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

MELISSA ANTONIO, individually and on behalf of all others similarly situated, Plaintiff, v. KEMPER CORPORATION and INFINITY INSURANCE COMPANY, Defendants.	CASE NO. 1:21-cv-01921 **CLASS ACTION COMPLAINT** Filed: April 9, 2021

Plaintiff MELISSA ANTONIO ("Plaintiff"), individually and on behalf of all others similarly situated, brings this action against Defendants KEMPER CORPORATION and INFINITY INSURANCE COMPANY ("Kemper," "Infinity," or "Defendants"), to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendants. Plaintiff makes the following allegations upon information and belief, except as to her own actions, the investigation of her counsel, and the facts that are a matter of public record:

NATURE OF THE ACTION

1. This class action arises out of the recent targeted cyber-attack against Defendants that allowed a third party to access Defendant Infinity's computer systems and data, resulting in the compromise of highly sensitive personal information belonging to thousands of customers, prospective customers, and employees from Defendants' computer networks (the "Cyber-Attack").

2. As a result of the Cyber-Attack, Plaintiff and Class Members suffered ascertainable injury and damages in the form of the imminent risk of future harm from their unlawfully accessed and compromised private and confidential information (including Social Security numbers), lost

value of their private and confidential information, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

3. Plaintiff's and Class Members' sensitive personal information—which was entrusted to Defendants, their officials and agents—was compromised, unlawfully accessed, and stolen due to the Cyber-Attack. Information compromised in the Cyber-Attack includes names and the following: Social Security numbers, driver's license numbers, and (in limited cases of certain employees) medical information in connection with medical leave or workers compensation claims (collectively the "Private Information").

4. Plaintiff brings this class action lawsuit on behalf of all those similarly situated to address Defendants' inadequate safeguarding of Class Members' Private Information that it collected and maintained.

5. Defendants maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant Infinity's computer network in a condition vulnerable to cyber-attacks of this type.

6. Upon information and belief, the mechanism of the Cyber-Attack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known and foreseeable risk to Defendants, and Defendants were on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

7. In addition, Defendants and their employees failed to properly monitor the computer network and systems that housed the Private Information. The Cyber-Attack persisted for two days in December 2020, and was discovered on December 26, 2020. Had Defendants properly monitored their property, they would have discovered the intrusion sooner.

8. Plaintiff's and Class Members' identities are now at risk because of Defendants'

negligent conduct since the Private Information that Defendants collected and maintained is now in the hands of data thieves.

9. Armed with the Private Information accessed in the Cyber-Attack, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' health information to target other phishing and hacking intrusions based on their individual health needs, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

10. As a further result of the Cyber-Attack, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

11. Plaintiff and Class Members have and may also incur out of pocket costs for, *e.g.*, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

12. As a direct and proximate result of the Cyber-Attack and subsequent data breach, Plaintiff and Class Members have suffered and will continue to suffer damages and economic losses in the form of: 1) the loss of time needed to: take appropriate measures to avoid unauthorized and fraudulent charges; change their usernames and passwords on their accounts; investigate, correct and resolve unauthorized debits, charges, and fees charged against their accounts; and deal with spam messages and e-mails received as a result of the Data Breach. Plaintiff and Class Members have likewise suffered and will continue to suffer an invasion of their property interest

in their own personally identifying information ("PII") such that they are entitled to damages for unauthorized access to and misuse of their PII from Defendants. And, Plaintiff and Class Members will suffer from future damages associated with the unauthorized use and misuse of their PII as thieves will continue to use the stolen information to obtain money and credit in their name for several years.

13. Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed and/or removed from the network during the Cyber-Attack.

14. Plaintiff seeks remedies including, but not limited to, compensatory damages, nominal damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendants' data security systems, future annual audits, and adequate credit monitoring services funded by Defendants.

15. Accordingly, Plaintiff brings this action against Defendants seeking redress for their unlawful conduct asserting claims for negligence, negligence *per se*, and violation of the Florida Unfair and Deceptive Trade Practices Act ("FUDTPA").

PARTIES

16. Plaintiff Melissa Antonio is an individual citizen of the State of Florida residing in Spring Hill, Florida. Plaintiff Antonio received notice from Defendants that the Data Breach had occurred following a "potential security incident," and that her personal data (including her name and Social Security number) was involved. A copy of the notice is attached hereto as **Exhibit A**.

17. Defendant Kemper Corporation ("Kemper") is a Delaware corporation with its principal place of business at 200 E. Randolph Street, Suite 3300, Chicago, Illinois, 60601.

18. Defendant Infinity Insurance Company ("Infinity") is an Indiana corporation with

its principal place of business at 2201 4th Avenue North, Birmingham, Alabama, 35203.

JURISDICTION AND VENUE

19. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). There are at least 100 putative Class Members, the aggregated claims of the individual Class Members exceed the sum or value of $5,000,000 exclusive of interest and costs, and Plaintiff Antonio and Members of the proposed Class are citizens of states different from Defendants.

20. This Court has jurisdiction over Defendants through their business operations in this District, the specific nature of which (*i.e.*, the sale of insurance policies and the gathering of personal information) occurs in this District. Defendants intentionally avail themselves of the markets within this District to render the exercise of jurisdiction by this Court just and proper.

21. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events and omissions giving rise to this action occurred in this District.

FACTUAL ALLEGATIONS

Defendants' Business

22. Defendant Kemper Corporation is one of the nation's leading specialized insurers, offering insurance for home, auto, life, health, and valuables and serving approximately 6.2 million policies. Kemper is licensed to sell insurance in all fifty (50) states and the District of Columbia.[1]

23. 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

[1] https://www.kemper.com/about-kemper (last accessed Apr. 9, 2021).

was one of the largest nonstandard auto insurers in the country.[2]

24. There is a unity of identity between the Defendants, with Infinity Insurance Company being a wholly owned subsidiary of Kemper.

25. In the ordinary course of doing business with Defendants, customers and prospective customers are required to provide Defendants with sensitive, personal and private information 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's a homeowner on the policy;
- Vehicle information; and
- Other driver information.

26. As a condition of seeking to become a policyholder with Defendants, Plaintiff Antonio was required to disclose some or all of the Private Information listed above, and disclosed her Social Security number to Defendant Infinity.

[2] https://www.businesswire.com/news/home/20180213006637/en/Kemper-to-Acquire-Infinity-in-1.4-Billion-Transaction (last accessed Apr. 9, 2021).

27. Defendants have promulgated, and place on their website, privacy policies for all of the jurisdictions in which they operate, including Florida.

28. In the course of collecting Private Information from consumers, including Plaintiff Antonio, Defendants promise to provide confidentiality and security for personal information.

29. Defendant Kemper promises that it will protect its consumers' privacy, expressly stating on its website "Kemper promises to keep your personal information safe and confidential."[3]

30. 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."[4]

31. 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).

32. 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 maintains record of internet usage information and inferences from PII collected.[5]

33. Information collected by Defendants about its customers and prospective customers, including Plaintiff Antonio, includes driving record, claims history with other insurers, and credit history information.

34. Defendant Infinity similarly promises and represents that it "take[s] reasonable

[3] https://customer.kemper.com/auto/privacy-policy (last accessed Apr. 9, 2021).
[4] *Id.*
[5] *Id.*

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."

35. Because of the highly sensitive and personal nature of the Private Information Defendants acquire and store with respect to its consumers, Defendants further promise to "restrict access to personal information about you to those employees and agents who need to know that information to provide products or services to you. We maintain physical, electronic, and procedural safeguards that comply with state and federal regulations to guard your personal information."[6]

The Cyber-Attack and Data Breach

36. On or about March 16, 2021, Defendant Infinity began notifying consumers and state Attorneys General about a data breach that occurred on December 26, 2020 (the "Data Breach"). *See* Exhibit A, Plaintiff's Notice of Data Breach.

37. According to the Notice of Data Breach letter, and letters sent to state Attorneys General, Infinity's security team "detected indications of a potential security incident on December 26, 2020," and "identified brief, unauthorized access to files on certain company servers in [its] network on two days in December 2020." *Id.*

38. Plaintiff Antonio was informed that her name and Social Security Number were accessed. *Id.*

39. The notice letter apologized for the "inconvenience" and offered a "complementary one-year membership" to Experian IdentityWorksSM credit monitoring service. The notice

[6] *Id.*

advised Plaintiff Antonio to "remain vigilant by reviewing your financial account statements for any unauthorized activity." *Id*.

40. Based on the Notice of Data Breach letter she received (Exhibit A to this Complaint), which informed Plaintiff that her Private Information was accessed on Defendants' network and computer systems, Plaintiff believes her name and Social Security number were stolen from Defendants' networks (and subsequently sold) in the Cyber-Attack.

41. Defendants had obligations created by contract, industry standards, common law, and representations made to Plaintiff and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

42. Plaintiff and Class Members provided their Private Information 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.

43. 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.

44. Data breaches, including those perpetrated against the banking/credit/financial sector of the economy, have become widespread.

45. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.[7]

46. Of the 1,473 recorded data breaches, 108 of them were in the banking/credit/financial industry, with the number of sensitive records being exposed exceeding

[7] 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 accessed Dec. 10, 2020).

100 million. In fact, over 62% of the 164 million sensitive records exposed in data breaches in 2019 were exposed in those 108 breaches in the banking/credit/financial sector.[8]

47. The 108 reported financial sector data breaches reported in 2019 exposed 100,621,770 sensitive records, compared to 2018 in which only 1,778,658 sensitive records were exposed in financial sector breaches.[9]

48. Indeed, cyber-attacks, 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.

Defendants Fail to Comply with FTC Guidelines

49. The Federal Trade Commission ("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.

50. 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 problems. The guidelines also recommend that businesses use an intrusion detection system to

[8] *Id*.
[9] *Id* at 15.

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.

51. 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.

52. 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.

53. 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.

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

Defendants Fail to Comply with Industry Standards

55. 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.

56. 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; training staff regarding critical points.

57. 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.

58. 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.

Defendants' Breach

59. Defendants breached their obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because they failed to properly maintain and safeguard their computer systems, networks, and data. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect customers' and prospective customers' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions, brute-force attempts, and clearing of event logs;

d. Failing to apply all available security updates;

e. Failing to install the latest software patches, update its firewalls, check user account privileges, or ensure proper security practices;

f. Failing to practice the principle of least-privilege and maintain credential hygiene;

g. Failing to avoid the use of domain-wide, admin-level service accounts;

h. Failing to employ or enforce the use of strong randomized, just-in-time local administrator passwords; and

i. Failing to properly train and supervise employees in the proper handling of inbound emails.

60. As the result of computer systems in dire need of security upgrading and inadequate procedures for handling cybersecurity threats, Defendants negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information.

Data Breaches Cause Disruption and Put Consumers at an Increased Risk of Fraud and Identity Theft

61. Defendants were well aware that the Private Information they collect is highly sensitive, and of significant value to those who would use it for wrongful purposes, like the cyber-criminals who perpetrated this Cyber-Attack.

62. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face

"substantial costs and time to repair the damage to their good name and credit record."[10]

63. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven (7) years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[11]

64. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

65. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information.

66. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

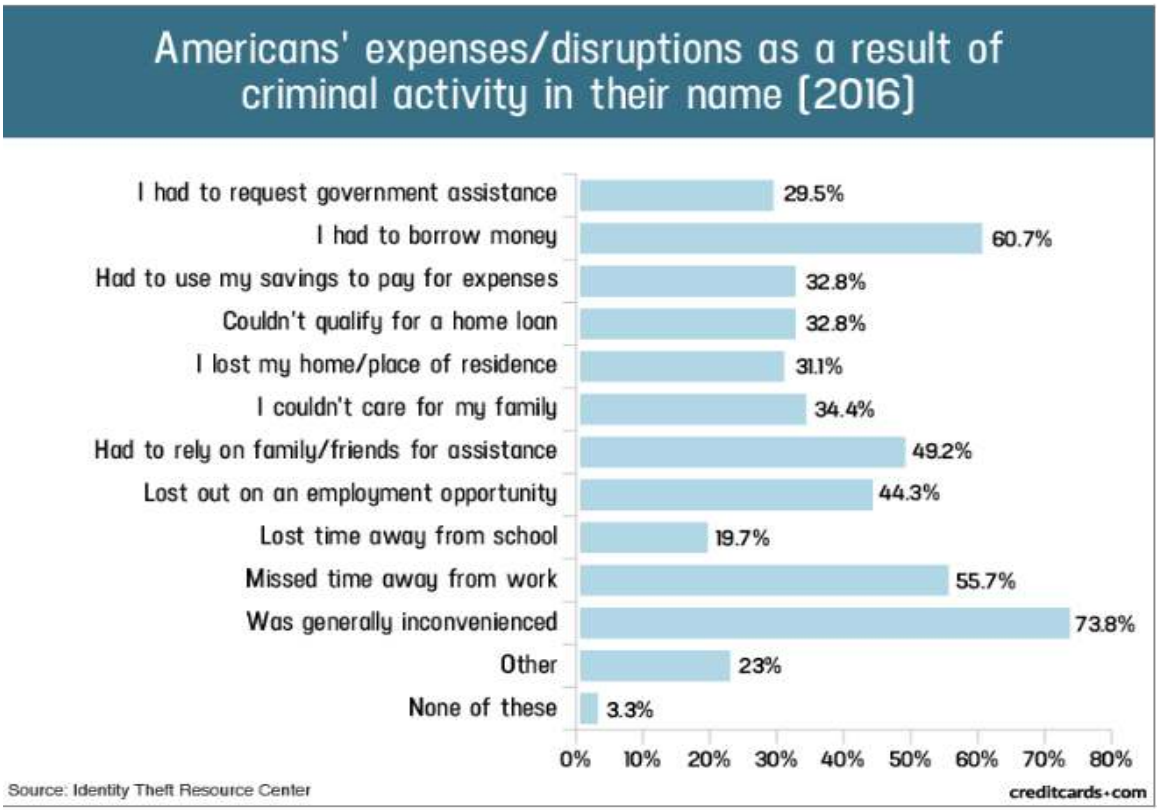
67. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[12]

---

[10] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited Apr. 12, 2019) ("GAO Report").

[11] *See* https://www.identitytheft.gov/Steps (last visited Dec. 8, 2020).

[12] *See* Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (Oct. 23, 2020) https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last accessed Dec. 10, 2020).



68. What's more, theft of Private Information is also gravely serious. PII is a valuable property right.[13]

69. Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

70. It must also be noted there may be a substantial time lag—measured in years—between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

[13] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

> [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.

See GAO Report at 29.

71. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

72. Indeed, a robust "cyber black market" exists in which criminals openly post stolen Private Information on multiple underground Internet websites.

73. Where the most private information belonging to Plaintiff and Class Members was accessed and removed from Defendants' network, and entire batches of that stolen information already dumped by the cyberthieves on the cyber black market, there is a strong probability that additional batches of stolen information are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

74. Thus, Plaintiff and Class Members must vigilantly monitor their financial accounts for many years to come.

75. While credit card information can sell for as little as $1-$2 on the black market, other more sensitive information can sell for as much as $363 according to the Infosec Institute. PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

76. The PII of consumers 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.

77. Social Security numbers are among the worst kind of personal 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 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.

78. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

79. Moreover, it is not an 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. Even then, a new Social Security number may not be effective, as "[t]he 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."[14]

80. This data, as one would expect, demands a much higher price on the black market.

[14] Brian 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-millions-worrying-about-identity-theft (last visited Oct. 28, 2020).

Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[15]

81. At all relevant times, Defendants knew or reasonably should have known these risks, the importance of safeguarding Private Information, and the foreseeable consequences if its data security systems were breached, and strengthened their data systems accordingly. Defendants were put on notice of the substantial and foreseeable risk of harm from a data breach, yet they failed to properly prepare for that risk.

Plaintiff's and Class Members' Damages

82. To date, Defendants have done absolutely nothing to provide Plaintiff and Class Members with relief for the damages they have suffered as a result of the Cyber-Attack and data breach, including, but not limited to, the costs and loss of time they incurred because of the Cyber-Attack. Defendants have only offered twelve (12) months of inadequate identity 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 Cyber-Attack.

83. Moreover, the twelve (12) months of credit monitoring offered to persons whose private information 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.

[15] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, Feb. 6, 2015, http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Oct. 28, 2020).

84. Defendants entirely fail to provide any compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII.

85. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Cyber-Attack.

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

87. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

88. Plaintiff and Class Members have been, and face substantial risk of being targeted in the future, subjected to phishing, data intrusion, and other illegal based on their Private Information as potential fraudsters could use that information to target such schemes more effectively to Plaintiff and Class Members.

89. Plaintiff 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 Cyber-Attack.

90. Plaintiff and Class Members also suffered a loss of value of their Private

Information when it was acquired by cyber thieves in the Cyber-Attack. Numerous courts have recognized the propriety of loss of value damages in related cases.

91. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

92. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Cyber-Attack. 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 Cyber-Attack relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Placing "freezes" and "alerts" with credit reporting agencies;

g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

h. Contacting financial institutions and closing or modifying financial accounts;

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

j. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

k. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

93. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, 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.

94. Further, as a result of Defendants' conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information—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.

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

CLASS ACTION ALLEGATIONS

96. Plaintiff incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

97. Plaintiff brings this action individually and on behalf of all other persons similarly situated ("the Class") pursuant to Federal Rule of Civil Procedure 23.

98. Plaintiff proposes the following Class definition(s), subject to amendment based on information obtained through discovery. Notwithstanding, at this time, Plaintiff bring this action and seeks certification of the following Class:

> All persons whose PII was compromised as a result of the Cyber-Attack that Infinity Insurance Company discovered on or about December 26, 2020, and who were sent notice of the Data Breach.

Excluded from the Class are Defendants' officers, directors, and employees; any entity in which Defendants have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendants. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

99. Plaintiff reserves the right to amend the definitions of the Class or add a Class if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

100. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

101. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of thousands of Defendants' customers, prospective customers, policyholders, and employees whose data was compromised in the Cyber-Attack and data breach.

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

a) Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

b) Whether Defendants failed to implement and maintain reasonable security

procedures and practices appropriate to the nature and scope of the information compromised in the Cyber-Attack;

c) Whether Defendants' data security systems prior to and during the Cyber-Attack complied with applicable data security laws and regulations;

d) Whether Defendants' data security systems prior to and during the Cyber-Attack were consistent with industry standards;

e) Whether Defendants owed a duty to Class Members to safeguard their Private Information;

f) Whether Defendants breached their duty to Class Members to safeguard their Private Information;

g) Whether computer hackers obtained Class Members' Private Information in the Cyber-Attack;

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

i) Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendants' misconduct;

j) Whether Defendants' conduct was negligent;

k) Whether Defendants' actions violated federal law;

l) Whether Defendants violated Florida's Deceptive and Unfair Trade Practices Act, Florida Statute § 501.203, *et seq*.; and

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

103. Typicality. Plaintiff's claims are typical of those of other Class Members because

Plaintiff's information, like that of every other Class Member, was compromised in the Cyber-Attack.

104. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the members of the Class, and has no interests antagonistic to those of other Class Members. Plaintiff's Counsel are competent and experienced in litigating class actions.

105. Predominance. Defendants have engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

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

107. Defendants have acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a

class-wide basis.

CAUSES OF ACTION

COUNT I

NEGLIGENCE
(On Behalf of Plaintiff and All Class Members)

108. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 107 above as if fully set forth herein.

109. Defendants required Plaintiff and Class Members to submit non-public personal information in order to obtain services or purchase life insurance products.

110. By collecting and storing this data in its computer property, and sharing it and using it for commercial gain, Defendants had a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendants' duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

111. Defendants owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

112. Defendants' duty of care to use reasonable security measures arose Defendants were in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

113. In addition, Defendants had a duty to employ reasonable security measures under

Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

114. Defendants breached their duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Failure to periodically ensure that their network system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to detect in a timely manner that Class Members' Private Information had been compromised;

f. Failing to timely notify Class Members about the Cyber-Attack so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

g. Failing to have mitigation and back-up plans in place in the event of a cyber-attack and data breach.

115. It was foreseeable that Defendants' failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the financial services industry.

116. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

117. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Cyber-Attack and data breach.

118. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II

Negligence *Per Se*
(On Behalf of Plaintiff and All Class Members)

119. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 107 above as if fully set forth herein.

120. Pursuant to Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

121. Plaintiff and Class Members are within the class of persons that the FTCA was intended to protect.

122. The harm that occurred as a result of the Data Breach is the type of harm the FTCA was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

123. Defendants breached their duties to Plaintiff and Class Members under the Federal Trade Commission Act by failing to provide fair, reasonable, or adequate computer systems and

data security practices to safeguard Plaintiff's and Class Members' Private Information.

124. Defendants' failure to comply with applicable laws and regulations constitutes negligence *per se.*

125. But for Defendants' wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

126. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendants' breach of its duties. Defendants knew or should have known that they were failing to meet their duties, and that Defendants' breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

127. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

COUNT III

Violation of Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. §§ 501.201, *et seq*. (On Behalf of Plaintiff and the Class)

128. Plaintiff realleges each and every allegation contained above, and incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

129. This cause of action is brought pursuant to the Florida Deceptive and Unfair Trade Practices Act ("FDUTPA"), Fla. Stat. §§ 501.201, *et seq.* The express purpose of the FDUPTA is to "protect the consuming public . . . from those who engage in unfair methods of competition, or unconscionable, deceptive, or unfair acts or practices in the conduct of any trade or commerce." Fla. Stat. § 501.202(2).

130. Defendants' sale of goods and services (insurance) at issue in this cause are "consumer transaction[s]" within the scope of the FDUTPA. Fla. Stat. §§ 501.201–501.213.

131. Plaintiff is a "consumer[s]" as defined by the FDUTPA. Fla. Stat. § 501.203.

132. Defendants are engaged in trade or commerce within the meaning of the FDUTPA.

133. The FDUTPA declares as unlawful "unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce." Fla. Stat. § 501.204(1).

134. The FDUPTA provides that "due consideration be given to the interpretations of the Federal Trade Commission and the federal courts relating to Section 5(a)(1) of the Trade Commission Act." Fla. Stat. § 501.204(2). Defendants' unfair and deceptive practices are likely to mislead—and have misled—the consumer acting reasonably under the circumstances. Fla. Stat. § 500.04; 21 U.S.C. § 343. As set forth above, Defendants' Data Breach was a result of its substandard data and cybersecurity practices in violation of the state and federal requirements as set forth above.

135. Pursuant to the FCRA, the FTCA, and Florida law (Fla. Stat. § 456.057 & § 501.171), Defendants were required by law to maintain adequate and reasonable data and cybersecurity measures to maintain the security and privacy of Plaintiff's and Class Members' Personal Information.

136. Defendants violated the FDUPTA by engaging in the unfair and deceptive practices described above, which offend public policies and are immoral, unethical, unscrupulous and substantially injurious to consumers. At all times material herein, Defendants failed to maintain adequate and reasonable data and cybersecurity protocols for Plaintiff's and Class Members' Personal Information in violation of state and federal laws and its own privacy practices and

policies.

137. Plaintiff has standing to pursue this claim because they have been injured by virtue of suffering a loss of privacy, money and/or property as a result of the wrongful conduct alleged herein. Plaintiff would not have purchased Defendants' goods and services (or paid as much) had she known the truth about Defendants' substandard and shoddy data and cybersecurity measures. Moreover, Defendants will continue to maintain Plaintiff's and Class Members' Personal Information for the indefinite future, giving them a strong interest in ensuring such data is protected with state of the art, industry standards to prevent future data breaches.

138. As a direct result of Defendants' actions and omissions of material facts, Plaintiff and Class Members did not obtain the value of the goods and services for which they paid; were induced to pay for (or pay more for) goods and services (insurance) that they otherwise would not have.

139. The damages suffered by Plaintiff and Class Members were directly and proximately caused by the deceptive, misleading and unfair practices of Defendants, as described above.

140. Plaintiff and Class Members seek declaratory judgment that Defendants' data security practices were not reasonable or adequate and caused the Data Breach under the FDUTPA, as well as injunctive relief enjoining the above described wrongful acts and practices of the Defendants and requiring Defendants to employ and maintain industry accepted standards for data management and security, including, but not limited to, proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing. Fla. Stat. § 501.211(1).

141. Additionally, Plaintiff and Class Members make claims for actual damages,

nominal damages, attorneys' fees and costs. Fla. Stat. §§ 501.2105, 501.211(2).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

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

b) For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

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

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

e) Ordering Defendants to pay for not less than three (3) years of credit monitoring services for Plaintiff and the Class;

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

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

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

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

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

Dated: April 9, 2021

Respectfully submitted,

/s/ *Gary M. Klinger*

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
Phone: (202) 429-2290
Fax: (202) 429-2294
dlietz@masonllp.com
gmason@masonllp.com

Attorneys for Plaintiff and the Proposed Class