Plaintiff was told by the individual that SunTrust would be able to stop the withdrawal if she opened a new account and transferred $10,000 into the new account by purchasing gift cards totaling that amount. Plaintiff was led to believe that after providing the gift card account numbers to the "SunTrust account manager" with whom she was dealing, the $10,000 would be deposited to her account.

136. The money was never deposited, and Ms. Macaronis later learned that the person with whom she had been speaking was not in fact a SunTrust representative.

137. Plaintiff disputed the $10,000 withdrawal, but SunTrust denied assistance or reimbursement.

138. As a result of the Data Breach, Ms. Macaronis has spent time dealing with the consequences of the breach, including confirming the legitimacy of the Data Breach, reviewing the accounts compromised by the breach, and working with her bank to handle the fraudulent activity which occurred on her account.

139. Ms. Macaronis is not aware of any other data breaches that could have resulted in the theft of her Social Security number. She is very careful about sharing her PII, and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

140. Ms. Macaronis stores any and all documents containing her PII in a safe and secure digital location and destroys any documents she receives in the mail that contain any of her PII or that may contain any information that could otherwise be used to compromise his financial accounts.

141. Ms. Macaronis suffered actual injury in the form of monetary losses stemming from the fraudulent activity on her bank account.

142. Ms. Macaronis suffered actual injury in the form of diminution in the inherent value of her PII—which was in the hands of Defendants and which was compromised in and as a result of the Data Breach.

143. Ms. Macaronis also suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has serious concerns for the loss of her privacy.

144. Ms. Macaronis has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of criminals.

145. Ms. Macaronis is worried about the theft of her PII and has a continuing interest in ensuring that Defendants protect and safeguard her PII, which remains in their possession, from future breaches.

Plaintiff Greggory Veech

146. Plaintiff Greggory Veech received the Notice of Data Breach from Defendant Infinity, dated May 25, 2021, on or about that date. The Notice informed him that an "unauthorized actor" targeted Infinity's insurance application prefill system beginning on January 7, 2021 and extracted Mr. Veech's PII, including, at least, his full name and driver's license number.

147. Mr. Veech has experienced a dramatic increase in the number of phishing calls and texts he receives since late-January 2021. He estimates that he receives twice as many scam texts since January 2021 than he did before that time.

148. In or about March 2021, Mr. Veech was notified by an auto insurance company that his application for insurance was accepted and that he owed a premium. Mr. Veech, however, had not applied for this insurance. He later discovered that an unauthorized third party used his PII to initiate this fraud and he closed the policy.

149. As a result of receiving the Data Breach Notice, Mr. Veech has spent time dealing with the consequences of the breach, including confirming the legitimacy of the Data Breach,

reviewing the information compromised by the breach, communicating with the insurance company about the fraudulent policy, dealing with the uptick in scam texts and calls, self-monitoring his accounts, exploring credit monitoring and identity theft insurance options, and signing up for and then using the free credit monitoring service offered by Defendants.

150. Mr. Veech is not aware of any other data breaches that could have resulted in the theft of his PII. He is very careful about sharing his PII, and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

151. Mr. Veech cross-shreds any documents he receives that contain any of his PII or that may contain any information that could otherwise be used to compromise his identity. Moreover, he periodically changes his passwords for his online accounts for added security.

152. Mr. Veech suffered actual injury in being forced to review phishing texts and in paying money to, or purchasing products from, Defendants during the Data Breach—expenditures which he would not have made had Defendants disclosed that they lacked computer systems and data security practices adequate to safeguard customers' PII from theft.

153. Mr. Veech suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that Plaintiffs entrusted to Defendants for the purpose of purchasing Defendants' products and which was compromised in and as a result of the Data Breach.

154. Mr. Veech also suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has serious concerns for the loss of his privacy.

155. Mr. Veech has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of criminals.

156. Mr. Veech is worried about this theft of his PII and has a continuing interest in ensuring that Defendants protect and safeguard his PII, which remains in their possession, from future breaches.

Defendants' Actions After the Data Breach Have Caused Further Harm

157. Because the Data Breach Notice sent by Defendants was so lacking in specificity, individuals, including Class Members, have been convinced that the Data Breach is a scam. A widespread theory has developed suggesting that the Notice was not actually sent by Infinity and was instead sent by a scammer to deceive people into signing up for what looks to be credit monitoring protection. Individuals across the country have taken to social media platforms to warn others not to be fooled by the letter and to not input any information into the credit monitoring website cited in the Data Breach Notice.[26]

158. Indeed, even the Highlands County Sheriff's Office in California has issued a "Scam Alert," instructing citizens who received a Data Breach Notice from Defendants to "throw it away" and "spread the word" that it is not legitimate.[27]

159. Despite the articles, YouTube videos,[28] and message board posts continuously developing across the internet warning people that the Infinity Data Breach is a scam, Defendants have failed to come forward and publicly acknowledge the legitimacy of the Data Breach. Some reporters have even taken the lack of confirmation of the Data Breach from the Defendants as further evidence that the letter is a scam.[29]

160. As a result of Defendants actions and inactions, individuals whose PII was indeed compromised in the Defendants' Data Breach are now not taking the necessary steps, such as signing up for credit monitoring, to protect themselves from future identity theft.

CLASS ALLEGATIONS

161. Plaintiffs bring this nationwide class action pursuant to rules 23(b)(2), 23(b)(3), and

---

[26] *See, e.g.,* https://www.reddit.com/r/Insurance/comments/m8v519/heads_up_to_those_with_infinity_insurance_data/ (last accessed Aug. 28, 2021).

[27] *See* https://nextdoor.com/agency-post/fl/highlands-county/highlands-county-sheriffs-office/scam-alert-infinity-insurance-181862649/ (last accessed, Aug. 28, 2021).

[28] https://www.youtube.com/watch?v=Ut-FB1AUbLY (last accessed, Apr. 4, 2021).

[29] *See* https://cinejoia.tv/infinity-insurance-company-data-breach/ (last accessed, Aug. 28, 2021).

23(c)(4) of the Federal Rules of Civil Procedure, individually and on behalf of all members of the following class:

> All natural persons residing in the United States whose PII was compromised in the Data Breach announced by Defendants on or about March 16, 2021 and on or about May 25, 2021 (the "Nationwide Class").

162. The California Subclass is defined as follows:

> All natural persons residing in California whose PII was compromised in the Data Breach announced by Defendants on or about March 16, 2021 and on or about May 25, 2021 (the "California Subclass").

163. The California Subclass together with the Nationwide Class are collectively referred to herein as the "Classes."

164. Excluded from the Classes are all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out, and all judges assigned to hear any aspect of this litigation and their immediate family members.

165. Plaintiffs reserve the right to modify or amend the definitions of the proposed Classes before the Court determines whether certification is appropriate.

166. **Numerosity**: The Classes are so numerous that joinder of all members is impracticable. Defendants have identified thousands of customers whose PII may have been improperly accessed in the Data Breach, and the Classes are apparently identifiable within Defendants' records.

167. **Commonality**: Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual members of the Classes. These include:

a. When Defendants actually learned of the Data Breach and whether their response was adequate;

b. Whether Defendants owed a duty to the Classes to exercise due care in collecting, storing, safeguarding and/or obtaining their PII;

c. Whether Defendants breached that duty;

d. Whether Defendants implemented and maintained reasonable security procedures and practices appropriate to the nature of storing the PII of Plaintiffs and members of the Classes;

e. Whether Defendants acted negligently in connection with the monitoring and/or protection of PII belonging to Plaintiffs and members of the Classes;

f. Whether Defendants knew or should have known that they did not employ reasonable measures to keep the PII of Plaintiffs and members of the Class secure and to prevent loss or misuse of that PII;

g. Whether Defendants have adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

h. Whether Defendants caused Plaintiffs' and members of the Classes damage;

i. Whether Defendants violated the law by failing to promptly notify Plaintiffs and members of the Classes that their PII had been compromised;

j. Whether Plaintiffs and the other members of the Classes are entitled to credit monitoring and other monetary relief;

k. Whether Defendants violated California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq*. (the "UCL");

l. Whether Defendants violated the California Consumer Privacy Act, Cal. Civ. Code § 1798.100, *et seq*. (the "CCPA"); and

m. Whether Defendants violated California's Consumers Legal Remedies Act, Cal. Civ. Code § 1750, *et seq*. (the "CLRA");

168. **Typicality**: Plaintiffs' claims are typical of those of the other members of the Classes because all had their PII compromised as a result of the Data Breach due to Defendants' misfeasance.

169. **Adequacy**: Plaintiffs will fairly and adequately represent and protect the interests of the members of the Classes. Plaintiffs' Counsel are competent and experienced in litigating privacy-related class actions.

170. **Superiority and Manageability**: Under rule 23(b)(3) of the Federal Rules of Civil Procedure, a class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Classes is impracticable. Individual damages for any individual member of the Classes are likely to be insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendants' misconduct would go unpunished. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

171. Class certification is also appropriate under Rule 23(a) and (b)(2) because Defendants have acted or refused to act on grounds generally applicable to the Classes, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Nationwide Class as a whole and as to each Subclass as a whole.

172. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants owed a legal duty to Plaintiffs and members of the Classes to exercise due care in collecting, storing, using, and safeguarding their PII;
b. Whether Defendants breached a legal duty to Plaintiffs and the members of the Classes to exercise due care in collecting, storing, using, and safeguarding their PII;
c. Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;
d. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; and
e. Whether members of the Classes are entitled to actual damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendants'

wrongful conduct.

FIRST CLAIM FOR RELIEF
Negligence
(On Behalf of Plaintiffs and the Nationwide Class Against All Defendants)

173. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 172.

174. Defendants owed a duty to Plaintiffs and Nationwide Class members to exercise reasonable care in obtaining, using, and protecting their PII from unauthorized third parties.

175. The legal duties owed by Defendants to Plaintiffs and Nationwide Class members include, but are not limited to the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII of Plaintiffs and Nationwide Class members in its possession;

b. To protect PII of Plaintiffs and Nationwide Class members in its possession using reasonable and adequate security procedures that are compliant with industry-standard practices; and

c. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly notifying Plaintiffs and Nationwide Class members of the Data Breach.

176. Defendants' duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a) (the "FTC Act"), which prohibits "unfair . . . practices in or affecting commerce," including, as interested and enforced by the Federal Trade Commission, the unfair practices by companies such as Defendants of failing to use reasonable measures to protect PII.

177. Various FTC publications and data security breach orders further form the basis of Defendants' duty. Plaintiffs and Nationwide Class members are consumers under the FTC Act.

Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and by not complying with industry standards.

178. Defendants breached their duties to Plaintiffs and Nationwide Class members. Defendants knew or should have known the risks of collecting and storing PII and the importance of maintaining secure systems, especially in light of the fact that data breaches have been surging since 2016.

179. Defendants knew or should have known that their security practices did not adequately safeguard Plaintiffs' and the other Nationwide Class members' PII.

180. Through Defendants' acts and omissions described in this Complaint, including Defendants' failure to provide adequate security and its failure to protect the PII of Plaintiffs and the Classes from being foreseeably captured, accessed, exfiltrated, stolen, disclosed, and misused, Defendants unlawfully breached their duty to use reasonable care to adequately protect and secure Plaintiffs' and Nationwide Class members' PII during the period it was within Defendants' possession and control.

181. Defendants breached the duties they owe to Plaintiffs and Nationwide Class members in several ways, including:

a. Failing to implement adequate security systems, protocols, and practices sufficient to protect employees' and customers' PII and thereby creating a foreseeable risk of harm;

b. Failing to comply with the minimum industry data security standards during the period of the Data Breach;

c. Failing to act despite knowing or having reason to know that their systems were vulnerable to attack; and

d. Failing to timely and accurately disclose to customers and employees that their PII had been improperly acquired or accessed and was potentially available for sale to criminals on the dark web.

182. Due to Defendants' conduct, Plaintiffs and Nationwide Class members are entitled to credit monitoring. Credit monitoring is reasonable here. The PII taken can be used for identity theft and other types of financial fraud against the Nationwide Class members.

183. Some experts recommend that data breach victims obtain credit monitoring services for at least ten years following a data breach.[30] Annual subscriptions for credit monitoring plans range from approximately $219 to $358 per year.

184. As a result of Defendants' negligence, Plaintiffs and Nationwide Class members suffered injuries that may include: (i) the lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including, but not limited to, time spent deleting phishing email messages and cancelling credit cards believed to be associated with the compromised account; (iv) the continued risk to their PII, which may remain for sale on the dark web and is in Defendants' possession and subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in their continued possession; (v) future costs in terms of time, effort, and money that will be expended to prevent, monitor, detect, contest, and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Nationwide Class members, including ongoing credit monitoring.

185. These injuries were reasonably foreseeable given the history of security breaches of this nature. The injury and harm that Plaintiffs and the other Nationwide Class members suffered was the direct and proximate result of Defendants' negligent conduct.

SECOND CLAIM FOR RELIEF
Negligence *Per Se*
(On Behalf of Plaintiffs and the Nationwide Class Against All Defendants)

[30] In the recent Equifax data breach, for example, Equifax agreed to free monitoring of victims' credit reports at all three major credit bureaus for four years, plus $1 million of identity theft insurance. For an additional six years, victims can opt for free monitoring by one credit bureau, Equifax. In addition, if a victim's child was a minor in May 2017, he or she is eligible for a total of 18 years of free credit monitoring under the same terms as for adults.

186. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 172.

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

188. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of the Data Breach for companies of Defendants' magnitude, including, specifically, the immense damages that would result to Plaintiffs and Members of the Classes due to the valuable nature of the PII at issue in this case—including Social Security numbers.

189. Defendants' violations of Section 5 of the FTC Act constitute negligence *per se*.

190. Plaintiffs and members of the Classes are within the class of persons that the FTC Act was intended to protect.

191. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and members of the Classes.

192. As a direct and proximate result of Defendants' negligence per se, Plaintiffs and members Classes have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not

limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII of their current and former employees and customers in their continued possession; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and members of the Classes.

193. Additionally, as a direct and proximate result of Defendants' negligence *per se*, Plaintiffs and members of the Classes have suffered and will suffer the continued risks of exposure of their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in their continued possession.

THIRD CLAIM FOR RELIEF
Violation of California's Unfair Competition Law
Cal. Bus. & Prof. Code § 17200, *et seq*.—Unlawful Business Practices
(On Behalf of Plaintiff Irma Carrera Aguallo and the California Subclass Against All Defendants)

194. Plaintiff Irma Carrera Aguallo re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 172.

195. Defendants have violated Cal. Bus. and Prof. Code § 17200, *et seq*., by engaging in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in Cal. Bus. Prof. Code § 17200 with respect to the services provided to the Nationwide Class or, in the alternative, the California Class.

196. Defendants engaged in unlawful acts and practices with respect to the services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiffs' and Nationwide and California Class members' PII with knowledge that the

information would not be adequately protected; and by storing Plaintiffs' and the Nationwide and California Class members' PII in an unsecure electronic environment in violation of California's data breach statute, Cal. Civ. Code § 1798.81.5, which requires Defendants to implement and maintain reasonable security procedures and practices to safeguard the PII of Plaintiffs and the Nationwide and California Class members.

197. In addition, Defendants engaged in unlawful acts and practices by failing to disclose the data breach to Nationwide and California Class members in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82. To date, Defendant has still not provided such information to Plaintiffs and the Nationwide and California Class members.

198. As a direct and proximate result of Defendants' unlawful practices and acts, Plaintiffs and the Nationwide and California Class members were injured and lost money or property, including but not limited to the price received by Defendants for the services, the loss of Nationwide and California Class members' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

199. Defendants knew or should have known that its computer systems and data security practices were inadequate to safeguard Nationwide and California Class members' PII and that the risk of a data breach or theft was highly likely. Defendants' actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Nationwide and California Class.

200. Nationwide and California Class members seek relief under Cal. Bus. & Prof. Code § 17200, et seq., including, but not limited to, restitution to Plaintiffs and Nationwide and California Class members of money or property that Defendants may have acquired by means of their unlawful, and unfair business practices, restitutionary disgorgement of all profits accruing to Defendants because of their unlawful and unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

FOURTH CLAIM FOR RELIEF
Violation of California's Unfair Competition Law
Cal. Bus. & Prof. Code § 17200, *et seq*.—Unfair Business Practices
(On Behalf of Plaintiff Irma Carrera Aguallo and the
California Subclass Against All Defendants)

201. Plaintiff Irma Carrera Aguallo re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 172.

202. Defendants engaged in unfair acts and practices by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiffs' and the Nationwide and California Class members' PII with knowledge that the information would not be adequately protected; and by storing Plaintiffs' and Nationwide and California Class members' PII in an unsecure electronic environment. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and Nationwide and California Class members. They were likely to deceive the public into believing their PII was securely stored, when it was not. The harm these practices caused to Plaintiffs and the Nationwide and California Class members outweighed their utility, if any.

203. Defendants engaged in unfair acts and practices with respect to the provision of services by failing to take proper action following the data breach to enact adequate privacy and security measures and protect Nationwide and California Class members' PII from further unauthorized disclosure, release, data breaches, and theft. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and Nationwide and California Class members. They were likely to deceive the public into believing their PII was securely stored, when it was not. The harm these practices caused to Plaintiffs and the Nationwide and California Class members outweighed their utility, if any.

204. As a direct and proximate result of Defendants' acts of unfair practices, Plaintiffs and the Nationwide and California Class members were injured and lost money or property, including but not limited to the price received by Defendants for the services, the loss of Nationwide and California Class members' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

205. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard the Nationwide and California Class members' PII and that the risk of a data breach or theft was highly likely. Defendants' actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Nationwide and California Classes.

206. Nationwide and California Class members seek relief under Cal. Bus. & Prof. Code § 17200, *et seq*., including, but not limited to, restitution to Plaintiffs and the Nationwide and California Class members of money or property that the Defendants may have acquired by means of their unfair business practices, restitutionary disgorgement of all profits accruing to Defendants because of their unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

FIFTH CLAIM FOR RELIEF
Violation of the California Consumer Privacy Act,
Cal. Civ. Code § 1798.100, *et seq*.
(On Behalf of Plaintiff Irma Carrera Aguallo and the
California Subclass Against All Defendants)

207. Plaintiff Irma Carrera Aguallo re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 172.

208. Defendants violated section 1798.150(a) of the California Consumer Privacy Act ("CCPA") by failing to prevent Plaintiff Aguallo's and California Subclass members' nonencrypted and nonredacted PII from unauthorized access and exfiltration, theft, or disclosure as a result of Defendants' violations of their duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII of Plaintiff Aguallo and California Subclass members.

209. As a direct and proximate result of Defendants' acts, Plaintiff Aguallo's and the California Subclass members' PII was subjected to unauthorized access and exfiltration, theft, or

disclosure through Kemper's computer systems and/or from the dark web, where hackers further disclosed Kemper's customers' PII.

210. As a direct and proximate result of Defendants' acts, Plaintiff Aguallo and the California Subclass members were injured and lost money or property, including but not limited to the price received by Defendants for the services, the loss of California Subclass members' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

211. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard California Subclass members' PII and that the risk of a data breach or theft was highly likely. Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiff Aguallo and the California Subclass members.

212. Defendant Kemper is a public company that is organized or operated for the profit or financial benefit of its shareholders, with $14.1 billion in assets. Kemper's wholly-owned subsidiary, Infinity, collects consumers' PII as defined in Cal. Civ. Code § 1798.140.

213. At this time, Plaintiff Aguallo and California Class members seek only actual pecuniary damages suffered as a result of Defendants' violations of the CCPA, injunctive and declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and any other relief the court deems proper.

214. On April 8, 2021, Plaintiff Aguallo provided written notice to Defendants identifying the specific provisions of this title she alleges they have violated. Within 30 days of Plaintiff Aguallo's written notice, Defendants failed to "actually cure" their violations of Cal. Civ. Code § 1798.150(a). Plaintiff Aguallo therefore seeks the greater of statutory damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater. *See* Cal. Civ. Code § 1798.150(b).

SIXTH CLAIM FOR RELIEF
Violation of California's Consumers Legal Remedies Act, Cal. Civ. Code § 1750, *et seq*.
(On Behalf of Plaintiff Irma Carrera Aguallo and the California Subclass Against All Defendants)

215. Plaintiff Irma Carrera Aguallo re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 172.

216. The CLRA was enacted to protect consumers against unfair and deceptive business practices. It extends to transactions that are intended to result, or which have resulted, in the sale or lease of goods or services to consumers. Defendants' acts, omissions, representations and practices as described herein fall within the CLRA because the design, development, and marketing of Defendants' insurance services are intended to and did result in sales of insurance services.

217. Plaintiffs Aguallo and the other California Subclass members are consumers within the meaning of Cal. Civ. Code §1761(d).

218. Defendants' acts, omissions, misrepresentations, and practices were and are likely to deceive consumers. By omitting key information about the safety and security of the Network and deceptively representing that it adequately maintained such information, Defendants violated the CLRA. Defendants had exclusive knowledge of undisclosed material facts, namely, that their Network was defective and/or unsecure, and withheld that knowledge from California Subclass members.

219. Defendants' acts, omissions, misrepresentations, and practices alleged herein violated the following provisions of section 1770 the CLRA, which provides, in relevant part, that:

> (a) The following unfair methods of competition and unfair or deceptive acts or practices undertaken by any person in a transaction intended to result or which results in the sale or lease of goods or services to any consumer are unlawful:
>
> (5) Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have . . . .
>
> (7) Representing that goods or services are of a particular standard, quality, or grade . . . if they are of another.

> (9) Advertising goods or services with intent not to sell them as advertised.\
>
> (14) Representing that a transaction confers or involves rights, remedies, or obligations which it does not have or involve, or which are prohibited by law.
>
> (16) Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

For purposes of the CLRA, omissions are actionable along with representations.

220. Defendants stored California Subclass members' PII on their network. Defendants represented to California Subclass members that their network was secure and that their PII would remain private. Kemper engaged in deceptive acts and business practices by providing in its Privacy Policy: "We keep your information safeguarded and confidential;" "[w]e will share information about you ONLY AS PERMITTED BY LAW;" and "[w]e will NOT share your personal information with any other companies without your consent."[31] Infinity also engaged in deceptive acts and business practices by providing in its Privacy Policy: "[W]e will not share your personal information with other Kemper companies for marketing purposes except as allowed by applicable law;" and "[w]e take[s] reasonable steps to protect personal information. These steps vary depending on the type of information we have. These steps include computer equipment and system safeguards and secured files and buildings."[32]

221. Defendants knew or should have known that it did not employ reasonable measures that would have kept California Subclass members' PII secure and prevented the loss or misuse of their PII. For example, Defendants failed to take reasonable steps to prevent the loss of PII through their servers through appropriate encryption and industry best practices.

222. Defendants' deceptive acts and business practices induced California Subclass members to provide PII, including Social Security numbers and driver's license numbers, for the purchase of insurance services. But for these deceptive acts and business practices, California

---

31 https://customer.kemper.com/auto/privacy-policy (last visited Aug. 30, 2021).

32 https://www.infinityauto.com/privacy-policy (last visited Aug. 30, 2021).

Subclass members would not have purchased insurance services, or would not have paid the prices they paid for the insurance services.

223. Defendants' representations that it would secure and protect California Subclass members' PII in its possession were facts that reasonable persons could be expected to rely upon when deciding whether to purchase insurance services.

224. California Subclass members were harmed as the result of Defendants' violations of the CLRA, because their PII was compromised, placing them at a greater risk of identity theft; they lost the unencumbered use of their PII; and their PII was disclosed to third parties without their consent.

225. California Subclass members suffered injury in fact and lost money or property as the result of Defendants' failure to secure their PII; the value of their PII was diminished as the result of Defendants' failure to secure their PII; and they have expended time and money to rectify or guard against further misuse of their PII.

226. Defendants' conduct alleged herein was oppressive, fraudulent, and/or malicious, thereby justifying an award of punitive damages.

227. As the result of Defendants' violations of the CLRA, Plaintiff Aguallo, on behalf of herself, California Subclass members, and the general public of the State of California, seek injunctive relief prohibiting Defendants from continuing these unlawful practices pursuant to California Civil Code § 1782(a)(2), and such other equitable relief, including restitution, and a declaration that Defendants' conduct violated the CLRA.

Pursuant to Cal. Civ. Code § 1782, on April 8, 2011, Plaintiff Aguallo mailed Defendants notice in writing, via U.S. certified mail, of the particular violations of Cal. Civ. Code § 1770 of the CLRA and demanded that they rectify the actions described above by providing complete monetary relief, agreeing to be bound by Defendants' legal obligations and to give notice to all affected customers of their intent to do so. Defendants failed to take the actions demanded to rectify their violations of the CLRA. Plaintiff Aguallo therefore also seeks statutory damages and attorneys' fees as allowed by the CLRA.

SEVENTH CLAIM FOR RELIEF
Breach of Implied Contract
(On Behalf of Plaintiffs and the Nationwide Class Against All Defendants)

228. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 174.

229. When Plaintiffs and Nationwide Class members provided their PII to Defendants in exchange for Defendants' products, they entered into implied contracts with Defendants under which—and by mutual assent of the parties—Defendants agreed to take reasonable steps to protect their PII.

230. Defendants solicited and invited Plaintiffs and Nationwide Class members to provide their PII as part of Defendants' regular business practices and as essential to the sales transaction process for card payment transactions. This conduct thus created implied contracts between Plaintiffs and Nationwide Class members on one hand, and Defendants on the other hand. Plaintiffs and Nationwide Class embers accepted Defendants' offers by providing their PII to Defendants in connection with their purchases from Defendants.

231. When entering into these implied contracts, Plaintiffs and Nationwide Class members reasonably believed and expected that Defendants' data security practices complied with relevant laws, regulations, and industry standards.

232. Defendants' implied promise to safeguard Plaintiffs' and Nationwide Class members' PII is evidenced by a duty to protect and safeguard PII that Defendants required Plaintiffs and Nationwide Class members to provide as a condition of entering into consumer transactions with Defendants.

233. Plaintiffs and Nationwide Class members paid money to Defendants to purchase products or services from Defendants. Plaintiffs and Nationwide Class Members reasonably believed and expected that Defendants would use part of those funds to obtain adequate data security. Defendants failed to do so.

234. Plaintiffs and Nationwide Class members, on the one hand, and Defendants, on the other hand, mutually intended—as inferred from customers' continued use of Defendants'

insurance services—that Defendants would adequately safeguard PII. Defendants failed to honor the parties' understanding of these contracts, causing injury to Plaintiffs and Nationwide Class members.

235. Plaintiffs and Nationwide Class members value data security and would not have provided their PII to Defendants in the absence of Defendants' implied promise to keep the PII reasonably secure.

236. Plaintiffs and Nationwide Class embers fully performed their obligations under their implied contracts with Defendants.

237. Defendants breached their implied contracts with Plaintiffs and Nationwide Class members by failing to implement reasonable data security measures and permitting the Data Breach to occur.

238. As a direct and proximate result of Defendants' breaches of the implied contracts, Plaintiffs and Nationwide Class members sustained damages as alleged herein.

239. Plaintiffs and Nationwide Class members are entitled to compensatory, consequential, and other damages suffered as a result of the Data Breach.

240. Plaintiffs and Nationwide Class members also are entitled to injunctive relief requiring Defendants to, *inter alia*, strengthen their data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Nationwide Class members.

EIGHTH CLAIM FOR RELIEF
Declaratory Judgment
(On Behalf of Plaintiffs and the Nationwide Class Against All Defendants)

241. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 172.

242. Defendants owe duties of care to Plaintiffs and Nationwide Class members which require them to adequately secure their PII.

243. Defendants still possess Plaintiffs' and Nationwide Class members' PII.

244. Defendants do not specify in either of the two *Notice of Data Breach* letters what steps they have taken to prevent this from occurring again.

245. Plaintiffs and Nationwide Class members are at risk of harm due to the exposure of their PII and Defendants' failure to address the security failings that lead to such exposure.

246. Plaintiffs, therefore, seek a declaration that (1) each of Defendants' existing security measures do not comply with their explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect customers' personal information, and (2) to comply with their explicit or implicit contractual obligations and duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to:

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

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training its security personnel regarding any new or modified procedures;

d. Segmenting user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendants' systems;

e. Conducting regular database scanning and security checks;

f. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

g. Purchasing credit monitoring services for Plaintiffs and Nationwide Class members for a period of ten years; and

h. Meaningfully educating Plaintiffs and Nationwide Class members about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

NINTH CLAIM FOR RELIEF
Unjust Enrichment
(On Behalf of Plaintiffs and the Nationwide Class Against All Defendants)

247. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 172.

248. Defendants benefited from receiving Plaintiffs' and Nationwide Class members' PII by their ability to retain and use that information for their own benefit. Defendants understood this benefit.

249. Defendants also understood and appreciated that Plaintiffs and Nationwide Class members' PII was private and confidential, and its value depended upon Defendants maintaining the privacy and confidentiality of that PII.

250. Plaintiffs and Nationwide Class members who were customers of Defendants conferred a monetary benefit upon Defendants in the form of monies paid for services available from Defendants.

251. Defendants appreciated or had knowledge of the benefits conferred upon them by Plaintiffs and Nationwide Class members. Defendants also benefited from the receipt of Plaintiffs' and Nationwide Class members' PII, as Defendants used it to facilitate the transfer of information and payments between the parties.

252. The monies that Plaintiffs and Nationwide Class members paid to Defendants for services were to be used by Defendants, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

253. Defendants also understood and appreciated that Plaintiffs' and Class Members' PII was private and confidential, and its value depended upon Defendants maintaining the privacy and confidentiality of that PII.

254. But for Defendants' willingness and commitment to maintain privacy and confidentiality, that PII would not have been transferred to and entrusted with Defendants. Indeed, if Defendants had informed Plaintiffs and Nationwide Class members that their data and cyber security measures were inadequate, Defendants would not have been permitted to continue to operate in that fashion by regulators, their shareholders, and their consumers.

255. As a result of Defendants' wrongful conduct, Defendants have been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and Nationwide Class members. Defendants continue to benefit and profit from their retention and use of the PII while its value to Plaintiffs and Nationwide Class Members has been diminished.

256. Defendants' unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged in this Complaint, including compiling, using, and retaining Plaintiffs' and Nationwide Class Members' PII, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

257. As a result of Defendants' conduct, Plaintiffs and Nationwide Class members suffered actual damages in an amount equal to the difference in value between the amount Plaintiffs and Nationwide Class members paid for their purchases with reasonable data privacy and security practices and procedures and the purchases they actually received with unreasonable data privacy and security practices and procedures.

258. Under principals of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiffs and Nationwide Class members because Defendants failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiffs and Nationwide Class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

259. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Nationwide Class members all unlawful or inequitable proceeds they received as a result of the conduct alleged herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all Nationwide Class members, request judgment against the Defendants and that the Court grant the following:

A. An order certifying the Classes as defined herein, and appointing Plaintiffs and their counsel to represent the Classes;

B. An order enjoining Defendants from engaging in the wrongful conduct alleged herein concerning disclosure and inadequate protection of the PII belonging to Plaintiffs and the members of the Classes;

C. An order instructing Defendants to purchase or provide funds for credit monitoring services for Plaintiffs and all members of the Classes;

D. An award of compensatory, statutory, nominal and punitive damages, in an amount to be determined at trial;

E. An award for equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

F. An award of reasonable attorneys' fees, costs, and litigation expenses, as allowable by law; and

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

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

Date: September 3, 2021

Respectfully Submitted,

By: */s/ M. Anderson Berry*

M. ANDERSON BERRY
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 777-7777

Facsimile: (916) 924-1829
aberry@justice4you.com

CARL V. MALMSTROM
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLC
111 W. Jackson Blvd., Suite 1700
Chicago, IL 60604
Telephone: (312) 984-0000
Facsimile: (212) 545-4653
malmstrom@whafh.com

RACHELE R. BYRD
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP
750 B Street, Suite 1820
San Diego, CA 92101
Telephone: (619) 239-4599
Facsimile: (619) 234-4599
byrd@whafh.com

GARY M. KLINGER
MASON LIETZ & KLINGER LLP
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (202) 429-2290
Fax: (202) 429-2294
gklinger@masonllp.com

GARY E. MASON
DAVID K. LIETZ
MASON LIETZ & KLINGER LLP
5101 Wisconsin Avenue NW, Suite 305
Washington, DC 20016
Telephone: (202) 429-2290
Facsimile: (202) 429-2294
dlietz@masonllp.com
gmason@masonllp.com

JEAN S. MARTIN *
FRANCESCA KESTER *
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: 813-559-4908
Facsimile: 813-222-4795
jeanmartin@forthepeople.com
fkester@forthepeople.com

Attorneys for Plaintiffs and the Class

*Admitted *Pro Hac Vice*