UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

JAY HEATH, EDWARD SHAPIRO, and DAISY BECERRA LOPEZ, individually and on behalf of all others similarly situated, Plaintiffs, v. INSURANCE TECHNOLOGIES CORP. and ZYWAVE, INC., Defendants.	Case No.: 3:21-cv-01444-N **FIRST AMENDED COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Jay Heath, Edward Shapiro, and Daisy Becerra Lopez ("Plaintiffs") bring this Class Action Complaint against Defendants Insurance Technologies Corporation ("ITC") and Zywave, Inc. ("Zywave" 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. Zywave and its wholly owned subsidiary, ITC, are information technology services companies. Among other services, Defendants supply a cloud-based agency management system to insurance companies called AgencyMatrix that brokers use to manage their businesses.

2. On or about May 10, 2021, ITC began notifying customers and state Attorneys General about a data breach that occurred on February 27, 2021 (the "Data Breach").[1] Hackers obtained information from ITC including personally identifiable information ("PII")[2] of thousands

[1] https://oag.ca.gov/ecrime/databreach/reports/sb24-540398 (last visited Nov. 15, 2021).

[2] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

of its clients' customers, potential customers, and other individuals, including, but not limited to, their names, Social Security numbers, driver's license numbers, dates of birth, and username/password information.

3. Defendant ITC represents on its website that it protects personal information: "We protect the security of your personal information. We take steps to protect your data from loss, misuse, alteration, destruction, or unauthorized access."[3]

4. 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 to assist them in engaging in identify theft and financial fraud. Because of Defendants' Data Breach, Class members' PII is still available and may be for sale on the dark web for criminals to access and abuse. Impacted consumers now face a lifetime risk of identity theft.

5. As the President of ITC acknowledged in a video posted to the ITC website: "Seventy-one percent of data breaches target small businesses. Consider the information stored in your office and any system you use…You've got a ton of personally identifiable information."[4]

6. ITC's President also represented that "security is not one way. We all must take it seriously *and be accountable to each other*. Not just for ourselves but also our customers."[5]

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

8. 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 to ascertain the

---

3 https://www.getitc.com/privacy.aspx (last visited Nov. 15, 2021).

4 https://resources.getitc.com/videos/security-matters (last visited Nov. 15, 2021).

5 *Id*. (last visited Nov. 15, 2021).

existence of security vulnerabilities, address them promptly and to detect security incidents. Defendants' conduct amounts to negligence and violates federal and state statutes.

9. Plaintiffs and similarly situated individuals have suffered injury as a result of Defendants' conduct. These injuries include, but are not limited to: (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; and (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; and (iv) deprivation of rights they possess under state consumer protection statutes.

PARTIES

10. Plaintiff Jay Heath is a citizen of Maryland residing in Baltimore, Maryland.

11. Plaintiff Edward Shapiro is a citizen of Pennsylvania residing in Philadelphia, Pennsylvania.

12. Plaintiff Daisy Becerra Lopez is a citizen of California residing in Stockton, California.

13. Defendant ITC is a Texas corporation with its principal place of business at 1415 Halsey Way Ste. 314, Carrollton, Texas, 75007. ITC offers information technology services and according to its website serves more than 200 insurance companies and more than 7,000 agencies.

14. Defendant Zywave is a Wisconsin corporation with its principal place of business at 10100 W. Innovation Dr., Ste. 300, Milwaukee, Wisconsin, 53226. Zywave is an insurance technology firm serving more than 6,000 carriers including, it claims, all of the top 100 U.S. insurance firms, with annual gross revenues in excess of $25 million.

15. ITC is a wholly-owned subsidiary of Zywave.

JURISDICTION AND VENUE

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

proposed class, and at least one member of the class is a citizen of a state different from Defendant.

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

18. 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 ITC 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

19. Defendant ITC is a provider of marketing, rating, and management software and services for insurance companies and agents. ITC sells its services and products across the United States.[6]

20. Defendant Zywave is an insurance technology provider focusing on cloud-based sales management, client delivery, content, and analytics solutions. Zywave acquired ITC in 2020 to expand its customer base to more than 15,000 insurance organizations globally.[7]

21. There is a unity of identity between the Defendants because Defendant ITC is a wholly owned subsidiary of Zywave. In fact, on August 16, 2021, Defendants responded together in one document to the separate 30-day notice letters sent to both Zywave and ITC by Plaintiff Lopez on or about June 25, 2021.

22. In the ordinary course of doing business with Defendants, Defendants collect sensitive PII from consumers such as:

- Name;
- Address;

[6] https://www.getitc.com/about/ (last visited Nov. 15, 2021).

[7] https://www.zywave.com/news/zywave-acquires-insurtech-frontrunner-itc-becomes-only-provider-to-offer-front-office-solutions-for-independent-insurance-agencies-across-all-lines-of-business/ (last visited Nov. 15, 2021).

- Phone number;
- Driver's license number;
- Social Security number;
- Date of birth;
- Email address;
- Gender; and
- Username and password.

23. In the course of collecting PII from consumers, including Plaintiffs, Defendants promise to provide confidentiality and security for personal information, including by promulgating and placing privacy policies on their website.

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

> We protect the security of your personal information. We take steps to protect your data from loss, misuse, alteration, destruction, or unauthorized access. We use sophisticated security technologies to secure users' ordering information, username, and password. We encrypt users' ordering information, username, and password (including users' credit card account number) using Secure Socket Layer ("SSL") technology. SSL is a proven coding system that lets your browser automatically encrypt, or scramble, data before you send it to us. To support this technology, users must have an SSL-capable browser. SSL is one of the safest encryption technologies available.[8]

25. Defendant Zywave similarly promises in its privacy policy: "Zywave will not otherwise disclose your personal information to any person or any organization, and Zywave will never sell your personal information to anyone."[9]

26. Zywave also represents that it "is committed to the security of personal information and has policies and procedures in place to protect the privacy of your personal information. Personal information shall be protected in a manner commensurate with its sensitivity and

[8] https://www.getitc.com/privacy.aspx (last visited Nov. 15, 2021).

[9] https://www.zywave.com/privacy-statement/ (last visited Nov. 15, 2021).

reasonable steps will be taken to prevent it from being stolen, lost, accessed, copied, used or modified without permission."[10]

27. Defendants, however, failed to protect and safeguard Plaintiffs' and Class members PII. In fact, there is no indication that Defendants followed even their most basic promises; for example, ITC does not claim in the notice letters that any of the stolen PII was encrypted or redacted, including usernames and passwords.

The Data Breach

28. On or about May 10, 2021, Defendant ITC began notifying consumers and state Attorneys General about a data breach that occurred on February 27, 2021.

29. According to the Notice of Data Breach letters and letters sent to state Attorneys General, "an unauthorized third party gained access to [ITC's] AgencyMatrix application," and "acquired certain personal information stored in that application."[11]

30. According to the Notice, ITC "immediately commenced an investigation" and contained the incident on March 4, 2021.[12]

31. However, despite first learning of the Data Breach in February 2021 and concluding the investigation in March 2021, Defendants did not take any "measures" to notify affected Class members for over two months, on or about May 10, 2021.

Defendants Were Aware of the Risks of a Data Breach

32. Defendants had obligations created by contract, industry standards, common law, and representations made to Plaintiffs and Class members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

33. Plaintiffs and Class members provided their PII to Defendants with the reasonable expectation and mutual understanding that Defendants would comply with their obligations to

---

10 *Id*.

11 https://oag.ca.gov/system/files/ITC%20-%20Model%20Notification%20to%20Insureds%20%28Updated%29_1_1.pdf (last visited Nov. 15, 2021).

12 *Id*.

keep such information confidential and secure from unauthorized access.

34. Defendants' data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches in the information technology sector preceding the date of the breach.

35. Data breaches, including those perpetrated against the information technology sector of the economy, have become widespread for some. For example, the United States saw 1,244 data breaches in 2018 and had 446.5 million exposed records.[13] Defendants understand this reality because ITC's CEO told customers of his product to "consider the information stored in your office and any system you use…You've got a ton of personally identifiable information" and that "security is not one way. We all must take it seriously and be accountable to each other. Not just for ourselves but also our customers."[14]

36. 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 repeated warnings to potential targets, so they are aware of, and prepared for, potential attacks. 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.

37. 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.[15] Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank and finance fraud.[16]

---

13 https://www.varonis.com/blog/data-breach-statistics (last visited Nov. 15, 2021).

14 https://resources.getitc.com/videos/security-matters (last visited Nov. 15, 2021).

15 *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 Nov. 15, 2021).

16 *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 number, date of birth, official State or government issued driver's license or identification number,

38. The PII of Plaintiffs and members of the Classes was taken by hackers to engage in identity theft or 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.

39. 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, 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 members of the Classes a result of a breach.

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

41. 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

42. 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.

43. 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 expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone

alien registration number, government passport number, employer or taxpayer identification number." *Id*.

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.

44. 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.

45. 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.

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

47. 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

48. 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.

49. Best cybersecurity practices that are standard in the information technology 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.

50. 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.

51. 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

52. 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 or changed, if at all, and can be easily used to perpetrate identity theft and other types of fraud.

53. 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.[17]

54. Social Security numbers, for example, 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

[17] *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 Nov. 15, 2021).

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.[18]

55. 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.

56. 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."[19]

57. 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 especially true if your other personal information, such as your name and address, remains the same.

---

[18] SSA, *Identity Theft and Your Social Security Number*, https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Nov. 15, 2021).

[19] 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 Nov. 15, 2021).

> 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.[20]

58. 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 constitutes a dream for hackers and a nightmare for Plaintiffs and the Classes. Stolen personal data of Plaintiffs and members of the Classes represents essentially one-stop shopping for identity thieves.

59. 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.

60. 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.[21]

61. 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

---

[20] 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 Nov. 15, 2021).

[21] *See* https://www.gao.gov/assets/gao-07-737.pdf (June 2007) at 29 (last visited Nov. 15, 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.

62. 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.

63. 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.

64. 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.

65. 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."[22]

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

[22] 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 Nov. 15, 2021).

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

67. According to a recent article in the New York Times, cyber thieves are using driver's licenses obtained via insurance company application prefill processes to submit and fraudulently obtain unemployment benefits.[23] 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).

The Plaintiffs' Experiences

Plaintiff Jay Heath

68. Plaintiff Jay Heath received the Notice of Data Breach from Defendant ITC, dated May 10, 2021, on or about that date. The Notice informed him that Defendants lost a file containing at least his full name, Social Security number, and possibly his date of birth and/or username and password for the AgencyMatrix application.

69. As a result of the Data Breach, Mr. Heath made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification letter, including but not limited to: researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; and researching credit monitoring and identity theft protection, including those offered by ITC. Mr. Heath now reviews his credit monitoring reports and/or checking account statements for irregularities two or three times per week, each time for approximately 5 minutes. This is valuable time Mr. Heath otherwise would have spent on other activities, including but not limited to work and/or recreation.

70. Mr. Heath is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

---

[23] *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 Nov. 15, 2021)

71. Mr. Heath suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that ITC obtained from Mr. Heath; (b) violation of his privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

72. Moreover, subsequent to the Data Breach, Mr. Heath also experienced a significant increase in the amount of suspicious, unsolicited phishing telephone calls he receives. Each day, Mr. Heath receives at least two scam phone calls, each of which appear to be placed with the intent to obtain personal information to commit identity theft by way of a social engineering attack.

73. Mr. Heath has spent a significant amount of time since the Data Breach responding to the impacts of the Data Breach. The time spent dealing with the fallout from the Data Breach is time Mr. Heath otherwise would have spent on other activities, such as work and/or recreation.

74. As a result of the Data Breach, Mr. Heath anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Mr. Heath is presently and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Edward Shapiro

75. Plaintiff Edward Shapiro received the Notice of Data Breach from Defendant ITC, dated May 10, 2021, on or about that date. The Notice informed him that Defendants lost a file containing, at least, his full name, driver's license, date of birth, and username and password for the AgencyMatrix application.

76. As a result of receiving the Data Breach notice, Mr. Shapiro has spent time dealing with the consequences of the breach, including confirming the legitimacy of the Data Breach, self-monitoring his accounts, exploring credit monitoring and identity theft insurance options, and calling in to sign up for the credit monitoring service offered by Defendants.

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

78. Mr. Shapiro is not aware of any other data breaches that could have resulted in the theft of his driver's license number, username or password. He is very careful about sharing his PII, and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

79. Mr. Shapiro stores any and all documents containing his PII in a safe and secure digital location and shreds 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.

80. Mr. Shapiro 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.

81. Mr. Shapiro 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.

82. Mr. Shapiro 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.

83. Mr. Shapiro 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.

84. Mr. Shapiro has become scared, nervous, and 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. As a result of the Data Breach, Mr. Shapiro is presently and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Daisy Becerra Lopez

85. Plaintiff Daisy Becerra Lopez received the Notice of Data Breach from Defendant ITC, dated May 10, 2021, on or about that date. The Notice informed her that Defendants lost a file containing at least her full name, driver's license number, and possibly her date of birth and/or username and password for the AgencyMatrix application.

86. As a result of the Data Breach, Ms. Lopez made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification letter, including but not limited to: researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; and researching credit monitoring and identity theft protection services, including those offered by ITC. Ms. Lopez now regularly reviews her credit monitoring reports and/or checks her account statements for irregularities. This is valuable time Ms. Lopez otherwise would have spent on other activities, including but not limited to work and/or recreation.

87. Ms. Lopez is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

88. Ms. Lopez suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of property that ITC obtained from Ms. Lopez; (b) violation of her privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

89. Moreover, subsequent to the Data Breach, Ms. Lopez also experienced a significant increase in the amount of suspicious, unsolicited phishing telephone calls and emails she receives. Each day, Ms. Lopez receives at least four scam phone calls/emails, each of which appear to be placed with the intent to obtain personal information to commit identity theft by way of a social engineering attack.

90. Ms. Lopez has spent a significant amount of time since the Data Breach responding to the impacts of the Data Breach. The time spent dealing with the fallout from the Data Breach

is time Ms. Lopez otherwise would have spent on other activities, such as work and/or recreation.

91. As a result of the Data Breach, Ms. Lopez anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Ms. Lopez is presently and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiffs' and Class Members' Damages

92. To date, Defendants have done absolutely nothing to provide Plaintiffs and Class members with relief for the damages they have suffered because 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 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 Data Breach. What is more, Defendants place the burden squarely on Plaintiffs and Class members by requiring them to expend time signing up for that service, as opposed to automatically enrolling all victims of this cybercrime.

CLASS ALLEGATIONS

93. Plaintiffs bring this nationwide class action pursuant to rules 23(b)(2), 23(b)(3), and 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 on or about May 10, 2021 (the "Nationwide Class").

94. The Maryland Subclass is defined as follows:

> All natural persons residing in Maryland whose PII was compromised in the Data Breach announced on or about May 10, 2021 (the "Maryland Subclass").

95. The Pennsylvania Subclass is defined as follows:

All natural persons residing in Pennsylvania whose PII was compromised in the Data Breach announced on or about May 10, 2021 (the "Pennsylvania Subclass").

96. The California Subclass is defined as follows:

All natural persons residing in California whose PII was compromised in the Data Breach announced on or about May 10, 2021 (the "California Subclass").

97. The Pennsylvania, Maryland and California Subclasses are referred to herein as the "Statewide Subclasses" and together with the Nationwide Class, are collectively referred to herein as the "Classes."

98. 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.

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

100. **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.

101. **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 Defendants violated the consumer protection statutes invoked below; and

k. Whether Plaintiffs and the other members of the Classes are entitled to money damages in an amount sufficient to pay for identity theft protection and other monetary relief;

102. **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.

103. **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.

104. **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.

105. 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 Class as a whole and as to each Subclass as a whole.

106. 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 (including money damages in an amount sufficient to pay for identity theft protection) or injunctive relief, and/or punitive damages as a result of Defendants' wrongful conduct.

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

107. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 106.

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

109. The legal duties owed by Defendants to Plaintiffs and 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 Class members in its possession;

b. To protect PII of Plaintiffs and 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 Class members of the Data Breach.

110. 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.

111. Various FTC publications and data security breach orders further form the basis of Defendants' duty. Plaintiffs and 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.

112. Defendants breached their duties to Plaintiffs and 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.

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

114. 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 Class members' PII during the period it was within Defendants' possession and control.

115. Defendants breached the duties they owe to Plaintiffs and 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.

116. Due to Defendants' conduct, Plaintiffs and Nationwide Class members are entitled to money damages in an amount sufficient to pay for identity theft protection services for the remainder of their respective lives. Identity theft protection services are reasonable here as it provides protection to consumers from identity theft and can alert them when a criminal is seeking

to engage in identity theft. The PII taken can be used for identity theft and other types of financial fraud against the Nationwide Class members.

117. 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 present and continuing 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.

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

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

119. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 106.

120. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant's, 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.

121. 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.

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

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

124. 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.

125. As a direct and proximate result of Defendants' negligence per se, Plaintiffs and members of the 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 its current and former employees and customers in its 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.

126. 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 Maryland's Personal Information Privacy Act,
Md. Comm. Code §§ 14-3501, et seq.
(On behalf of Plaintiff Heath and the Maryland Subclass)

127. Mr. Heath re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 106.

128. In relevant part, the Maryland Personal Information Privacy Act ("PIPA") states:

> To protect Personal Information from unauthorized access, use, modification, or disclosure, a business that owns or licenses Personal Information of an individual residing in the State shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of Personal Information owned or licensed and the nature and size of the business and its operations.

Md. Comm. Code § 14-3503(a).

129. Thus, the plain language of PIPA requires businesses to implement and maintain "reasonable security practices and procedures" based on the personal information they collect.

130. "Personal Information" is defined to include "[a]n individual's first name or first initial and last name in combination with any one or more of the following data elements, when the name or the data elements are not encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable:...a passport number...[a]n account number, a credit card number, or a debit card number, in combination with any required security code, access code, or password, that permits access to an individual's financial account." Md. Comm. Code § 14-3503(e)(1).

131. Further, PIPA requires a business that has discovered or has been notified of a security breach to conduct a prompt investigation to determine if Personal Information has or will be misused. Md. Comm. Code § 14-3504(b)(1). If so, "the business shall notify the individual of the breach" and that notification "shall be given as soon as reasonably practical after the business discovers or is notified of the breach of a security system." Md. Comm. Code §§ 14-3504(b)(2), 14-3504(c)(2).

132. As alleged herein, Defendants did not maintain reasonable security measures appropriate to the nature of their Personal Information as required by PIPA.

133. As alleged herein, Defendants did not provide timely notice of their data breach as required by PIPA.

134. As a direct and proximate result of Defendant's actions, Mr. Heath and Maryland Subclass members have suffered and will continue to suffer injury, loss of privacy, and other economic and non-economic losses.

135. As a result, Mr. Heath and Maryland Subclass members are entitled to all monetary and non-monetary relief available for Defendants' violations of PIPA.

FOURTH CLAIM FOR RELIEF
Violation of Maryland's Consumer Protection Act
Deceptive and Unfair Trade Practices
Title 13, Section 13-101, *et seq.*
(On behalf of Plaintiff Heath and the Maryland Subclass)

136. Mr. Heath re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 106.

137. In relevant part, the Maryland Consumer Protection Act prohibits "unfair or deceptive trade practices" which include:

> False, falsely disparaging, or misleading oral or written statement, visual description, or other representation of any kind which has the capacity, tendency, or effect of deceiving or misleading consumers;...

> Representation that: Consumer goods, consumer realty, or consumer services have a sponsorship, approval, accessory, characteristic, ingredient, use, benefit, or quantity which they do not have;...
>
> Failure to state a material fact if the failure deceives or tends to deceive;...
>
> Advertisement or offer of consumer goods, consumer realty, or consumer services ...[w]ithout intent to sell, lease, or rent them as advertised or offered;...
>
> Deception, fraud, false pretense, false premise, misrepresentation, or knowing concealment, suppression, or omission of any material fact with the intent that a consumer rely on the same in connection with: [t]he promotion or sale of any consumer goods...or consumer service;...[or] [t]he subsequent performance of a merchant with respect to an agreement of sale, lease, or rental;...

Md. Comm. Code § 13-301.

138. In addition, a violation of the Maryland PIPA constitutes a violation of the Maryland CPA. See Md. Comm. Code § 14-3508 ("A violation of [subtitle 35: Maryland Personal Information Protection Act]: (1) Is an unfair or deceptive trade practice within the meaning of Title 13 of this article; and (2) Is subject to the enforcement and penalty provisions contained in Title 13 of this article.").

139. As alleged herein, Defendants violated the Maryland PIPA which constitutes a violation of the CPA.

140. As alleged herein, Defendants further violated the CPA based on their material representations and omissions regarding their data security.

141. As a direct and proximate result of Defendant's actions, Mr. Heath and Maryland Subclass members have suffered and will continue to suffer injury, loss of privacy, and other economic and non-economic losses.

142. As a result, Mr. Heath and Maryland Subclass members are entitled to all monetary and non-monetary relief available for Defendants' violations of the CPA.

FIFTH CLAIM FOR RELIEF
Pennsylvania Unfair Trade Practices and Consumer Protection Law
73 Pa. Cons. Stat. §§ 201-2 & 201-3, *et seq*.
(On behalf of Plaintiffs Shapiro and the Pennsylvania Subclass)

143. Mr. Shapiro re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 106.

144. Defendants are each a "person," as meant by 73 Pa. Cons. Stat. § 201-2(2).

145. Plaintiff and Pennsylvania Subclass members purchased goods and services in "trade" and "commerce," as meant by 73 Pa. Cons. Stat. § 201-2(3), primarily for personal, family, and/or household purposes.

146. Defendants engaged in unfair methods of competition and unfair or deceptive acts or practices in the conduct of their trade and commerce in violation of 73 Pa. Cons. Stat. Ann. § 201-3, including, but not limited to, the following:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class Members' Personal and Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Personal and Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1302d, *et seq*., and the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class Members' Personal Information and PHI, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1302d, *et seq*., and the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class Members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1302d, *et seq*., and the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801.

147. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

148. Defendants intended to mislead Mr. Shapiro and Class members and induce them to rely on their misrepresentations and omissions.

149. Had Defendants disclosed to Mr. Shapiro and Pennsylvania Subclass members that their data systems were not secure and thus vulnerable to attack, Defendants would have been

unable to continue in business and they would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendants held themselves out as secure and were trusted with sensitive and valuable PII regarding thousands of consumers, including Plaintiff Shapiro and the Pennsylvania Subclass members.

150. Defendants accepted the responsibility of each being a "steward of data" while keeping the inadequate state of their security controls secret from the public.

151. Mr. Shapiro and the Pennsylvania Subclass members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

152. Defendants acted intentionally, knowingly, and maliciously to violate the Pennsylvania Unfair Trade Practices and Consumer Protection Law, and recklessly disregarded Plaintiff's and Pennsylvania Subclass members' rights. Past data breaches in the healthcare industry put Defendant on notice that their security and privacy protections were inadequate.

153. As a direct and proximate result of Defendants' unfair methods of competition and unfair or deceptive acts or practices and Plaintiff's and the Pennsylvania Subclass members' reliance on them, Plaintiff Shapiro and Pennsylvania Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from disruption of medical care and treatment; fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal and Private Information.

154. Mr. Shapiro and the Pennsylvania Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $100

(whichever is greater), treble damages, attorneys' fees and costs, and any additional relief the Court deems necessary or proper.

SIXTH CLAIM FOR RELIEF
Declaratory Judgment
(On Behalf of Plaintiffs, the Nationwide Class, and the Statewide Subclasses Against All Defendants)

155. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 154 as though fully set forth herein.

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

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

158. 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.

159. 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.

160. 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 its 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.

SEVENTH CLAIM FOR RELIEF
Unjust Enrichment
(On Behalf of Plaintiffs, the Nationwide Class and the Statewide Subclasses Against All Defendants)

161. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 106.

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

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

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

165. 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.

166. 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.

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

168. But for Defendants' willingness and commitment to maintain privacy and confidentiality, that PII would not have been transferred to and untrusted 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, its shareholders, and its consumers.

169. 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.

170. 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 is secure from intrusion and theft by hackers and identity thieves.

171. 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.

172. 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.

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

EIGHTH CLAIM FOR RELIEF
Violation of California's Consumer Privacy Act, Cal. Civ. Code § 1798.150
(On behalf of Plaintiff Lopez and the California Class)

174. Ms. Lopez and the California Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 106.

175. Defendants violated section 1798.150(a) of the California Consumer Privacy Act ("CCPA") by failing to prevent Ms. Lopez's and the California Class's 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 Ms. Lopez and the California Class.

176. As a direct and proximate result of Defendants' acts, Ms. Lopez's and the California Class's PII was subjected to unauthorized access and exfiltration, theft, or disclosure through

Defendants' computer systems and/or from the dark web, where hackers may have further disclosed the PII of Ms. Lopez and the California Class.

177. As a direct and proximate result of Defendants' acts, Ms. Lopez and the California Class were injured and lost money or property, including but not limited to the loss of the California Class's legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

178. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard the California Class's 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 Ms. Lopez and the California Class.

179. Defendants are affiliated corporations organized or operated for the profit or financial benefit of their owners or shareholders with annual gross revenues in excess of twenty-five million dollars. Defendants do business in California and collect their customers' PII as defined in Cal. Civ. Code § 1798.140.

180. Pursuant to Section 1798.150(b) of the CCPA, Ms. Lopez gave written notice to Defendants of their violations of section 1798.150(a) by a certified mail dated June 25, 2021. Ms. Lopez sent separate letters to Zywave and ITC on that date, but received a single response by email from Defendants' counsel on August 16, 2021; the file name of the attachment is "Zywave Response to CCPA 30 Day Notice Re Lopez" and the subject line includes "Insurance Technologies Corp."

181. Defendants, however, failed to "actually cure" their violations within 30 days of the written notice, and failed, pursuant to § 1798.150(b) to "provide[] the consumer an express written statement that the violations have been cured and that no further violations shall occur."

182. As a result, Ms. Lopez and the California Class seek relief under § 1798.150(a), including, but not limited to, 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; injunctive or declaratory relief; any other relief the Court deems proper; and attorneys' fees and costs pursuant to Cal. Code Civ. Proc. § 1021.5.

NINTH CLAIM FOR RELIEF
Violation of California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq*. – Unlawful Business Practices and Deceptive Business Practices Act
(On behalf of Plaintiff Lopez and the California Class)

183. Plaintiffs and the Classes, or, alternatively, Ms. Lopez and the California Class, re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 106.

184. Defendants' business practices as complained of herein violate California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq*. (the "UCL").

185. In violation of the UCL, Defendants have engaged 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.

186. Specifically, Defendants engaged in unlawful acts and practices by failing to establish adequate security practices and procedures as set forth above, by soliciting and gathering the PII of Plaintiffs and the Class knowing that the information would not be adequately protected, and by storing the PII of Plaintiffs and the Class in an unsecure electronic system in violation of California's data breach statute, Cal. Civ. Code § 1798.81.5, which requires Defendants to undertake reasonable measures to safeguard the PII of Plaintiffs and the Class.

187. Defendants' actions and practices are "unfair" business practices in violation of the UCL, because, among other things, the gravity of the harm to Plaintiffs and the Class outweighs the utility of Defendants' conduct. This conduct includes Defendants' failure to adequately ensure the privacy, confidentiality, and security of the PII that Plaintiffs and the Class entrusted to Defendants and Defendants' failure to have adequate data security measures in place.

188. In addition, Defendants engaged in unlawful acts and practices by failing to timely and accurately disclose the data breach to Plaintiffs and the Class, in violation of the duties imposed by Cal. Civ. Code § 1798.82.

189. Defendants knew or should have known that their data security practices with respect to their computer systems were inadequate to safeguard the PII of Plaintiffs and the Class and that, as a result, the risk of a data breach or theft was highly likely. Defendants' unlawful practices and acts were negligent, knowing, and willful, and/or wanton and reckless with respect to the rights of Plaintiffs and the Class.

190. As a direct and proximate result of Defendants' unlawful acts and practices, Plaintiffs and the Class suffered injury in fact and lost money or property, including but not limited to the loss of their legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

191. In addition, Plaintiffs and the Class have incurred and will continue to incur economic damages related to the Data Breach, including loss of time and money spent remedying the Data Breach, and the costs of credit monitoring, purchasing credit reports, and implementing credit freezes to prevent opening of unauthorized account, among others.

192. Accordingly, Plaintiffs and the Class seek relief under Cal. Bus. & Prof. Code § 17200, et seq., including, but not limited to, restitution to Plaintiffs and the Class of money or property that Defendants acquired by means of their unlawful and unfair business practices, disgorgement of all profits Defendants received as a result 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.

TENTH CLAIM FOR RELIEF
Violation of California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, et seq. – Unfair Business Practices Act
(On behalf of Plaintiff Lopez and the California Class)

193. Plaintiffs and the Nationwide Class, or, alternatively, Ms. Lopez and the California Class, re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 106.

194. Defendants' practices as complained of herein violate California's UCL.

195. Specifically, Defendants engaged in unfair acts and practices by failing to establish adequate security practices and procedures, by soliciting and collecting the PII of Plaintiffs and the Class, knowing that the information would not be adequately protected, and by storing the PII in an unsecure electronic system. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or damaging to Plaintiffs and the Class as they were likely to deceive them into believing their PII was securely stored when it was not.

196. Defendants' actions and practices constitute "unfair" business practices in violation of the UCL, because, among other things, the gravity of the harm to Plaintiffs and the Class outweighs the utility of Defendants' conduct. This conduct includes Defendants' failure to adequately ensure the privacy, confidentiality, and security of the data Plaintiffs and the Class entrusted to them and Defendants' failure to have adequate data security measures in place.

197. Specifically, Defendants engaged in unfair acts and practices by failing to take appropriate action following the data breach to mitigate the effects of the Data Breach, enact adequate privacy and security measures, and protect the PII of Plaintiffs and the Class from further unauthorized disclosure, release, data breaches, and theft. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and damaging to Plaintiffs and the Class.

198. As a direct and proximate result of Defendants' unfair practices and acts, Plaintiffs and the Class were injured and lost money or property, including but not limited to the loss of their 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 their computer systems and data security practices were inadequate to safeguard the PII of Plaintiffs and the Class 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 Plaintiffs and the Class.

200. Accordingly, Plaintiffs and the Class seek relief under Cal. Bus. & Prof. Code § 17200, *et seq*., including, but not limited to, restitution to Plaintiffs and the Class of money or property that Defendants may have acquired by means of their unfair business practices, 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.

201. Plaintiffs and the Class reserve the right to amend this Complaint as of right to seek damages and relief under Cal. Civ. Code § 1798.100, *et seq.*

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all 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. Injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class members, including but not limited to an order:

   i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

   ii. requiring Defendants to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

   iii. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiffs and Class members unless Defendants can provide to the Court reasonable justification for the retention and use of such information

when weighed against the privacy interests of Plaintiffs and Class members;

iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiffs and Class members;

v. prohibiting Defendants from maintaining the PII of Plaintiffs and Class members on a cloud-based database;

vi. requiring Defendants to engage independent 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;

vii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendants to audit, test, and train their security personnel regarding any new or modified procedures;

ix. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised hackers cannot gain access to other portions of Defendants' systems;

x. requiring Defendants to conduct regular database scanning and securing checks;

xi. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class members;

xii. requiring Defendants to routinely and continually conduct internal training and

education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendants to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendants to meaningfully educate all Class members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

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.

Dated: November 19, 2021

Respectfully submitted,

/s/ M. Anderson Berry

M. ANDERSON BERRY**
ALEX SAUERWEIN*
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778
Facsimile: (916) 924-1829
aberry@justice4you.com
asauerwein@justice4you.com

JOE KENDALL
Texas Bar No. 11260700
KENDALL LAW GROUP, PLLC
3811 Turtle Creek Blvd., Ste. 1450
Dallas, TX 75219
Telephone: 214/744-3000
Facsimile: 214/744-3015
jkendall@kendalllawgroup.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

JOHN A. YANCHUNIS
RYAN MAXEY*
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: 813-559-4908
Facsimile: 813-222-4795
jyanchuins@forthepeople.com
rmaxey@forthepeople.com

Counsel for Plaintiffs and the Class

**Pro hac vice forthcoming*
***Pro hac vice*