THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

JENNIFER RAND, Individually and On Behalf Of A Class Similarly Situated, Plaintiff, v. THE TRAVELERS INDEMNITY COMPANY, Defendant.	Case No.: 7:21-cv-10744 (VLB) **JURY TRIAL DEMANDED**

AMENDED CLASS ACTION COMPLAINT

Plaintiff Jennifer Rand ("Plaintiff") brings this Amended Class Action Complaint ("Amended Complaint"), on behalf of herself and all others similarly situated, against Defendant The Travelers Indemnity Company ("Travelers" or "Defendant"), alleging as follows based upon information and belief, and investigation of counsel, except as to the allegations specifically pertaining to her, which are based on personal knowledge.

PARTIES

1. Plaintiff is a citizen of Westchester County, State of New York.

2. Defendant is an insurance company, incorporated in the State of Connecticut with its headquarters in the State of Connecticut, and doing business in this District and throughout the United States.

3. In the alternative, Defendant is an insurance company, part of the Travelers Companies, Inc. conglomerate, which is incorporated in the State of Minnesota with its headquarters in New York State and doing business in this District and throughout the United States.

4. Defendant The Travelers Indemnity Company[1] is a company that issues automobile no-fault and liability policies, with its principal place of business at One Tower Square in Hartford, Connecticut.

JURISDICTION AND VENUE

5. The Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 as it arises under the laws of the United States, including the Driver's Privacy Protection Act, 18 U.S.C. §§ 2721, *et seq.*

6. Alternatively, the Court has subject matter jurisdiction under the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d) because Plaintiff and Defendant are citizens of different states and the amount in controversy exceeds $5,000,000.

7. The Court also has supplemental jurisdiction over Plaintiff's state law claims pursuant to 28 U.S.C. § 1367(a) because the state law claims are related to claims in the action within such original jurisdiction and they form part of the same case or controversy under Article III of the United States Constitution.

8. This Court has personal jurisdiction over Defendant because (i) Defendant actively markets its products and conducts a substantial business in and throughout New York, where there are a considerable number of Defendant customers; (ii) Defendant is registered with the New York State Department of Financial Services which regulates insurers in the state; and (iii) the wrongful acts alleged in the Amended Complaint, including Defendant's intentional disclosure of Plaintiff's New York State Driver's License number, caused harm to Plaintiff in New York.

[1] The Travelers family of insurance companies, like other large auto insurers, consists of numerous affiliated companies that offer different types of insurance across the country.

9. Venue is proper in this District, pursuant to 28 U.S.C. § 1391(b)(2), because a substantial part of the acts, omissions, and events giving rise to Plaintiff's claims occurred in this District.

FACTS

10. Plaintiff brings this class action against Defendant for its: (i) failure to properly secure and safeguard highly valuable, protected personally identifiable information, including without limitation, Driver's License numbers ("PII"); (ii) failure to comply with industry standards to protect information systems that contain PII; (iii) unlawful disclosure of Plaintiff's and Class members' PII; and (iv) failure to provide adequate notice to Plaintiff and other Class members that their PII had been disclosed and compromised.

11. Plaintiff seeks, among other things, damages and orders requiring Defendant to fully and accurately disclose the PII and other information that has been compromised and/or disclosed, to adopt reasonably sufficient security practices and safeguards to protect Plaintiff's and the Class's PII from unauthorized disclosures, and to prevent incidents like this disclosure from occurring again in the future. Plaintiff further seeks an order requiring Defendant to provide identity theft protective services to Plaintiff and Class members for their lifetimes, as Plaintiff and Class members are at imminent risk and will continue to be at imminent risk of identity theft due to the disclosure of their PII as a result of Defendant's conduct described herein.

12. Defendant's policies and practices allowed unauthorized third parties to obtain Plaintiff's and Class members' PII through the use of Defendant's online insurance quote and/or policy process (the "Data Breach").

13. Defendant intentionally configured and designed its online system to auto-populate responses to requests for insurance quotes with certain PII obtained from third-party data

providers, including Driver's License numbers, and to disclose that PII to whomever submitted the request. If not for Traveler's intentional configuration and design of its systems, it would not have disclosed Plaintiff's and Class members' PII to non-parties.

14. The Data Breach was a direct and proximate result of Defendant's flawed online system configuration and design, which unnecessarily disclosed PII to anyone who submitted a request for an insurance quote, its failure to verify whether users were even eligible for Defendant's insurance policy, and its failure to implement and follow basic security procedures, such as validating the identity of insurance applicants before disclosing their highly sensitive PII.

15. The Data Breach was a direct and proximate result of Defendant's flawed online system configuration and design, which, rather than requesting certain PII *from* the applicant, instead provided sensitive PII *to* the applicant. This is an especially egregious design flaw where the applicant has no need to obtain the PII from the Defendant, and, as set forth below, Defendant was specifically warned against using this flawed system as a means of generating its business.

16. Because Defendant essentially left its (cyber) door wide open for unauthorized users to access and pilfer individuals' PII, Plaintiff's and Class members' PII is now in the hands of non-parties.

17. As a result, Plaintiff and, upon information and belief Class members, experienced actual identify theft, as well as substantially increased risk of future identity theft, both currently and for the indefinite future.

18. According to the New York State Attorney General, 88,858 individuals were affected and 3,912 of them are in New York State.

19. According to a written response from the Attorney General of the State of Connecticut, 1,779 residents of Connecticut were similarly affected.

20. Plaintiff's and Class members' PII, including their Driver's License numbers, that were unnecessarily disclosed by the Defendant in the Data Breach, are highly valuable because it is readily useable to commit fraud and identity theft.

21. The highly confidential PII that was compromised in the Data Breach is considered a valuable treasure trove that can be sold on the Dark Web and/or used to commit identity theft or other fraud for the foreseeable future.

22. Armed with the private information accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.*, filing for unemployment benefits and other governmental benefits, or aggregating it with other information to open new financial accounts in Class members' names, take out loans in Class members' names, file fraudulent tax returns using Class members' information, obtain driver's licenses in Class members' names but with another person's photograph, and give false information to police during an arrest.

23. As a result of the Data Breach, 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.

24. Plaintiff and Class members 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.

25. Driver's License numbers especially can be used to file fraudulent unemployment claims, to open a new account, take out a loan in someone's name, or commit income tax refund fraud as several states (including New York) require a Driver's License number for a tax return. The non-parties who obtained Plaintiff's and Class members' PII can use this information to

commit a host of other financial crimes, including identity theft, and can sell this information to other identity thieves who will do the same.

26. Consequently, Plaintiff and Class members have had to spend, and will continue to spend, significant time and money in the future to protect themselves due to Defendant's actions.

27. Plaintiff, on behalf of herself and all others similarly situated, bring claims for negligence, negligence *per se*, violation of the Driver's Privacy Protection Act ("DPPA"), violation of New York's consumer protection act, and injunctive relief claims.

28. Plaintiff seeks damages and injunctive relief requiring Defendant to adopt reasonably sufficient practices to safeguard the PII that remains in Defendant's custody in order to prevent incidents like the Data Breach from reoccurring in the future. Given that information relating to the Data Breach, including the systems that were impacted, the configuration and design of Defendant's website, and the method of accessing PII in Defendant's insurance quoting process remain exclusively in Defendant's control, Plaintiff anticipates additional support for her claims will be uncovered following a reasonable opportunity for discovery.

29. Defendant is authorized to sell and does sell property and casualty insurance in New York State.

30. Defendant has a website that solicits the business of customers in New York State.

31. Plaintiff never gave her PII to Defendant.

32. Defendant obtained Plaintiff's PII without her permission.

33. Defendant obtained Plaintiff's PII without her permission.

34. On December 10, 2021, Defendant sent Plaintiff a form letter to Plaintiff's home in Westchester County, admitting to Plaintiff that between April 2021 and November 17, 2021,

Defendant allowed an unknown person to access Plaintiff's non-public personal information through Defendant's agency portal.

35. Defendant claims that its agency portal is used by its insurance agents to obtain quotes for customers and prospective customers.

36. The form letter sent by Defendant to Plaintiff is intentionally vague as to the details of the Data Breach and besides being an admission against interest as to Defendant, its self-serving statements cannot be accepted for the truth of the matters asserted therein.

37. In its letter, Defendant claims as follows:

> **What Happened?**
>
> On November 12, 2021, Travelers discovered suspicious activity relating to our agency portal, which is used by our agents to obtain quotes for customers and prospective customers. We immediately launched an investigation and determined that between April 2021 and November 17, 2021, an unauthorized party used the credentials of a limited number of agents to access the portal to obtain information sourced from a third party. Please note that Travelers' network was not Impacted by this event.
>
> **What information Was Involved?**
>
> The personal information may have included your name, address, date of birth, and driver's license number

38. Defendant represented to Plaintiff that there were other impacted individuals to whom the same events happened.

39. Since the announcement of the Data Breach, Plaintiff has been required to spend her valuable time and resources in an effort to detect and prevent any additional misuses of her PII. Plaintiff would not have to undergo such time-consuming efforts but for the Data Breach.

40. As a result of the Data Breach, Plaintiff has been and will continue to be at heightened risk for fraud and identity theft, and its attendant damages for years to come. Such risk is real and impending, and is not speculative, given the highly sensitive nature of the PII

compromised by the Data Breach, and, upon information and belief, this information has already been illegally used by non-parties after the Data Breach.

A. The Travelers Insurance Application Process

41. Defendant and its related entities offer insurance, banking, investment, retirement, and mortgage services. Defendant proclaims:

> Your privacy is important to us. When we quote or sell an insurance policy to a person, we get information about the people and property that we're insuring. This Privacy Notice describes the types of information about you ("personal information") we collect, where we get it, and how we use, share and protect it.

42. Defendant's products and services are only available to customers who agree to pay for the services provided by Defendant.

43. To enjoy these services, an individual must first become a paying customer of Defendant.

44. Under Defendant's current framework on its website, which it configured and designed, individuals seeking an insurance quote from Defendant are only required to provide minimal information. The remainder of the information needed to process the request is typically obtained from the relevant state's department of motor vehicles ("DMV") or other third parties, such as insurers or data aggregators, who receive this information from state DMVs.

45. This is by design. Defendant, like other insurers, intentionally allows individuals requesting a quote to provide only limited information. This is a benefit to Defendant as it allows Defendant to employ less workers and handle less phone calls from consumers.

46. In addition, this makes the process faster and less burdensome on the consumer, increasing the likelihood that they submit the application and thus increasing the number of requests for quotes that Defendant receives. However, this 'shortcut' process and intentional

design feature on Defendant's systems also makes it extremely ripe for exploitation and misuse by non-parties, such as what occurred to Plaintiff and Class members.

47. Upon information and belief, if a user receives an auto insurance quote from Defendant, Defendant discloses the user's Driver's License number on the quote.

48. However, this process of applying for an insurance quote is easily exploitable by non-parties to obtain the PII of other individuals, such as Plaintiff and Class members, who are not voluntary customers of Defendant.

49. For example, anyone who possess only minimal and basic information of Plaintiff and Class members—such as a name, an address, and a date of birth, some of which may have been stolen or found elsewhere—can submit fraudulent requests for insurance quotes to extract more detailed and sensitive PII from Defendant's system, such as Driver's License numbers, which Defendant provides in response to the on-line request on the final insurance quote. By repeating this extraction process for multiple individuals, non-parties can develop a cache of highly sensitive personal information, including Driver's License numbers, that they can then use to commit fraud or identity theft or sell such PII on the dark web to other bad actors.

50. Tim Sadler, CEO of email security firm Tessian, points out why driver's license numbers are very sought after by non-parties: "[…] It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification or use the information to craft curated social engineering phishing attacks."[2]

[2] https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/ (Last visited on March 3, 2022).

51. The hackers may be using these driver's license numbers to fraudulently apply for unemployment benefits in someone else's name. According to Sadler, this is a very lucrative scam for hackers and these license numbers are in "high demand."[3]

52. On information and belief, the PII data residing in Defendant's database(s) was not encrypted.

53. On information and belief, the cyberattack was reported to law enforcement.

54. Plaintiff and Class members are entitled to security of their PII. As a business for profit collecting and storing sensitive information, and as an entity with access to sensitive data such as Driver's License numbers, Defendant has a duty to ensure that such private, sensitive information is not disclosed or disseminated to unauthorized third parties.

55. Upon informing Plaintiff and the Class that their PII was accessed without authorization, Defendant offered those impacted individuals a complimentary one-year subscription to the Cyberscout identity theft protection service.

56. The offer of credit and identity monitoring services is an admission by Defendant that the impacted customers are subject to an imminent threat of identity theft and financial fraud.

57. To date, Defendant has merely offered complimentary identity theft and credit monitoring services for a period of one year. This offer, however, 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 it entirely fails to provide any compensation for the unauthorized release and disclosure of Plaintiff's and Class members' PII.

58. Furthermore, Defendant's identity theft and credit monitoring offer to Plaintiff and Class members squarely places the burden on Plaintiff and Class members, rather than on the

[3] *Id.*

Defendant, to investigate and protect themselves from Defendant's tortious acts resulting in the Data Breach. Rather than automatically enrolling Plaintiff and Class members in identity theft and credit monitoring services upon discovery of the breach, Defendant merely sent instructions offering the services to affected consumers with the recommendation that they sign up for the services.

59. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identify thieves use identifying data such as Social Security Numbers to open financial accounts, receive government benefits and incur charges and credit in a person's name.[4] As the GAO Report states, this type of identity theft is the most harmful because it often takes some time for the victim to become aware of the theft, and the theft can impact the victim's credit rating adversely.[5]

60. Accordingly, identify theft victims must spend countless hours and large amounts of money repairing the impact to their credit.

61. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the dark web for years. According to the GAO Report:

> [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.

---

[4] U.S. Gov. Accountability Office, GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Theft is Limited; However, the Full Extent is Unknown* (2007); https://www.gao.gov/assets/gao-07-737.pdf (Last visited on March 3, 2022).

[5] *Id.*

62. A 2014 study by the U.S. Department of Justice found that the average cost to a victim of identity theft is $1,343.[6]

63. According to a 2019 report, identity fraud caused nearly $17 billion in damage to victims and that the most common types of identity fraud are opening new credit card and bank accounts, business and personal loans, auto loans, and student loans.[7]

64. Indeed, data breaches and identity theft and financial fraud have a crippling effect on individuals and detrimentally impact the economy.

65. For all the above reasons, Plaintiff and Class members have suffered harm; and there is a substantial risk of injury to Plaintiff and Class members that is imminent and concrete and that will continue for years to come.

66. Plaintiff still does not have a full understanding of the extent of the intrusion into Defendant's computer system, nor a full understanding of what data was taken and where it is now. Defendant has undoubtedly performed a forensic examination of the intrusion. That report will be discoverable. That report will likely show the continuing threat that Defendant's lack of a secure data system poses to Plaintiff and the Class and the harm suffered as a result.

B. Defendant Was On Notice That A Data Breach Was Likely

67. On February 16, 2021, the New York State Department of Financial Services ("NYSDFS") issued a cyber security fraud alert (the "February 2021 Cyber Fraud Alert") to the

---

[6] *See* Cody Gredler, *The Real Cost of Identity Theft*, CSID (Sept. 9, 2016); https://staging.experianpartnersolutions.com/2016/09/real-cost-identity-theft/ (Last visited on March 3, 2022).

[7] *See* Gayle Sato, *The Unexpected Costs of Identity Theft*, Experian (Sept. 30, 2020); https://www.experian.com/blogs/ask-experian/what-are-unexpected-costs-of-identity-theft/ (Last visited on March 3, 2022).

Chief Executive Officers, Chief Information Officers, Chief Information Security Officers, Senior Information Officers, and Data Privacy Officers of all regulated entities, including Defendant.

68. A copy of the NYSDFS February 2021 Cyber Fraud Alert can be found at: https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210216_cyber_fraud_alert#_ednref1.

69. The February 2021 Cyber Fraud Alert informed those entities that cyber criminals were exploiting cybersecurity flaws on websites to steal nonpublic information ("NPI"), specifically referencing 23 NYCRR § 500.01(g).

70. 23 NYCRR § 500.01(g)(2)(ii) defines NPI as "all electronic information that is not publicly available information and is: any information concerning an individual which because of name, number, personal mark, or other identifier can be used to identify such individual, in combination with any one or more of the following data elements: drivers' license number or non-driver identification card number."

71. Specifically, the February 2021 Cyber Fraud Alert warned:

(a) that cyber criminals were targeting "***websites that offer instant online automobile insurance premium quotes . . . to steal unredacted driver's license numbers***;"

(b) "the activity appears to be part of an overall increase to steal NPI, driven in part by increase fraud activity during the pandemic;"

(c) "this stolen information has been used to submit fraudulent claims for pandemic and unemployment benefits;" and

(d) there were communications on "***cybercrime forums offering to sell techniques to access driver's license numbers from auto insurance websites and step-by-step instruction on how to steal them***."

72. In light of this criminal activity, NYSDFS warned that all websites who offer instant online automobile insurance premium quotes "are vulnerable to this type of data theft."

73. To prevent this type of data theft, the NYSDFS recommended that all regulated entities should "review whether it is necessary to display any NPI – even redacted to users, especially on public-facing websites. NPI should not be displayed on public-facing websites unless there is a compelling reason to do so."

74. NYSDFS further recommended that "[e]ntities that maintain any public-facing website that displays or transmits NPI should also take the following steps:"

- Conduct a thorough review of public-facing website security controls, including but not limited to a review of its Secure Sockets Layer (SSL), Transport Layer Security (TLS), and HTTP Strict Transport Security (HSTS) and Hypertext Markup Language (HTML) configurations;

- Review public-facing websites for browser web developer tool functionality. Verify and, if possible, limit the access that users may have to adjust, deface, or manipulate website content using web developer tools on the public-facing websites;

- Review and confirm that its redaction and data obfuscation solution for NPI is implemented properly throughout the entire transmission of the NPI until it reaches the public-facing website;

- Ensure that privacy protections are up to date and effectively protect NPI by reviewing who is authorized to see NPI, which applications use NPI, and where NPI resides;

- Search and scrub public code repositories for proprietary code; and

- Block the IP addresses of the suspected unauthorized users and consider a quote limit per user session.

75. On March 30, 2021, NYSDFS followed up with a second alert (the "March 2021 Cyber Fraud Alert Follow-Up") to the Chief Executive Officers, Chief Information Officers, Chief Information Security Officers, Senior Information Officers, and Data Privacy Officers of all regulated entities, including Defendant, concerning the exploitation of data pre-fill systems.

76. A copy of the NYSDFS March 2021 Cyber Fraud Alert Follow-Up can be found at: https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210330_cyber_alert_followup.

77. In its March 2021 Cyber Fraud Alert Follow-Up, NYSDFS "**urge[d] personal lines insurers and other financial services companies to avoid displaying prefilled NPI on public-facing websites considering the serious risk of theft and consumer harm."** (Emphasis in the original).

78. The NYSDFS March 2021 Cyber Fraud Alert Follow-Up recommended that "[t]o combat this cybercrime, the following basic security steps should be implemented. Companies that continue to use Instant Quote Websites should also be prepared for cybercriminals to continue using new methods of attack," including:

- **Disable prefill of redacted NPI.** Avoid displaying prefilled NPI, especially on public-facing websites. *See* 23 NYCRR 500.09.

- **Install Web Application Firewall (WAF).** WAFs help protect websites from malicious attacks and exploitation of vulnerabilities by inspecting incoming traffic for suspicious activity. *See* 23 NYCRR 500.02(b)(2).

- **Implement CAPTCHA.** Cybercriminals use automated programs or "bots" to steal data. Completely Automated Public Turing Tests ("CAPTCHA") attempt to detect and block bots. *See* 23 NYCRR 500.02(b)(2).

- **Improve Access Controls for Agent Portals.** Agent portals typically allow agents access to consumer NPI, and robust access controls are required by DFS's cybersecurity regulation. Measures that should be implemented include:

    - MFA, *see* 23 NYCRR 500.12;
    - Robust password policy, *see* 23 NYCRR 500.03 and 500.07; and

- Limitations on login attempts, *see* 23 NYCRR 500.03 and 500.07.

- **Training and awareness.** Employees and agents should be trained to identify social engineering attacks. Employees and agents should know not to disclose NPI, including DLNs, over the phone. Robotic scripts with grammatical errors or repeated statements used during dialogue are key identifiers of fraudulent calls. *See* 23 NYCRR 500.14.

- **Limit access to NPI.** Employees and agents should only have access to sensitive information that is necessary to do their job. *See* 23 NYCRR 500.03(d) and 500.07.

- **Wait until payments have cleared before issuing a policy.** Auto insurers should consider waiting until an eCheck, credit card, or debit card payment has been cleared by the issuing bank before generating an online policy and granting the policyholder access to NPI. *See* 23 NYCRR 500.02, 500.03, 500.07, and 500.09.

- **Protect NPI received from data vendors.** Ensure that APIs used to pull data files, including JSON and XML, from data vendors are not directly accessible from the internet or agent portals. *See* 23 NYCRR 500.02(b)(2) and 500.08.

79. Defendant is an entity regulated by NYSDFS and received and/or had knowledge of the February 2021 Cyber Fraud Alert and the March 2021 Cyber Fraud Alert Follow-Up.

80. Defendant did not follow NYSDFS's recommendations to secure Plaintiff's and Class members' PII.

81. Defendant suffered the type of data breach that NYSDFS predicted and warned it about.

82. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches preceding the date of the breach.

83. In light of recent high profile data breaches at other large companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), Advanced Info Service (8.3 billion records, May

2020), Defendant knew or should have known that its electronic records would be targeted by cyber criminals.

C. Defendant's Data Breach

84. On December 10, 2021, Defendant notified Plaintiff and claimed that:

> **What Happened?**
>
> On November 12, 2021, Travelers discovered suspicious activity relating to our agency portal, which is used by our agents to obtain quotes for customers and prospective customers. We immediately launched an investigation and determined that between April 2021 and November 17, 2021, an unauthorized party used the credentials of a limited number of agents to access the portal to obtain information sourced from a third party. Please note that Travelers' network was not Impacted by this event.
>
> **What information Was Involved?**
>
> The personal information may have included your name, address, date of birth, and driver's license number.

85. As these cyber criminals have already used the PII compromised in the Data Breach to commit financial fraud and identity theft, Plaintiff and Class members have been and remain at an imminent risk of future fraud and identity theft.

D. Defendant Obtains, Collects And Stores Plaintiff's And Class Members' PII

86. In the ordinary course of doing business as an automobile insurer, Defendant regularly requires its customers and prospective customers to provide their sensitive, personal and private protected information in order to register and use Defendant's services.

87. Additionally, automobile insurers, such as Defendant, also store and obtain additional personal information that they receive from other sources. For instance, automobile insurers share claims information among themselves to help weed out consumers who switch to other providers. These insurers also have access to a consumer's Driver's License number, current auto policy data, and make and model of a consumer's vehicle. Often, this information needed to

process the request is typically obtained from the relevant state DMVs or other third parties, such as insurers or data aggregators, who receive this information from state DMVs.

88. As an automobile insurer, Defendant purposefully aims to make applying for a policy as easy as possible in order to attract new customers and increase its business. To do so, Defendant only requires a minimal amount of information to apply for a policy. The remainder of the information is filled in from data acquired from other sources.

89. Cyber criminals employ a variety of techniques for obtaining this PII, including extracting data from the website's code, using web developer tools meant for debugging, and calling live agents with enough other information to persuade them to hand over other forms of personal information, such as Driver's License numbers. Indeed, the practice is so prominent there are 'how-to guides' that aspiring criminals can buy that have appeared on cybercrime forums.

90. But Defendant did not have to configure or design its systems in this way. For example, instead of auto populating insurance quote fields with highly sensitive PII, Defendant could have validated the user's information and processed the quote on the 'back-end' after receiving the applicant's information. Nor was there a need for Defendant to disclose highly sensitive PII, like a purported applicant's Driver's License number in response to a request for a quote.

91. If the request for an insurance quote was a legitimate request, the requesting party would already possess their Driver's License Number and would not need to get it from Defendant.

92. Defendant is in complete operation, control, and supervision of its website and systems, including the insurance quote portal it provides to its agents. Defendant intentionally configured and designed its website and systems this way because it helped to increase the number

of quotes requested, benefiting its business, without regard to Plaintiff's and Class members' PII which was disclosed to non-parties in the process given this exploitability.

93. By obtaining, using, disclosing, and deriving a benefit from Plaintiff's and Class members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class members' PII from disclosure.

94. Thus, Defendant had access to Plaintiff's and Class members' PII, including their Driver's License Numbers, which was stored on Defendant's computer systems, which it then intentionally disclosed when generating a quote.

95. Plaintiff and Class members reasonably expect that insurance service providers such as Defendant will use the utmost care to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

96. Defendant acknowledges that it has an obligation to protect PII from disclosure. Defendant states on its website that:

> The Travelers Indemnity Company and its affiliates ("Travelers") value your privacy. This Online Privacy Statement will inform you about how we use and disclose information that we and our service providers collect from your visits to travelers.com and other websites owned or operated by us (the "Websites"), through the software applications made available by us for use on or through computers and mobile devices (the "Apps"), through use of social media pages that we control ("Social Media Pages"), and through email messages that we send to you (collectively, including the Websites, the Apps, and our Social Media Pages, the "Services").
>
> This Online Privacy Statement only applies to information collected through the Services. If you have purchased or applied for an insurance product from us, please also see our Privacy Statement for Individual U.S. Personal Insurance Consumers, which applies to the information that we collect about policyholders and applicants, through the Services as well as any other medium. Travelers does business in a number of different jurisdictions. Additional Privacy Statements may apply depending on your jurisdiction or customer relationship.

Privacy Statement for Individual U.S. Personal Insurance Consumers

Your privacy is important to us. When we quote or sell an insurance policy to a person, we get information about the people and property that we're insuring. This Privacy Notice describes the types of information about you ("personal information") we collect, where we get it, and how we use, share and protect it. It applies to current and former Travelers personal insurance customers in the United States.

A few key points include:

- We collect personal information from you, your agent, and from third parties
- We will not share your personal information with others for their marketing purposes without your permission
- We maintain safeguards designed to help prevent unauthorized use, access and disclosure of personal information.

97. Defendant also claims it does the following:

What type of information do we collect?

You give us most of what we need in the application process. To make sure what we have is correct, or to obtain additional information, we may need to check back with you. For example, you may be asked to give us more details in writing, via e-mail or over the phone. In addition, we may obtain other information, including but not limited to the following:

- Information from consumer reporting agencies and other insurance support organizations to the extent permitted by law. This may include items such as credit history, credit-based insurance score, driving record, accident and motor vehicle conviction history, and claim history. Information given to us by an insurance support organization, including consumer reporting agencies, may be retained by them and disclosed to others.
- Your past insurance history, including information about your policies and claims, from insurance support organizations or your former insurers.
- Information regarding your property. We may obtain this through third party reports and through a property inspection. We or an independent inspector may visit the property to inspect its condition, or we may use an unmanned aircraft system. We may obtain geospatial information, and take pictures or video. If we

need more details about the property, we may need to schedule an interior inspection.

- Information from government agencies or independent reporting companies.

- Other third party data relating to the insured risk, such as possible drivers and vehicles associated with your household and odometer readings associated with any vehicle(s).

- In some instances, we may need to know about your health. For example, if we need to know whether a physical limitation will affect your ability to drive, we may ask for a statement from your doctor.

How do we use your personal information

We use the personal information we collect to sell, underwrite and rate, service and administer insurance; to handle claims; to create and market products and services; to prevent and detect fraud; to satisfy legal or regulatory requirements; and for other business purposes and as otherwise allowed by law.

Once you're insured with us, we will retain details about your policy(ies). This may include, among other things, bill payment, transaction or claim history and details, as well as other information.

When you give us a telephone number, you consent to being contacted at that number, including if the number is for a cell phone or other wireless device. We may contact you in person, by recorded message, by the use of automated dialing equipment, by text (SMS) message, or by any other means your device is capable of receiving, to the extent permitted by law and for reasonable business purposes, including to service your policy or alert you to other relevant information.

How do we share your personal information?

We do not give or sell your personal information to nonaffiliated third parties for their own marketing purposes without your prior consent.

We may give the personal information we collect to others to help us conduct, manage or service our business. When we do, we require them to use it only for the reasons we gave it to them. We may give, without your past permission and to the extent permitted by law, personal information about you to certain persons or organizations such as: your agent or insurance representative; our affiliated property and casualty insurance companies; independent claim adjusters or investigators; persons or organizations that conduct research; insurance support

organizations (including consumer reporting agencies); third party service providers; another insurer; law enforcement; state insurance departments or other governmental or regulatory agencies; or as otherwise required or permitted by law. Information we share with insurance support organizations, such as your claims history, may be retained by them and disclosed to others

We may also share your personal information: to comply with legal process; to address suspected fraud or other illegal activities; or to protect our rights, privacy, safety or property, and/or that of you or others.

How do we protect your personal information?

We maintain physical, electronic and administrative safeguards designed to help protect personal information. For example, we limit access to personal information and require those who have access to use it only for legitimate business purposes.

Security

When you do business with Travelers online, you can be sure that we've made it our priority to help keep your personal information safe and confidential. Your privacy is important to us. We're careful about how your information is gathered, used and shared as outlined in our "Online Privacy Statement".

98. Defendant also makes the following claims:

Travelers Cybersecurity Practices

Travelers takes data security seriously and has a multi-faceted approach to strengthen the security of customer information. We use administrative, technical and physical safeguards to protect information in our care. We have established a wide range of comprehensive data security protections and maintain an overall data risk management strategy that includes monitoring emerging security threats and assessing appropriate responsive measures and steps to react accordingly.

Organizational Structure

The Travelers Cybersecurity department is led by the Chief Information Security Officer (CISO), who has responsibility for cybersecurity, risk and business continuity programs. The CISO reports to the Chief Information Officer and is a member of the enterprise risk team. The CISO provides quarterly updates on the cybersecurity, risk and business continuity programs to the Board of Directors and executive management. Our security team is comprised of over 100 trained individuals, many of whom hold advanced industry certifications.

Policy and Governance

At Travelers, data protection is embedded throughout our business operations and information technology program. Our goal is to provide a disciplined approach to safeguarding our customer data and company information assets. As a foundation to this approach, Travelers maintains a comprehensive set of cybersecurity policies and standards which have been developed in collaboration with a wide range of disciplines, such as information technology, cybersecurity, legal, compliance and business. Annually, Travelers undergoes an SSAE 18 SOC 2 examination by an independent external audit firm. In addition, we continuously self-assess against our internal policies, which are in alignment with and based upon ISO 27001, using our internal risk assessment process and a wide variety of frameworks and regulations available, such as the NIST Cybersecurity Framework, New York Department of Financial Services Cybersecurity Requirements for Financial Services Companies, and the Payment Card Industry Data Security Standard. Our comprehensive and collaborative approach allows us to further the organizational culture of data security awareness, the effectiveness of data governance and the responsiveness to evolving data management protocols.

99. Defendant further claims:

Technology

Travelers utilizes sophisticated tools designed to protect information through the use of technology including: multifactor authentication, firewalls, intrusion detection and prevention systems, vulnerability and penetration testing, and identity management systems. We implement encryption using a risk-based approach. Our identity and access management systems employ both commercial authentication products from leading companies as well as internally developed systems based on prevailing industry standards. We include periodic recertification access for key data, and we utilize multifactor authentication based on the level of risk. We monitor events to understand exceptions to normal processing and then act on those anomalies. We participate in vulnerability information sharing networks and track industry and government intelligence sources for impact in the marketplace and deploy necessary updates as appropriate. Travelers has a robust software patch management process that includes risk assessment and risk-based update schedules. These systems are designed, implemented and maintained to provide a high level of security to safeguard sensitive data.

Training

Travelers provides its employees with data security awareness, education and training. Travelers has a team of cybersecurity personnel engaged in data risk

management education and ongoing training to employees with access to Travelers information assets. Our annual security awareness training covers a broad range of security topics from password protection and social engineering to privacy and compliance. We provide ongoing training via computer-based training, targeted training, security materials and presentations, company intranet articles, email publications and various simulation exercises.

Third Party Relationships

Travelers utilizes a comprehensive cybersecurity diligence and oversight process for its third-party vendors. This process is a component of Travelers' supplier management program. Prior to the commencement of services, Cybersecurity performs a risk/rating assessment of all vendors that will have access to and process Travelers data and conducts formal, comprehensive risk assessments on certain service providers based on the risk/rating assessment. Re-assessment occurs on an ongoing basis, the frequency of which is determined based on a risk assessment and rating process. The assessment process utilizes a comprehensive questionnaire which addresses aspects of the vendors' data security controls and policies, including business continuity, as well as onsite assessments for higher risk relationships.

100. In addition, Defendant claims to have procedures in place to respond to cyber intrusions:

Incident Response

Travelers has implemented a Security Incident Response Framework. The framework is a set of coordinated procedures and tasks that will be executed by the Travelers incident response team to ensure timely and accurate resolution of computer security incidents. Travelers uses risk analysis to select components of the plan to test. We conduct tabletop exercises, testing components of the plan several times annually.

Compliance

Travelers expects all employees to act in accordance with the highest standards of personal and professional integrity in all aspects of their employment and to comply with all applicable laws and Travelers policies.

Our cybersecurity framework includes regular compliance assessments with Travelers policies and standards and applicable state and federal statutes and regulations. Compliance with our internal data security controls is validated through the use of security monitoring utilities and through rigorous internal and external audits. In addition, we proactively perform self-assessments against regulatory frameworks such as the NIST Cybersecurity Framework.

101. Despite Defendant's lofty statements regarding cybersecurity, Defendant's configuration and design of its own systems that resulted in the Data Breach proved otherwise.

102. Plaintiff still does not have a full understanding of the extent of the intrusion into Defendant's computer system, nor a full understanding of what data was taken and where it is now. Defendant has undoubtedly performed a forensic examination of the intrusion. That report will be discoverable. That report will likely show the continuing threat that Defendant's lack of a secure data system poses to Plaintiff and the Class and the harm suffered as a result. In its letter to Plaintiff, Defendant claims "the security of personal information is a top priority of ours, and we continually take steps to further enhance our systems."

103. Though Plaintiff did not apply for insurance with Defendant on her own, she was nonetheless an involuntary "member" of Defendant's system once non-parties used her information to fraudulently create an account. Defendant, by its own admission, therefore, owed Plaintiff the same duty to protect her PII as other customers.

104. Despite Defendant's commitment to protecting personal information, Defendant failed to prioritize data and cyber security by adopting reasonable data and cyber security measures to prevent and detect the unauthorized access to Plaintiff's and Class members' PII.

105. Had Defendant remedied its security deficiencies, heeded advice from government regulators, followed industry guidelines, and adopted security measures recommended by experts in the field, Defendant would have prevented intrusion into its information systems and, ultimately, the theft of Plaintiff's and Class members' confidential PII.

E. The Value Of Private Information And Effects Of Unauthorized Disclosure

106. Defendant was well aware that the protected PII it acquires, stores, and utilizes is highly sensitive and of significant value to the owners of the PII and those who would use it for wrongful purposes.

107. PII is a valuable commodity to identity thieves, particularly when it is aggregated in large numbers. Former Attorney General William P. Barr made clear that consumers' sensitive personal information commonly stolen in data breaches "has economic value." The purpose of stealing large caches of personal data is to use it to defraud individuals or to place it for illegal sale and to profit from other criminals who buy the data and use it to commit fraud and identity theft. Indeed, cyber criminals routinely post stolen personal information on anonymous websites, making the information widely available to a criminal underworld.

108. There is an active and robust market for this information. As John Sancenito, president of *Information Network Associates*, a company which helps companies with recovery after data breaches, explained after a data breach "[m]ost of the time what [data breach hackers] do is they steal the data and then they sell the data on the dark web to the people who actually commit the fraud." PII is valued on the dark web at approximately $1 per line of information.

109. Driver's License numbers in particular—which were compromised as a result of the Data Breach—are highly sought after by cyber criminals on the dark web because they are unique to a specific individual and extremely sensitive.

110. *Experian*, a globally recognized credit reporting agency, has explained "[n]ext to your Social Security number, your driver's license number is one of the most important pieces of information to keep safe from thieves." This is because a Driver's License number is connected to an individual's vehicle registration, insurance policies, records on file with the DMV, NY

Department of Taxation and Finance and other government agencies, places of employment, doctor's offices, and other entities.

111. For these reasons, Driver's License numbers are highly sought out by cyber criminals because they are one of the most valuable pieces of information to facilitate identity theft and fraud. This information is valuable because cyber criminals can use this information to open credit card accounts, obtain insurance policies and submit fraudulent claims, open cell phone contracts, file fraudulent tax returns, file unemployment applications, as well as obtain bank loans under a person's name.

112. Further, unlike credit or debit card numbers in a payment card data breach, which can quickly be frozen and reissued in the aftermath of a breach, the type of PII at stake here—unique Driver's License numbers—cannot be easily replaced.

113. The ramifications of Defendant's failure to keep Plaintiff's and Class members' PII secure are long lasting and severe. To avoid detection, identity thieves often hold stolen data for months or years before using it. Also, the sale of stolen information on the "dark web" may take months or more to reach end-users, in part because the data is often sold in small batches as opposed to in bulk to a single buyer. Thus, Plaintiff and Class members must vigilantly monitor their financial accounts *ad infinitum*.

114. Thus, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to it and of the foreseeable consequences if its systems were breached. Defendant failed, however, to take adequate cyber security measures to prevent the Data Breach from occurring.

F. FTC Guidelines, NY Shield Act And The DPPA

115. Defendant is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

116. The FTC has promulgated numerous guides for businesses that 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.

117. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.

118. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private 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.

119. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

120. Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII, or to prevent the disclosure of such information to unauthorized individuals, as reflected by the sensitive Driver's License information provided in its response to requests for insurance quotes, constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

121. Defendant was at all times fully aware of its obligations to protect the PII of consumers because of its business of obtaining, collecting, and disclosing PII as well as collecting, storing, and using other confidential personal and financial information. Defendant was also aware of the significant repercussions that would result from its failure to do so.

122. Defendant also had an obligation to use reasonable security measures under New York's Shield Act (N.Y. Gen. Bus. Law § 899-aa, *et seq.* (known as the "NY Shield Act"), which requires businesses that collect private information to implement reasonable cybersecurity safeguards to protect that information.

123. The NY Shield Act also mandates the implementation of a data security program, including measures such as risk assessments, workforce training and incident response planning and testing, and became effective on or about March 21, 2020.

124. Defendant also had an obligation under the DPPA. The DPPA was enacted in 1994 in response to safety and privacy concerns stemming from the ready availability of personal information contained in state motor vehicle records. The DPPA was passed in the backdrop of the murder of actress Rebecca Schaeffer, whose murderer obtained her unlisted address through the California Department of Motor Vehicle (DMV). Additional concerns were raised when witnesses testified in hearings before Congress regarding the privacy of DMV information of domestic violence victims and law enforcement officers, among other safety concerns surrounding

driver information. To address these concerns, the DPPA restricts the disclosure of personal information from motor vehicle records to certain permissible purposes expressly defined by the act.

125. The unauthorized disclosures of information have long been seen as injurious. The common law alone will sometimes protect a person's right to prevent the dissemination of private information. Indeed, it has been said that privacy torts have become well-ensconced in the fabric of American law. And with privacy torts, improper dissemination of information can itself constitute a cognizable injury. Because damages for a violation of an individual's privacy are a quintessential example of damages that are uncertain and possibly unmeasurable, causes of action such as the DPPA provide privacy tort victims with a monetary award calculated without the need of proving actual damages.

126. The DPPA states that "[a] [s]tate department of motor vehicles, and any officer, employee, or contractor thereof, shall not knowingly disclose or otherwise make available to any person or entity: personal information, as defined in 18 U.S.C. 2725(3), about any individual obtained by the department in connection with a motor vehicle record, except as provided in subsection (b) of this section." 18 U.S.C. § 2721(a)(1).

127. Defendant had an obligation to use reasonable security measures under the DPPA, which further states that "[i]t shall be unlawful for any person knowingly to obtain or disclose personal information, from a motor vehicle record, for any use not permitted under section 2721(b) of this title." 18 U.S.C. § 2722(a).

128. Thus, the DPPA provides citizens with a private right of action in the event that their private information is knowingly obtained, disclosed, or used in a manner other than for the enumerated permissible purposes. The DPPA states: "[a] person who knowingly obtains, discloses

or uses personal information, from a motor vehicle record, for a purpose not permitted under this chapter [18 U.S.C. §§ 2721, *et seq*.] shall be liable to the individual to whom the information pertains, who may bring a civil action in a United States district court." 18 U.S.C. § 2724(a).

129. The default rule under the DPPA is non-disclosure. The DPPA is structured such that 18 U.S.C. § 2721(a)(1) and 18 U.S.C. § 2722(a) provide the general prohibition on the release and use of motor vehicle information, and § 2721(b) enumerates fourteen specific exceptions to the general prohibition. Disclosing information to cyber criminals is not one of them. Because the PII was disclosed to unauthorized individuals—*i.e.*, cyber criminals—there is no argument to be made that disclosure was "for a permissible purpose."

G. Plaintiff And Class Members Suffered Damages

130. This Data Breach was foreseeable, in light of the much-publicized wave of data breaches in recent years. Since at least 2015, the Federal Bureau of Investigation ("FBI") has specifically advised private industry about the threat of "Business E-Mail Compromise" ("BEC"). The FBI calls BEC "a growing financial fraud that is more sophisticated than any similar scam the FBI has seen before and one—in its various forms—that has resulted in actual and attempted losses of more than a billion dollars to businesses worldwide." The FBI notes that "scammers' methods are extremely sophisticated," and warns companies that "the criminals often employ malware to infiltrate company networks."[8]

131. Accordingly, Defendant knew, given the vast amount of PII it collects, manages, and maintains, that it was a target of security threats, and therefore understood the risks posed by

[8] BUSINESS E-MAIL COMPROMISE: AN EMERGING GLOBAL THREAT, https://www.fbi.gov/news/stories/business-e-mail-compromise (last visited March 3, 2022).

unsecure data security practices and systems. Defendant's failure to heed warnings and to otherwise maintain adequate security practices resulted in this Data Breach.

132. Defendant, at all relevant times, had a duty to Plaintiff and Class members to properly secure their PII, encrypt and maintain such information using industry standard methods, train their employees, utilize available technology to defend their systems from invasion, act reasonably to prevent foreseeable harm to Plaintiff and Class members, and promptly notify Plaintiff and Class members when Defendant became aware of the potential that consumer PII may have been compromised.

133. Defendant had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite their obligation to protect such information. Accordingly, Defendant breached their common law, statutory, and other duties owed to Plaintiff and Class members.

134. Defendant's duty to use reasonable security measures also arose 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 by entities such as Defendant.

135. Defendant's duty to use reasonable security measures also arose under New York's SHIELD Act (General Business Law § 899-bb), requiring businesses that collect private information on New York residents to implement reasonable cybersecurity safeguards to protect that information. It mandates the implementation of a data security program, including measures such as risk assessments, workforce training and incident response planning and testing, and became effective on or about March 21, 2020. It covers all employers, individuals or

organizations, regardless of location, that collect private information on New York residents. Its definition of PII includes driver's license numbers.

136. The Federal Trade Commission has established data security principles and practices for businesses as set forth in its publication, Protecting Personal Information: A Guide for Business.[9] Among other things, the FTC states that companies should encrypt information stored on computer networks and dispose of consumer information that is no longer needed. The FTC also says to implement policies for installing vendor-approved patches to correct problems, and to identify operating systems. The FTC also recommends that companies understand their network's vulnerabilities and develop and implement policies to rectify security deficiencies. Further, the FTC recommends that companies utilize an intrusion detection system to expose a data breach as soon as it occurs; monitor all incoming traffic for activity that might indicate unauthorized access into the system; monitor large amounts of data transmitted from the system and have a response plan ready in the event of a data breach. 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, alien registration number, government passport number, employer or taxpayer identification number." (17 C.F.R. § 248.201 (2013)).

137. The FTC has prosecuted a number of enforcement actions against companies for failing to take measures to adequately and reasonably protect consumer data. The FTC has viewed

[9] https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (last visited March 3, 2022).

and treated such security lapses as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45.

138. Defendant failed to maintain reasonable data security procedures and practices.

139. Accordingly, Defendant did not comply with state and federal law requirements and industry standards, as discussed above.

140. Defendant was at all times fully aware of its obligations to protect the PII of consumers. Defendant was also aware of the significant consequences that would result from its failure to do so.

141. As a result of the data breach and Defendant's failure to provide timely notice to Plaintiff and Class members, Plaintiff's and Class members' PII are now in the hands of unknown hackers, and Plaintiff and Class members now face an imminent, heightened, and substantial risk of identity theft and other fraud, which is a concrete and particularized injury traceable to Defendant's conduct. Accordingly, Plaintiff and the Class members have suffered "injury-in-fact." *See Attias v. CareFirst, Inc.*, 865 F.3d 620 (D.C. Cir. 2017).

142. As a direct and proximate result of Defendant's wrongful actions and inaction, Plaintiff and Class members have suffered injury and damages, including the increased risk of identity theft and identity fraud, improper disclosure of PII, the time and expense necessary to mitigate, remediate, and sort out the increased risk of identity theft and to deal with governmental agencies, including the New York State Department of Labor and all those administering unemployment benefits, as a result of fraudulent claims ostensibly made on their behalf.

143. The ramifications of Defendant's failure to keep PII secure are long lasting and severe. Consumer victims of data breaches are more likely to become victims of identity fraud,

occurring 65 percent of the time. In 2019 alone, consumers lost more than $1.9 billion to identity theft and fraud.

144. Plaintiff and Class members have faced an actual as well as substantial and imminent risk of identity theft and fraud as a result of the Data Breach. Unauthorized individuals carried out the Data Breach and stole the personal information of Plaintiff and Class members with the intent to use it for fraudulent purposes and/or sell it to other cyber criminals.

145. The risk of identity theft is particularly substantial when the PII compromised, in this instance Driver's License numbers, is unique to a specific individual and extremely sensitive.

146. Plaintiff and Class members have already spent and will spend substantial amounts of time monitoring their accounts for identity theft and fraud and reviewing their financial affairs more closely than they otherwise would have done but for the Data Breach. These efforts are burdensome and time-consuming.

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

148. Further, many Class members will incur out of pocket costs for protective measures, such as identity theft protection, credit monitoring, credit report fees, credit freeze fees, and similar costs related to the Data Breach.

149. Besides the monetary damage sustained in the event of identity theft, consumers may also spend anywhere from approximately 7 hours to upwards to over 1,000 hours trying to resolve identity theft issues. The Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems."

150. Despite all of the publicly available knowledge of the continued compromises of PII and the importance of securing such information, Defendant's commitment to privacy fell by the wayside. Rather than protect Plaintiff's and Class members' PII, Defendant ignored these risks and knowingly configured and designed its systems in a way that disclosed this information to cyber criminals.

151. As an auto insurance company that handles personal information containing Driver's License numbers as part of its business model, Defendant was well aware of the requirements and purpose of the DPPA.

152. As an entity that receives information obtained from state DMVs, Defendant was well-informed that the PII it collected was highly sensitive personal data, and that disclosure of that information to the public would violate the DPPA.

153. Critically, only Defendant had control over the configuration and design of its own systems, and knowingly chose to forego the necessary data protection techniques needed for it to secure Plaintiff's and Class members' PII.

154. Despite the clear dangers that the insecure use of PII poses, Defendant knowingly chose to configure and design its systems to disclose Plaintiff's and Class members' PII to unauthorized third parties.

155. As a result of Defendant's failure to prevent the Data Breach, Plaintiff and Class members have suffered and will continue to suffer injuries, including loss of time and productivity through efforts to ameliorate, mitigate, and deal with the future consequences of the Data Breach; theft of their valuable PII; the actual, imminent, and certainly impeding injury flowing from fraud and identity theft posed by their PII being disclosed to unauthorized recipients and cyber criminals; damages to and diminution in value of their PII; and continued risk to Plaintiff's and the Class

members' PII, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the PII that was entrusted to it.

CLASS ALLEGATIONS

156. Plaintiff brings this case individually and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the following nationwide class:

> All individuals in the United States whose PII was disclosed on insurance quotes or policies by Defendant to unauthorized third parties.

157. Excluded from the Class is Defendant, its subsidiaries and affiliates, its officers, directors and members of their immediate families and any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

158. Plaintiff reserves the right to modify or amend the definition of the proposed Class, if necessary, before this Court determines whether certification is appropriate.

159. The requirements of Rule 23(a)(1) are satisfied. The Class described above is so numerous that joinder of all individual members in one action would be impracticable. According to the Bureau of Internet & Technology of the State of New York Office of Attorney General, the Data Breach affected approximately 88,858 individuals, including approximately 3,912 New York State residents. The disposition of the individual claims of the respective Class members through this class action will benefit both the parties and this Court.

160. The exact size of the Class and the identities of the individual members thereof are ascertainable through Defendant's records, including but not limited to, the information implicated in the Data Breach.

161. The requirements of Rule 23(a)(2) are satisfied. There is a well-defined community of interest and there are common questions of fact and law affecting Class members. The questions of fact and law common to the Class predominate over questions which may affect individual members and include the following:

(a) Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class members;

(b) Whether Defendant was negligent in collecting and disclosing Plaintiff's and Class members' PII;

(c) Whether Defendant had duties not to disclose the PII of Plaintiff and Class members to unauthorized third parties;

(d) Whether Defendant took reasonable steps and measures to safeguard Plaintiff's and Class members' PII;Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class members;

(e) Whether Defendant breached their duties to exercise reasonable care in handling Plaintiff's and Class members' PII by disclosing that information on insurance quotes in the manner alleged herein, including failing to comply with industry and governmental regulator standards;

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

(g) Whether Defendant intentionally configured and designed its online system to benefit its business in such a way that it foreseeably allowed unauthorized

persons and/or cyber criminals to gain access to the PII of Plaintiff and Class members;

(h) Whether Defendant had respective duties not to use the PII of Plaintiff and Class members for non-business purposes;

(i) Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class members that their PII had been compromised;

(j) Whether Defendant violated 18 U.S.C. §§ 2721, *et seq.*, by disclosing Plaintiff's and Class members' PII;

(k) Whether Defendant violated New York General Business Law, § 349, *et seq.*;

(l) Whether Plaintiff and Class members are entitled to damages as a result of Defendant's wrongful conduct; and

(m) Whether Plaintiff and Class members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

162. The requirements of Rule 23(a)(3) are satisfied. Plaintiff's claims are typical of the claims of Class members. The claims of the Plaintiff and Class members are based on the same legal theories and arise from the same failure by Defendant to safeguard PII. Plaintiff and Class members each had their PII disclosed by Defendant to an unauthorized third party.

163. The requirements of Rule 23(a)(4) are satisfied. Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the Class members. Plaintiff will fairly, adequately, and vigorously represent and protect the interests of Class members and has no interests antagonistic to the Class members. In addition, Plaintiff has

retained counsel who are competent and experienced in the prosecution of class action litigation. The claims of Plaintiff and Class members are substantially identical as explained above. While the aggregate damages that may be awarded to the Class members are likely to be substantial, the damages suffered by the individual Class members are relatively small. As a result, the expense and burden of individual litigation make it economically infeasible and procedurally impracticable for each member of the Class to individually seek redress for the wrongs done to them. Certifying the case as a class will centralize these substantially identical claims in a single proceeding, which is the most manageable litigation method available to Plaintiff and the Class and will conserve the resources of the parties and the court system, while protecting the rights of each member of the Class. Defendant's uniform conduct is generally applicable to the Class as a whole, making relief appropriate with respect to each Class member.

CAUSES OF ACTION

COUNT I

(NEGLIGENCE)

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

165. Defendant owed a duty under common law to Plaintiff and Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

166. More specifically, this duty included, among other things: (a) designing, maintaining, and testing Defendant's systems, including its website, to ensure that Plaintiff's and Class members' PII in Defendant's possession was adequately secured and protected; (b)

implementing processes that would detect a breach of its security system in a timely manner; (c) timely acting upon warning and alerts, including those generated by its own security systems, regarding intrusions to its networks; (d) maintaining data security measures consistent with industry and governmental regulator standards; and (e) ensuring that Defendant's systems did not disclose Plaintiff's or Class members' PII to unauthorized third-parties who fraudulently submitted requests for insurance quotes.

167. Defendant's duty to use reasonable care arose from several sources, including but not limited to those described below.

168. Defendant had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class members were the foreseeable and probable victims of any inadequate security practices on the part of Defendant. By collecting and disclosing valuable PII that is routinely targeted by criminals for unauthorized access, Defendant was obligated to act with reasonable care to protect against these foreseeable threats.

169. Defendant admits that it has a duty to protect consumer data. *See* ¶ 96.

170. Defendant had a duty not to engage in conduct that creates a foreseeable risk of harm to Plaintiff and Class members.

171. Defendant breached the duties owed to Plaintiff and Class members and thus was negligent. Specifically, Defendant breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the PII of Plaintiff and Class members; (b) design its on-line systems to prevent unauthorized users from making Plaintiff and Class members involuntary customers of Defendant and then extracting PII from Defendant's on-line system; (c) detect the breach while it was ongoing; (d) maintain security systems consistent with industry and governmental regulator

standards; and (e) disclose that Plaintiff's and Class members' PII in Defendant's possession had been or was reasonably believed to have been, stolen or compromised.

172. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class members, their PII would not have been compromised.

173. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members have suffered injuries, including:

(a) Actual fraud;

(b) Theft of their PII;

(c) Diminution in value of their PII;

(d) Costs associated with requested credit freezes;

(e) Costs associated with the detection and prevention of identity theft;

(f) Costs associated with purchasing credit monitoring and identity theft protection services;

(g) Lowered credit scores resulting from credit inquiries following fraudulent activities;

(h) Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Defendant's Data Breach;

(i) The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being disclosed to cyber criminals;

(j) Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendant with the societal understanding that Defendant would

safeguard Plaintiff's and Class members' data against theft and not allow access and misuse of their data by others; and

(k) Continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff and Class members.

174. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

COUNT II

(NEGLIGENCE *PER SE*)

175. Plaintiff restates and realleges all proceeding factual allegations above as if fully set forth herein.

Negligence *Per Se* Under Section 5 Of The FTC Act

176. 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 companies such as Defendant for failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

177. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with the industry standards, including, disclosing full Driver's License numbers in plain text in response to requests for insurance quotes and configuring and designing its website to speed up the application process by auto populating quote fields at the risk of disclosing Plaintiff's and Class members' highly sensitive data. Defendant's conduct was

particularly unreasonable given the nature and amount of PII it obtained and disclosed and the foreseeable consequences of a data breach.

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

179. Plaintiff and Class members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

180. Moreover, the harm that has occurred is the type of harm that the FTC Act was intended to guard against. Indeed, the FTC has pursued over fifty 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 suffered by Plaintiff and Class members.

181. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members have been injured as described herein and above, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

Negligence *Per Se* Under the DPPA

182. The DPPA states that "[i]t shall be unlawful for any person knowingly to obtain or disclose personal information, from a motor vehicle record, for any use not permitted under section 2721(b) of this title." 18 U.S.C. § 2722(a).

183. The DPPA also states that "[a] State department of motor vehicles, and any officer, employee, or contractor thereof, shall not knowingly disclose or otherwise make available to any person or entity: personal information, as defined in 18 U.S.C. 2725(3), about any individual obtained by the department in connection with a motor vehicle record, except as provided in subsection (b) of this section." 18 U.S.C. § 2721(a)(1).

184. As alleged herein, Defendant utilizes PII obtained from motor vehicle records, including Driver's License numbers, in connection with processing insurance applications.

185. Under the DPPA, Defendant owed a duty to Plaintiff and other Class members to protect and not disclose their PII, including Driver's License numbers, obtained from motor vehicle records.

186. Defendant violated the DPPA by intentionally configuring and designing its insurance quote application portal on its website to disclose Plaintiff's and Class members' PII to anyone who requested an insurance quote. Defendant installed no protections or security measures to protect this information and willfully disclosed it to cyber criminals through the intentional configuration and design of its insurance quote application portal. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and disclosed and the foreseeable consequences of a data breach.

187. Alternatively, Defendant had constructive notice that it had disclosed the PII of Plaintiff and Class members to unauthorized third parties, because it should have been aware that configuring and designing its website to disclose Plaintiff's and Class members' PII to anyone who submitted a request for a quote without authentication or other security protections would cause the disclosure of this information.

188. At the very least, Defendant was willfully ignorant that its website, servers, and systems were configured without any protections to store Plaintiff's and Class members' PII and would disclose that personal information to cyber criminals.

189. Defendant's violation of the DPPA constitutes negligence *per se*.

190. Plaintiff and Class members are within the class of persons that the DPPA was intended to protect against because the DPPA was expressly designed to protect a person's personal information contained in motor vehicle records from unauthorized disclosure.

191. Moreover, the harm that has occurred is the type of harm the DPAA is intended to guard against, *i.e.*, the unauthorized disclosure of personal information from motor vehicle records.

192. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members have been injured as described herein and above, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

Negligence *Per Se* Under The NY Shield Act, N.Y. Gen. Bus. Law § 899-aa, *et seq.*

193. Under N.Y. Gen. Bus. Law § 899-bb(2)(a) "[a]ny person or business that owns or licenses computerized data which includes private information of a resident of New York shall develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information including, but not limited to, disposal of data."

194. "Private information" is defined as "personal information" in combination with at least one other data element defined in N.Y. Gen. Bus. Law § 899-aa(1)(b), such as driver's license numbers.

195. "Personal information" is defined as "any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person." N.Y. Gen. Bus. Law § 899-aa(1)(a).

196. Defendant owns or licenses computerized data that includes the private information, (*i.e.*, names and driver's license numbers) of New York residents, including Plaintiff. As such, Defendant was required to implement and maintain "reasonable safeguards" to protect this information.

197. Pursuant to N.Y. Gen. Bus. Law § 899-bb(2)(b), *et seq.*, Defendant was required to implement a "data security program" that includes reasonable "administrative" "technical" and "physical safeguards."

198. Reasonable administrative safeguards that Defendant should have, but did not undertake, include: (a) designating one or more employees to coordinate a security program; (b) identifying reasonably foreseeable internal and external risks; (c) assessing the sufficiency of safeguards in place to control the identified risks; (d) training and managing employees in the security program practices and procedures; (e) selecting service providers capable of maintaining appropriate safeguards, requiring those safeguards by contract; and (f) adjusting the security program in light of business changes or new circumstances.

199. Reasonable technical safeguards that Defendant should have, but did not, undertake include: (a) assessing risks in network and software design; (b) assessing risks in information processing, transmission, and storage; (c) detecting, preventing, and responding to attacks or system failures; and (d) regularly testing and monitoring the effectiveness of key controls, systems, and procedures.

200. Reasonable physical safeguards that Defendant should have, but did not, undertake include: (a) assessing risks of information storage and disposal; (b) protecting against unauthorized access to or use of private information during or after the collection, transportation and destruction or disposal of the information; and (c) disposing of private information within a reasonable amount of time after it is no longer needed for business purposes by erasing electronic media so that the information cannot be read or reconstructed.

201. Defendant breached its duties to Plaintiff and Class members under the NY Shield Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' private information and personal information.

202. Defendant's violation of the NY Shield Act constitutes negligence *per se*.

203. Plaintiff and Class members are within the class of persons that the NY Shield Act was intended to protect because the NY Shield Act was expressly designed to protect New York residents' private and personal information.

204. The harm that has occurred is the type of harm the NY Shield Act is intended to guard against. Indeed, the entire purpose of the NY Shield Act is to prevent the occurrence of data breaches, like the Defendant Data Breach, which put consumers' PII at risk.

205. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class members, Plaintiff and Class members would not have been injured, or would not have been injured to as great a degree.

206. The injury and harm suffered by Plaintiff and Class members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that a breach of its duties would cause Plaintiff and Class members to suffer foreseeable harm associated with the exposure of their private information and personal information.

207. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members have been injured as described herein and above, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

208. Whether under the FTC Act, the DPPA, or the NY Shield Act, each independently constitutes negligence *per se*.

COUNT III

(VIOLATION OF 18 U.S.C. §§ 2721, *et seq.* (DPPA))

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

210. Pursuant to 18 U.S.C. § 2722(a), "[i]t shall be unlawful for any person knowingly to obtain or disclose personal information, from a motor vehicle record, for any use not permitted under section 2721(b) of this title."

211. Pursuant to 18 U.S.C. § 2721(a)(1), "[a] [s]tate department of motor vehicles, and any officer, employee, or contractor thereof, shall not knowingly disclose or otherwise make available to any person or entity: personal information, as defined in 18 U.S.C. 2725(3), about any individual obtained by the department in connection with a motor vehicle record, except as provided in subsection (b) of this section."

212. The DPPA provides a civil cause of action against "a person who knowingly obtains, discloses or uses personal information, from a motor vehicle record, for a purpose not permitted" under the statute. 18 U.S.C. § 2724(a).

213. "Person" is defined as "an individual, organization or entity." 18 U.S.C. § 2725(2). Defendant is a "person" under the DPPA.

214. "Personal information" is defined as "information that identifies an individual, including an individual's . . . driver identification number. . ." 18 U.S.C. § 2725(3). Plaintiff's and Class members' PII, which includes Driver's License numbers, is "personal information" under the DPPA.

215. "Motor vehicle record" is defined as "any record that pertains to a motor vehicle operator's permit, motor vehicle title, motor vehicle registration, or identification card issued by a department of motor vehicles." 18 U.S.C. § 2725(1). Defendant obtains motor vehicle records containing Plaintiff's and Class members' PII, including their Driver's License numbers.

216. Defendant obtains motor vehicle records as part of its business operations intended to generate online insurance quotes and/or insurance policy processing for profit.

217. Defendant's disclosure of Plaintiff's and Class members' personal information to unauthorized individuals violated 18 U.S.C. §§ 2722(a) and/or 2721(a)(1).

218. Defendant's disclosure of personal information was not a permitted use under 18 U.S.C. § 2721(b).

219. Defendant knowingly obtained and/or disclosed Plaintiff's and Class Member's personal information, which came from a motor vehicle record, for a purpose not permitted under the DPPA.

220. Defendant knowingly and voluntarily configured and designed its insurance quote application portal on its website to disclose Plaintiff's and Class members' PII to anyone who requested an insurance quote, all in direct violation of the DPPA.

221. Defendant installed no protections or security measures to protect this exposed information and willfully disclosed it to cyber criminals through the intentional configuration and design of its insurance quote application portal.

222. Alternatively, Defendant had constructive notice that it had disclosed the PII of Plaintiff and Class members to unauthorized third parties, because it should have been aware that configuring and designing its website to disclose Plaintiff's and Class members' PII to anyone who submitted a request for a quote without authentication or other security protections would cause the disclosure of this information.

223. Further, Defendant was on notice of the February 2021 Cyber Fraud Alert and March 2021 Cyber Fraud Alert Follow-Up which informed Defendant that cyber criminals were exploiting cybersecurity flaws on automobile insurance websites who offer instant online automobile insurance premium quotes by stealing nonpublic information, including Driver's License numbers.

224. At the very least, Defendant was willfully ignorant that its website, servers, and systems were configured and designed without any protections to store Plaintiff's and Class members' PII and would disclose that personal information to cyber criminals.

225. Merriam-Webster's dictionary defines "disclose" as "to make known or public," "to expose to view," or, alternatively, "to open up." None of these definitions requires an identified intended recipient. Instead, disclosure is the act of exposure. Whether or not Defendant meant for identifiable third parties to access the information is not relevant. All that is required for a knowing disclosure is a voluntary action.

226. Pursuant to 18 U.S.C. § 2724(b)(1)-(4), Plaintiff seeks, on behalf of herself and members of the Class (1) actual damages, not less than statutory liquidated damages in the amount of $2,500; (2) punitive damages; (3) reasonable attorneys' fees and costs; and (4) preliminary and equitable relief as the Court determines to be appropriate.

COUNT IV

(NEW YORK GENERAL BUSINESS LAW, N.Y. GEN. BUS. LAW § 349, *et seq.*)

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

228. New York General Business Law § 349 ("§ 349") prohibits "deceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state." § 349(a).

229. Plaintiff and Class members are "person[s]" within the meaning of § 349.

230. Plaintiff is authorized to bring a private action under § 349(h).

231. Defendant conducts business and provides its services, including auto insurance quotes and policies, in the State of New York.

232. In the conduct of its business, trade, and commerce, and in furnishing services in the State of New York, Defendant's actions were directed at consumers.

233. In the conduct of their business, trade, and commerce, and in furnishing services in the State of New York, Defendant engaged in deceptive, unfair, and unlawful trade acts or practices, in violation of § 349(a), including but not limited to, the following:

(a) Collecting, storing, and/or gaining access to Plaintiff's and Class members' PII without their knowledge or consent;

(b) Failing to disclose to Plaintiff's and Class members that it would collect, store, and/or gain access to their PII;

(c) Failing to disclose to Plaintiff's and Class members that it would disclose their PII without their knowledge or consent;

(d) Failing to develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of Plaintiff' and Class members' PII, and omitting, suppressing, and concealing the material fact of that failure;

(e) Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and omitting, suppressing, and concealing the material fact of that failure;

(f) Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class members' PII, including by implementing and maintaining reasonable security measures;

(g) Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

(h) Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class members' PII;

(i) 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' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45; and

(j) Failure to comply with the NY Shield Act as a *per se* violation of N.Y. Gen. Bus. Law § 899-bb(2)(d).

234. Defendant systematically engaged in these deceptive, misleading, and unlawful acts and practices, to the detriment of Plaintiff and Class members.

235. Defendant willfully engaged in such acts and practices and knew that it violated § 349 or showed reckless disregard for whether it violated § 349.

236. As a direct and proximate result of Defendant's deceptive trade practices, Plaintiff and Class members suffered injury and/or damages, including the loss of their legally protected interest in the confidentiality and privacy of their PII.

237. The above unfair and deceptive practices and acts by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

238. Defendant knew or should have known that the online system it configured and designed, its data security practices, and its unauthorized disclosures were inadequate to safeguard Class members' PII and that therefore the risk of data breach or PII disclosures to unauthorized third parties was highly likely. Defendant's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless.

239. Plaintiff and Class members seek relief under § 349(h), including, but not limited to, actual damages, treble damages, statutory damages, injunctive relief, and/or attorneys' fees and costs.

COUNT V

(DECLARATORY AND INJUNCTIVE RELIEF)

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

241. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Amended Complaint.

242. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class members' PII and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and Class members from further data breaches that compromise their PII. Plaintiff alleges that Defendant's data security measures remain inadequate. Defendant publicly denies these allegations. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of her PII and remains at imminent risk that further compromises of her

PII will occur in the future. Defendant has not revealed to Plaintiff what specific measures and changes Defendant has undertaken in response to the Data Breach.

243. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

(a) Defendant owes a legal duty to secure consumers' PII and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, the NY Shield Act, and the DPPA;

(b) Defendant continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII; and

(c) Defendant's ongoing breaches of its legal duty continue to cause Plaintiff harm.

244. This Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry and government regulatory standards to protect consumers' PII. Specifically, this injunction should, among other things, direct Defendant to:

(a) engage third party auditors, consistent with industry standards, to test its systems for weakness and upgrade any such weakness found;

(b) audit, test, and train its data security personnel regarding any new or modified procedures and how to respond to a data breach;

(c) regularly test its systems for security vulnerabilities, consistent with industry standards;

(d) implement an education and training program for appropriate employees regarding cybersecurity.

245. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lacks an adequate legal remedy, in the event of another data breach at Defendant's operations. The risk of another such breach is real, immediate, and substantial. If another breach at Defendant occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and she will be forced to bring multiple lawsuits to rectify the same conduct.

246. The hardship to Plaintiff if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

247. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Defendant, thus eliminating the additional injuries that would result to Plaintiff and consumers whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff on behalf of herself and all others similarly situated, prays for relief as follows:

(A) For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

(B) For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

(C) For damages in an amount to be determined by the trier of fact;

(D) For an order of restitution and all other forms of equitable monetary relief;

(E) Declaratory and injunctive relief as described herein;

(F) Awarding Plaintiff reasonable attorneys' fees, costs, and expenses;

(G) Awarding pre- and post-judgment interest on any amounts awarded; and

(H) Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMAND

A jury trial is demanded on all claims so triable.

Dated: March 3, 2022

Respectfully submitted,

GAINEY McKENNA & EGLESTON

By: */s/ Thomas J. McKenna*
Thomas J. McKenna
Gregory M. Egleston
501 Fifth Avenue, 19th Floor
New York, NY 10017
Telephone: (212) 983-1300
Facsimile: (212) 983-0383
Email: tjmckenna@gme-law.com
Email: gegleston@gme-law.com

Counsel for Plaintiff