Exhibit A

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

IN RE LEMONADE, INC. DATA DISCLOSURE LITIGATION	Case No. 1:25-cv-04106-JHR-KHP **CONSOLIDATED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Gregory Klein, Leslie Linwood Rich, and Brian Murray ("Plaintiffs"), individually and on behalf of all others similarly situated, by and through their undersigned counsel, bring this class action complaint against defendants Lemonade, Inc. and Lemonade Insurance Agency, LLC (collectively, "Defendants" or "Lemonade") and allege as follows:

I. INTRODUCTION

1. Driver's license numbers (DLNs) are highly valuable pieces of personal information (PI). Threat actors seek them out as a critical part of a fraudulent, synthetic identity. DLNs are particularly useful to identity thieves in applying for unemployment or other government benefits.

2. In recognition of the sensitivity of driver's license information (and its utility to identity thieves), Congress passed the Driver's Privacy Protection Act, 18 U.S.C. §§ 2721, *et seq.* (DPPA), which restricts access to driver's license information—including DLNs—among other PI defined in the statute; mandates that private companies limit use that information to a handful of enumerated purposes; and prohibits unauthorized disclosure.

3. Defendants provide private passenger automobile insurance policies in the United States. They market their insurance policies through their website, https://www.lemonade.com/car, which contains an online quoting platform ("Quote Platform") through which prospective customers can apply for insurance coverage and receive a quote.

4. In violation of the DPPA, Defendants knowingly and willfully designed and implemented a feature on their Quote Platform that auto-populated—and thereby disclosed—an individual's DLN after only a bare minimum of publicly available information was entered about an individual (i.e., name, address, etc.).

5. Defendants disclosed DLNs through their Quote Platform even though the requesting users had no permissible purpose to access or view the numbers under the DPPA. And they did so without taking any steps to verify the identity of the user requesting the DLNs, or otherwise ensuring DLNs were shown to only the individuals to whom they belonged.[1]

6. Defendants did so for their own self-interest: to increase the likelihood that consumers would complete their applications and purchase insurance policies. By automatically populating consumers' DLNs in the Quote Platform, Defendants sidestepped the process of asking Quote Platform visitors to manually enter their DLNs, reducing consumer friction in the quote process, and selling more insurance. But they did so at the expense of individuals' privacy—displaying their highly sensitive DLNs.

7. Defendants obtained these DLNs from a third party's "prefill" service.

8. Nothing about Defendants' underwriting or insurance quoting process required them to obtain prefilled DLNs, use them for marketing or sales, or display them through their website. Indeed, Defendants had offered online insurance quotes to applicants long before they incorporated this auto-population feature into their Quote Platform.

9. Instead, Defendants added the auto-population feature to gain a competitive advantage in their sales process. That is, the less information requested from the prospective

[1] Jonathan Greig, *Insurance firm Lemonade says breach exposed driver's license numbers,* THE RECORD (Apr. 14, 2025), https://therecord.media/lemonade-insrance-breach-numbers-license.

customer, the more likely they are to finish the application and purchase insurance from Defendants.

10. By knowingly and intentionally designing and implementing the auto-population feature on their Quote Platform and obtaining and using prefilled DLNs rather than customer-provided DLNs, Defendants knowingly and intentionally obtained, used, and disclosed the DLNs of Plaintiffs and members of the class, in violation of the DPPA.

11. In essence, in their pursuit of increased sales, Defendants intentionally created a website that allowed anyone to look up another person's DLN, merely by entering rudimentary information about such a person.

12. Unsurprisingly, Defendants' profit-seeking conduct quickly caught the attention of opportunists, who utilized Defendants' Quote Platform to obtain the highly sensitive DLNs of approximately 190,000 consumers, including Plaintiffs, over the course of *17 months* (the "Data Disclosure"). Defendants failed to discover this for nearly *two years*—i.e., from when the Data Disclosure began in April 2023 until Defendants discovered it in March 2025.[2]

13. Defendants sent letters to individuals impacted by the Data Disclosure beginning on or about April 10, 2025 (the "Notice" or "Notices"). The Notices stated that between April 2023 and September 2024 it was discovered that "due to a vulnerability in [Lemonade's] Online Flow, certain driver's license numbers for identifiable individuals were likely exposed."[3]

14. In the Notices, Defendants acknowledged that DLNs accessed through the Data Disclosure can be used to conduct various forms of fraud and identity theft. They advised impacted individuals to "Review Accounts and Credit Reports" and set up "Security Freezes and Fraud

[2] *Id.*

[3] LEMONADE, Individual Template Notice, https://oag.ca.gov/system/files/Template%20Individual%20Notice%20%28Version%201%29.pdf

Alerts." Defendants urged impacted individuals to "remain vigilant with respect to reviewing your account statement and credit reports, and you should promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities." They noted that following their advice regarding precautionary steps could "delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit."[4]

15. Defendants' Notices revealed that the DLNs were obtained after the input of names, dates of birth, and addresses (commonly referred to as "phone book" information)—information publicly available through a simple Google search or accumulated in databases and widely available on the internet.

16. As a result of the Data Disclosure, Plaintiffs' privacy has been invaded, their sensitive driver's license information is in the hands of unauthorized third parties, and they face a substantially increased risk of identity theft and fraud. Accordingly, Plaintiffs now must take immediate and time-consuming steps to protect themselves from identity theft and fraud.

17. To redress Defendants' illegal, self-interested, profit-seeking conduct, Plaintiffs bring this class action on behalf of themselves and all other individuals who had their DLNs improperly obtained by Defendants, improperly used by Defendants, or improperly displayed or otherwise disclosed on Defendants (the "Class" or "Class Members").

18. Plaintiffs, on behalf of themselves and all Class Members, seek remedies, including monetary damages and injunctive relief (including relief under the federal Declaratory Judgment Act), for negligence, negligence per se, violations of the DPPA, violations of New York General

[4] *Id.*

Business Law and, on behalf of the Connecticut class defined below, violations of Connecticut Unfair Trade Practices Act.

II. PARTIES

19. Plaintiff **Gregory Klein** is a resident and citizen of the State of New York.

20. Plaintiff **Leslie Linwood Rich** is a resident and citizen of the State of Arizona.

21. Plaintiff **Brian Murray** is a resident and citizen of the State of Connecticut.

22. Defendant **Lemonade, Inc.** is a company with its principal place of business in New York, New York. Defendant, though its affiliates, insures private passenger automobiles and provides homeowner and other types of insurance for qualified applicants.

23. Defendant **Lemonade Insurance Agency, LLC** is a domestic limited liability company organized under the laws of New York, with its principal place of business in New York, New York. Defendant Lemonade Insurance Agency, LLC is an affiliate of Lemonade, Inc., with whom it has a managing general agency agreement.[5]

III. JURISDICTION AND VENUE

24. This Court has subject-matter jurisdiction over this action under 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.*

25. This Court also has supplemental jurisdiction over Plaintiffs' state-law claims under 28 U.S.C. § 1367(a).

26. Alternatively, this Court has subject-matter jurisdiction over this action under the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), because the aggregate amount in

[5] Justin Mathew, *Report on Examination of Lemonade Insurance Company as of Dec. 31, 2022*, at 5, N.Y. DEP'T OF FIN. SERV. (June 21, 2024), https://www.dfs.ny.gov/system/files/documents/2024/06/16023f22.pdf.

controversy exceeds $5 million, exclusive of interest and costs; the number of members of the proposed Class exceeds 100; and diversity exists because, upon information and belief, at least one Class Member and Defendants are citizens of different states.

27. The Court has personal jurisdiction over Defendants because they maintain their headquarters and principal places of business in this District and conduct significant business in this District, thus availing themselves of New York's markets by selling auto insurance policies therein; Defendants have sufficient minimum contacts with New York; and a substantial part of the conduct giving rise to Plaintiffs' claims occurred in this District.

28. Venue properly lies in this District under 28 U.S.C. § 1391 because, *inter alia*, a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in, were directed to, and/or emanated from this District; Defendants transact substantial business and have agents in this District; a substantial part of the conduct giving rise to Plaintiffs' claims occurred in this District; and because Defendants are headquartered within this District.

IV. FACTUAL ALLEGATIONS

A. Defendants collect vast amounts of sensitive PI—including DLNs.

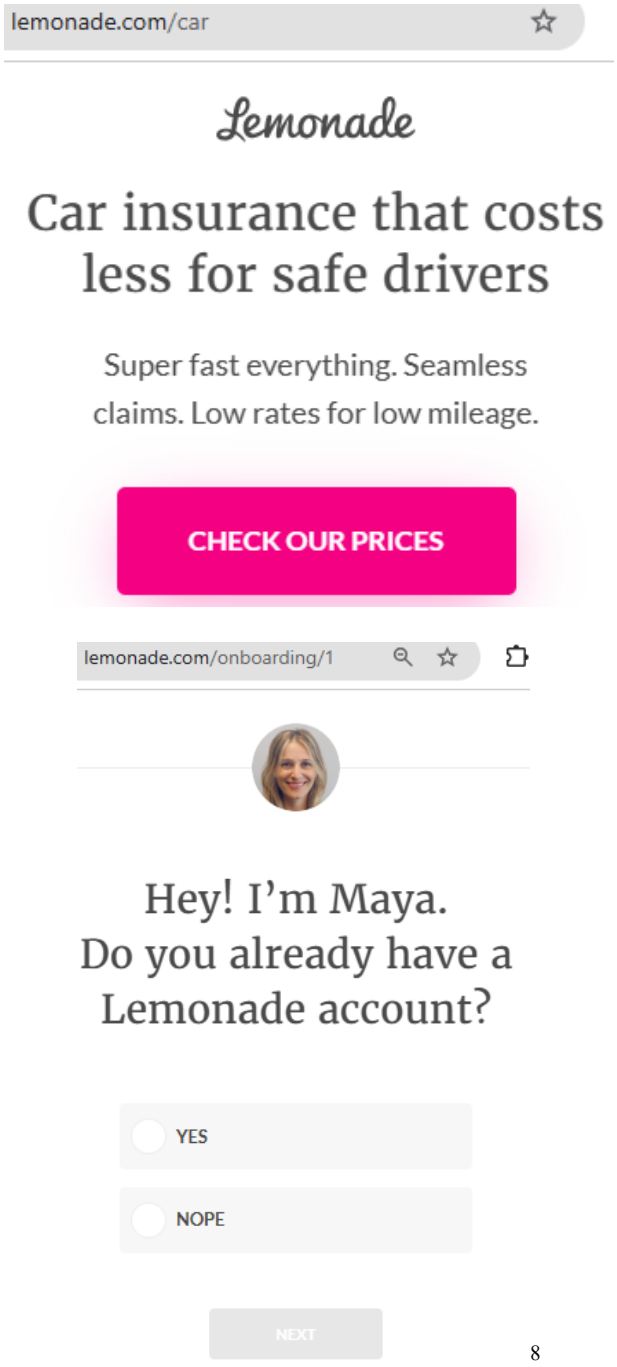
29. Defendants offer private passenger automobile insurance to individuals nationwide.

30. Defendants' marketing is primarily through direct response methods in which Defendants provide insurance quotes directly to consumers through their website.

31. Like other insurance providers, Defendants have a publicly available online Quote Platform.[6]

[6] *See* LEMONADE, https://www.lemonade.com/car (last visited Aug. 27, 2025).

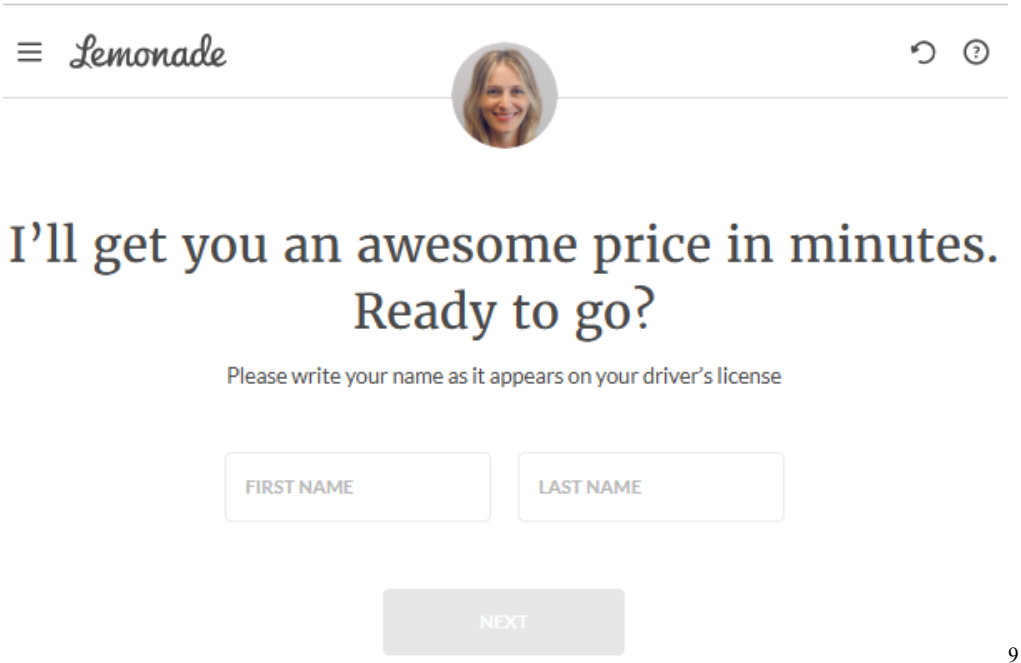
32. Visitors to Defendants' Quote Platform can get a quote instantly after providing basic personal information in a series of pages on Defendants' website, as depicted below[7]:



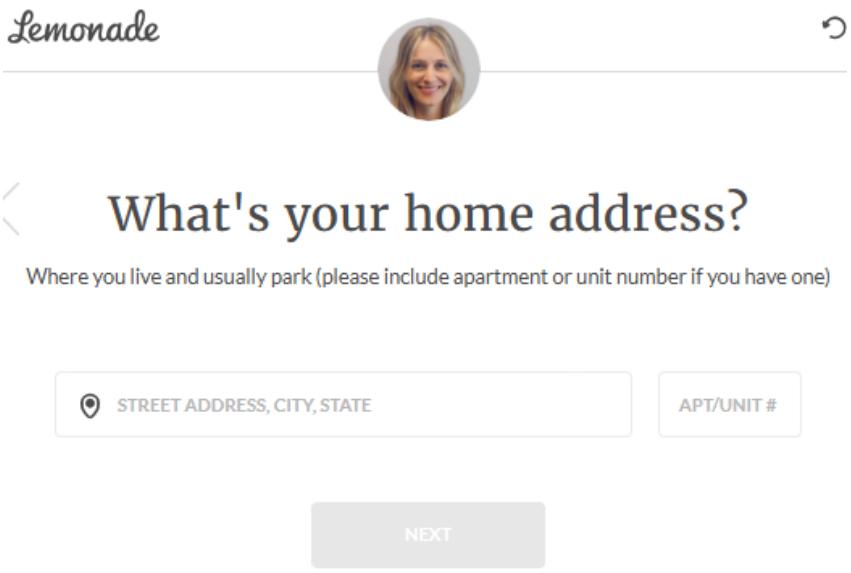
[8]

[7] *Id.*

[8] LEMONADE, *Onboarding,* https://www.lemonade.com/onboarding/1 (last visited Aug. 27, 2025).



9



10

33. Defendants' Quote Platform uses the information entered by the website visitor to request DLNs from a third-party vendor. It then automatically prefills the DLN that the vendor returns.

[9] LEMONADE, *Pricing Tool,* https://www.lemonade.com/car/1?f=1 (last visited Aug. 27, 2025).

[10] LEMONADE, *Pricing Tool,* https://www.lemonade.com/car/2 (last visited Aug. 27, 2025).

34. Specifically, Defendants' quoting feature asks a visitor to the site for a name, date of birth, and address. It takes no steps to verify that the user is entering their own information. Once that information is entered, however, Defendants' system auto-populates the Quote Platform with the corresponding DLN. In doing so, Defendants made that DLN visible to the unverified person entering the information on the Defendants' Quote Platform.

35. A person's name, date of birth, and address are often easily obtained. Defendants knew that this information was often available to the public at no cost, and that cybercriminals are commonly in possession of such data.[11]

36. Defendants nevertheless knowingly and intentionally designed their Quote Platform to function as a driver's license lookup tool, allowing criminals to use an automated process to harvest DLNs that Defendants were knowingly and intentionally disclosing through the coding created for their Quote Platform.

37. The proposed Class includes many people who never applied for insurance with Defendants, were not Defendants' customers, and may not even have been aware of Defendants' existence until the Data Disclosure occurred. In other words, unauthorized parties availed themselves of the PI that Defendants made publicly available via their Quote Platform on a wholesale basis.

[11] For example, "[s]ince approximately 2009, MyLife has purchased public record data about individuals from data brokers. … MyLife uses that data to create a 'public listing' or profile for these individuals, which can be accessed through their website, www.mylife.com. … On their website, MyLife has profiles purporting to cover at least 320 million individuals. ... Information that may be available through a *free search may include: name; city and state of residence; … email address, and mailing address associated with the profile; date of birth*; …." *United States v. MyLife.com, Inc.*, 567 F. Supp. 3d 1152, 1157-58 (C.D. Cal. 2021) (citations omitted) (emphasis added).

38. Defendants' Quote Platform did not require verification that the person or automated process accessing the system was actually the individual for whom the information was being entered.

39. In addition, Defendants' Quote Platform did not employ effective, industry-standard security measures to detect whether the website visitor was, in fact, a "bot" or other automated process rather than an individual person.

40. Instead, Defendants knowingly and intentionally configured their online Quote Platform to provide DLNs when anyone, including bots, merely entered basic information such as a person's name, date of birth, and address.

41. The Data Disclosure did not require any hacking, stolen credentials, breaking into any systems, or bypassing any firewalls. Defendants simply made the DLNs publicly available.

B. Defendants contravened the purpose of the DPPA.

42. Prior to the enactment of the DPPA, Congress found that most states freely turned over DMV information to whomever requested the data, with few restrictions. 137 Cong. Rec. 27,327 (1993).

43. Because of the lack of restrictions, Congress grew concerned that potential criminals could easily obtain the private information of potential victims. 140 Cong. Rec. 7929 (1994) (statement of Rep. Porter Goss).

44. These concerns did, in fact, materialize in the occurrence of crime, harassment, and stalking. Most notably, in 1989, a stalker shot and killed Rebecca Schaeffer, an up-and-coming actor, after obtaining her unlisted home address from the California DMV. 137 Cong. Rec. 27,327 (1993). In advocating for the DPPA, Representative Jim Moran (D-VA) recounted thieves using information from the DMV to learn home addresses and commit burglary and theft. 137 Cong. Rec. 27,327 (1993). Similarly, Senator Barbara Boxer (D-CA) explained how a man used the

DMV to obtain the home addresses of several young women and sent them harassing letters. 39 Cong. Rec. 29,466 (1993). In another instance, a woman who visited a clinic that performed abortions found black balloons outside her home after a group of anti-abortion activists sought to harass her upon seeing her car in the clinic's parking lot. 139 Cong. Rec. 29,462 (1993) (statement of Sen. Chuck Robb).

45. In response to public outrage over the Schaeffer murder, and growing concern for the threat to public safety that free access to DMV records posed, Congress enacted the DPPA "to protect the personal privacy and safety of licensed drivers consistent with the legitimate needs of business and government." S. Res. 1589, 103rd Cong. §1(b), 139 Cong. Rec. 26,266 (1993) (enacted).

46. Additionally, in enacting the DPPA, Congress was motivated by their "[c]oncern[] that personal information collected by States in the licensing of motor vehicle drivers was being released – even sold – with resulting loss of privacy for many persons." *Akkawi v. Sadr*, No. 2:20-CV-01034-MCE-AC, 2021 WL 3912151, at *4 (E.D. Cal. Sept. 1, 2021) (citing *Maracich v. Spears*, 570 U.S. 48, 51–52 (2013) (alterations in original)). The release of private information such as DLNs and other motor vehicle records was the exact impetus for the DPPA's passage.

47. Congress sought to expressly prohibit "disclosing personal information obtained by the department in connection with a motor vehicle record . . . ." *Chamber of Com. of United States v. City of Seattle*, 274 F. Supp. 3d 1140, 1154 (W.D. Wash. 2017). DLNs are thus explicitly listed as "personal information" from "motor vehicle records" under the DPPA. *See* 18 U.S.C. 2725(1), (3). As such, Congress used their lawmaking authority to properly elevate the disclosure of DLNs and other motor vehicle records into a concrete harm, a harm that bears a sufficiently close relationship to the tort of public disclosure long recognized at common law.

48. By knowingly obtaining and using the PI of Plaintiffs and the Class for sales and marketing purposes, and by knowingly disclosing that PI to the public, Defendants ran afoul of the purpose of the DPPA, and threatened the privacy and safety of licensed drivers, for whose protection the statute was enacted. Defendants' actions constituted a concrete injury and particularized harm to Plaintiffs and Class Members, that would not have happened but for Defendants' failure to adhere to the DPPA. Plaintiffs were harmed by the public disclosure of their DLNs in addition to the other harms enumerated herein.

C. Defendants were on notice that cybercriminals were harvesting DLNs from insurers' quote platforms, like their own. They disclosed DLNs anyway.

49. In their Notice, Defendants informed consumers that their sensitive PI—namely, DLNs—was compromised in a security incident, which it described as follows:

> Through certain of their subsidiaries, Lemonade offers car insurance policies through an online application process at www.lemonade.com/car (the "Online Flow"). Using the Online Flow to obtain an insurance quote and purchase a policy, an individual enters certain information – name, date of birth, and residential address. On March 24, 2025, we learned that due to a vulnerability in our Online Flow, certain driver's license numbers for identifiable individuals were likely exposed.
>
> Lemonade believes that the unauthorized exposures spanned from approximately April 2023 through September 2024.

50. Although the Notice indicates that Defendants "promptly took steps to eliminate the vulnerability," the notice also makes clear that Defendants failed to discover the Data Disclosure for *17 months* while it remained ongoing, and failed to detect it for *two years* after it begun.

51. Defendants' obtainment of the DLNs, use of the DLNs, their Data Disclosure, and their violation of the law—including the DPPA—assisted an ongoing and concerted campaign by fraudsters to engage with insurers' Quote Platforms to obtain DLNs to perpetuate known occurrences of fraud and identity theft.

52. On February 16, 2021, the New York State Department of Financial Services (DFS) issued an alert to automobile insurers regarding an ongoing systemic and aggressive campaign to engage with public-facing insurance websites—particularly those that offer instant online automobile insurance quotes like Defendants' website—to obtain non-public information, in particular unredacted DLNs.[12] According to the alert, the unauthorized collection of DLNs appeared to be part of a growing fraud campaign targeting pandemic and unemployment benefits. DFS first became aware of the campaign when it received reports from two auto insurers in December 2020 and January 2021 that cybercriminals were targeting their websites that offer instant online automobile insurance quotes to obtain unredacted DLNs.

53. Insurers' instant online auto quoting websites are the primary entry point for cybercriminals to access consumers' PI. As the industry has accelerated adoption of faster-quoting processes and tools to achieve competitive advantage, new vulnerabilities have opened.[13]

54. According to DFS, insurers noticed an unusually high number of abandoned quotes or quotes not pursued after the display of the estimated insurance premium. On the instant quote websites, "criminals entered valid name, any date of birth and any address information into the required fields" and "then displayed an estimated insurance premium quote along with partial or redacted consumer [PI] including a driver's license number. The attackers captured the full, unredacted [DLNs] without going any further in the process and abandoned the quote."[14]

55. In January 2021, DFS alerted approximately a dozen entities maintaining such websites that they were likely targets of unauthorized third parties looking to gain access to New

[12] *See* N.Y. DEP'T OF FIN. SERV., Industry Letter Re: Cyber Fraud Alert (Feb. 16, 2021), https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210216_cyber_fraud_alert#_edn.

[13] *Id.*

[14] *Id*.

Yorkers' PI, and specifically DLNs. Following the alert, six additional insurers reported the malicious targeting of their websites to DFS—two of which reported that the fraudsters failed to gain access to PI, and four of which reported that fraudsters either gained access to PI or that their investigation was still ongoing. In the alert, DFS did not name the websites affected or the insurers.

56. The DFS issued a second cyber fraud alert on March 30, 2021, urging companies like Defendants to avoid displaying prefilled DLNs "considering the serious risk of theft and consumer harm."[15]

57. The increase in interest in DLNs is, in part, a product of the changes brought on by the COVID-19 pandemic, as various types of financial transactions that used to be conducted exclusively in person have been transferred online. Some states are also allowing residents to use their expired driver's licenses for various purposes for an extended period, due to the difficulty in securing the in-person DMV appointments necessary to renew them.[16]

58. Unsurprisingly, fraudulent unemployment claims spiked during the pandemic, as more money became available to displaced workers and the requirements for filing eased. Many states even paid out tens of millions of dollars to scammers, a phenomenon largely driven by the unauthorized use of fraudulently obtained PI. Threat actors have been caught using not just sensitive personal data for these fraudulent unemployment claims but also hacking into existing unemployment accounts to change bank payment information.[17]

---

[15] N.Y. DEP'T OF FIN. SERV., Industry Letter Re: Cyber Fraud Alert Follow-Up (Mar. 30, 2021), https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210330_cyber_alert_followup.

[16] Scott Ikeda, *Geico Data Breach Leaks Driver's License Numbers, Advises Customers to Watch Out for Fraudulent Unemployment Claims*, CPO MAGAZINE (Apr. 23, 2021), https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/.

[17] *Id.*

59. The United States Department of Labor estimates that pre-pandemic fraudulent unemployment claims accounted for about 10% of all filings.[18] A normal yearly cost for fraudulent unemployment claims is about $3 billion; recent reports indicate that this number ballooned to $200 billion during the pandemic. Fraudulent first-time claims drove a lot of this activity, but experts expect the problem to persist even as most Americans head back to work. Some will fail to notify the state unemployment office of their change in employment status, creating an opening for scammers.

60. Defendants knew that they were using driver's license information on their online sales Quote Platform. Defendants also knew that this platform was created and maintained in a way that allowed fraudsters to plug in readily, publicly available basic PI of other persons, and that the website would auto-populate driver's license information once that basic information was entered. Indeed, Defendants were responsible for their Quote Platform, including its design and design features. Defendants thus knew or should have known that their website and the website's auto-populate feature disclosed consumers' DLNs to unauthorized third parties. This is exactly how Defendants designed their website to operate.

61. Defendants knew that they were obtaining and using DLNs for marketing and sales purposes, and that they were disclosing DLNs to the public. But they failed to assess—or intentionally ignored—reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of consumers' PI, and failed to implement basic safeguards to protect the security, confidentiality, and integrity of that information.

[18] Megan DeMatteo, *Unemployment fraud costs victims $200 billion annually in the U.S.—here's how to protect yourself*, CNBC SELECT (Dec. 3, 2023), https://www.cnbc.com/select/how-to-protect-yourself-from-unemployment-fraud/.

62. By adding the auto-population feature to their Quote Platform, which Defendants knowingly and intentionally chose to do, Defendants intended to use the DLNs and make the returned information easily accessible to anyone who entered basic information into their system.

63. Defendants did not impose any security protocols to ensure that website visitors entered and accessed PI only about themselves. Defendants did not impose effective security protocols to prevent automated bots from accessing consumers' PI.

64. Thus, Defendants knowingly used and posted consumers' DLNs directly to all members of the public through their knowing, intentional creation of their Quote Platform and the functionality they designed and implemented therein.

D. Defendants acknowledged that the use of data and the Data Disclosure created a substantial risk of identity theft and fraud.

65. The harm caused to Plaintiffs and Class Members by Defendants' obtainment, use, and disclosure of DLNs is already apparent. Criminals now possess Plaintiffs' and Class Members' DLNs, and their only purpose in obtaining and possessing that information is to monetize that data by selling it on the darknet or dark web or using it to commit other types of fraud.

66. Defendants' Notices put the burden on Plaintiffs and Class Members to take mitigating steps to protect their information: "remain vigilant with respect to reviewing your account statement and credit reports, and you should promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities" and explains how to obtain one's credit reports, including initiating a credit freeze, checking the consumer's credit report, and enrolling in identity theft insurance.

67. Having received the Notices about this Data Disclosure, it is reasonable for Plaintiffs and Class Members to believe that the risk of future harm (including identity theft or fraud) is substantial and imminent, and to take steps to mitigate that substantial risk of future harm.

Defendants' specific instructions and warnings in the Notices relate to the fact that threat actors take DLNs for the purpose of committing fraud in the name of the person whose DLN is taken.

E. The DLNs Defendants obtained, used, and then disclosed in their Data Disclosure are highly valuable to fraudsters.

68. It is well known among companies that store or have access to sensitive PI that DLNs are valuable and frequently targeted by criminals. The PI that Defendants voluntarily disclosed via their Quote Platform in violation of state and federal law is very valuable to phishers, identity thieves, cybercriminals, and other fraudsters, especially as an unprecedented number of criminals are filing fraudulent unemployment benefit claims, and driver's license information is uniquely connected to the ability to file such claims and commit other financial fraud. Unsecured sites that contain or transmit PI like DLNs require notice to consumers when the data is stolen because it can be used to commit identity theft and other types of fraud.

69. The DLNs disclosed in Defendants' Data Disclosure are significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. By contrast, the information exposed in Defendants' Data Disclosure can be used to *open* fraudulent bank accounts and credit and debit cards, or to take out loans, especially student loans. The DLNs disclosed in Defendants' Data Disclosure are also more valuable because they are long lasting, and difficult (if not impossible) to change.

70. With access to an individual's driver's license number, criminals can commit all manner of fraud, including: obtaining government benefits in the victim's name, filing fraudulent tax returns using the victim's information, or obtaining a driver's license or official identification card in the victim's name but with the thief's picture. In addition, identity thieves may obtain a job, rent a house, or receive medical services in the victim's name, and may even give the victim's

DLN during an arrest, resulting in an arrest warrant being issued in the victim's name.[19] They can also use the driver's license when receiving a ticket or to provide to an accident victim, to replace or access account information on social media sites, to obtain a mobile phone, to dispute or approve a SIM swap, to redirect U.S. mail, to gain unauthorized access to the United States, to claim a lost or stolen passport, to use as a baseline to obtain a Commercial Driver's License, or to engage in phishing or other social engineering scams.

71. Fraudsters often aggregate information taken from data security incidents to build profiles on individuals. These profiles combine publicly available information with information discovered in previous data security incidents and exploited vulnerabilities. Unique identifiers such as Social Security numbers, DLNs, usernames, and financial account numbers (e.g., credit cards, insurance policy numbers, etc.) are critical to forging an identity. Persistent identifiers, such as Social Security numbers and DLNs, are particularly valuable. When not all information is available, the information that is stolen is used to socially engineer a victim into providing additional information so a "fullz"[20] profile can be obtained.

72. There is no legitimate or legal reason for anyone to use Defendants' website to acquire driver's license information on Plaintiffs and Class Members. Dark Net Markets ("DNMs"), or the "dark web," is a heavily encrypted part of the internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the dark web due to this encryption, which allows users and criminals to conceal identities and online activity. When malicious actors obtain ill-gotten PI, that information often ends up on the dark web because the

[19] *See* FED. TRADE COMM'N, *Warning Signs of Identity Theft*, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited Aug. 27, 2025).

[20] "Fullz" is slang used by threat actors and various criminals meaning "full information," a complete identity profile or set of information for an entity or individual.

malicious actors buy and sell that information for profit.[21] "Why else would hackers . . . steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities." *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015).

73. Any non-public data, especially government-issued identification numbers like a driver's license or non-driver's identification number, has criminal value.[22] For example, a fake U.S. citizenship kit for sale—passport, Social Security number, driver's license, and birth certificate—is offered on the dark web for 0.218 bitcoin (or $1,400 at the time) and a stolen/fake driver's license (by U.S. state) for $200 in bitcoin.[23]

74. Blogger John Egan, from the national credit reporting company Experian, emphasized the value of driver's license information to thieves and cautioned:

> Your stolen driver's license number can be the key to unlock all sorts of fraud, such as opening financial accounts in your name or creating fake IDs. [If] stolen in a data breach. . . it can wreak havoc on your finances.[24]

75. In fact, according to the data privacy and cyber security publication CPO Magazine:

> To those unfamiliar with the world of fraud, driver's license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation. Tim Sadler, CEO of email security firm Tessian, points out why this is not the case and

---

[21] IDENTITY FORCE, *Shining a Light on the Dark Web with Identity Monitoring* (Feb. 1, 2020), https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last visited Aug. 27, 2025).

[22] IDENTITY THEFT RESOURCE CENTER, *Can Someone Steal Your Identity From Your Driver's License?* (April 16, 2025), https://www.idtheftcenter.org/can-someone-steal-your-identity-from-your-drivers-license/ (last visited Aug. 27, 2025).

[23] Daniel Shkedi, *Heart of Darkness: Inside the Darknet Markets that Fuel Financial Cybercrime*, BIOCATCH BLOG (Dec. 5, 2018) [https://web.archive.org/web/20210905231044/https://www.biocatch.com/blog/financial-cybercrime-darknet-markets].

[24] John Egan, *What Should I Do If My Driver's License Number Is Stolen?*, EXPERIAN (June 13, 2024), https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/.

> why these numbers are very much sought after by cyber criminals: ". . . 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. . . . bad actors may be using these driver's license numbers to fraudulently apply for unemployment benefits in someone else's name, a scam proving especially lucrative for hackers as unemployment numbers continue to soar. . . . In other cases, a scam using these driver's license numbers could look like an email that impersonates the DMV, requesting the person verify their driver's license number, car registration or insurance information, and then inserting a malicious link or attachment into the email."[25]

76. Further, an article on TechCrunch explains that it is driver's license or non-driver's identification numbers themselves that are the critical missing link for a fraudulent unemployment benefits application:

> Many financially driven criminals target government agencies using stolen identities or data. But many U.S. states require a government ID — like a driver's license — to file for unemployment benefits. To get a driver's license number, fraudsters take public or previously breached data and exploit weaknesses in auto insurance websites to obtain a customer's driver's license number. That allows the fraudsters to obtain unemployment benefits in another person's name.[26]

77. The use of stolen DLNs to obtain unemployment benefits under another person's name was confirmed by the New York State DFS on February 16, 2021, in its industry letter described above, which stated that they had "recently learned of a systemic and aggressive campaign to exploit cybersecurity flaws in public-facing websites to steal [PI, including from] websites that provide an instant quote … [and that] DFS has confirmed that, at least in some cases,

---

[25] Scott Ikeda, *Geico Data Breach Leaks Driver's License Numbers, Advises Customers to Watch Out for Fraudulent Unemployment Claims*, CPO MAGAZINE (Apr. 23, 2021), https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/.

[26] Zach Whittaker, *Geico admits fraudsters stole customers' driver's license numbers for months*, TECHCRUNCH (Apr. 19, 2021), https://techcrunch.com/2021/04/19/geico-driver-license-numbers-scraped/#:~:text=To%20get%20a%20driver's%20license,beneftheir%20in%20another%20person's%20name.

this stolen information has been used to submit fraudulent claims for pandemic and unemployment benefits."[27]

78. The process that was used by cybercriminals to extract the data from Defendants' website was likely automated. The identity thieves have demonstrated the value they place on DLNs by engaging in a systematic and business-like process for collecting them from Defendants' Data Disclosure and from additional insurers' websites offering instant quotes.

79. The United States Government Accountability Office noted in a June 2007 report on data breaches (the "GAO Report") that, when criminals use PI to open financial accounts, receive government benefits, and make purchases and secure credit in a victim's name, this type of identity fraud can be the most harmful because it may take some time for a victim to become aware of the fraud, and can adversely impact the victim's credit rating in the meantime.[28] The GAO Report also states that identity theft victims will face "substantial costs and inconveniences repairing damage to their credit records . . . [and their] good name."[29]

F. Defendants failed to comply with Federal Trade Commission requirements.

80. Federal and state governments established security standards and issued recommendations to minimize unauthorized data disclosures, and knowing disclosures of information via public websites, and the resulting harm to individuals and financial institutions. The Federal Trade Commission (FTC) has promulgated numerous guides for businesses

[27] N.Y. DEP'T OF FIN. SERV., *supra* note 12.

[28] *See* U. S. GOV'T ACCOUNTABILITY OFF., GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), http://www.gao.gov/assets/270/262899.pdf.

[29] *Id.*

highlighting 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.[30]

81. In 2016, the FTC updated their publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[31] Among other things, the guidelines note businesses should properly dispose of PI that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[32]

82. Also, the FTC recommends that companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify third-party service providers have implemented reasonable security measures.[33]

83. Highlighting the importance of protecting against these types of disclosures, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect PI, treating the failure to employ reasonable and appropriate measures to protect against

---

[30] FED. TRADE COMM'N, *Start With Security: A Guide for Business* (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[31] *See* FED. TRADE COMM'N, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

[32] *Id.*

[33] FED. TRADE COMM'N, *Start With Security, supra* note 30.

unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their Data security obligations.[34]

84. Through the intentional design and implementation of their online Quote Platform, and failure to secure Plaintiffs' and Class Members' PI, Defendants knowingly allowed the public—and thieves—to utilize their online Quote Platform to obtain access to and collect individuals' PI.

85. Defendants failed to employ reasonable and appropriate measures to protect against unauthorized disclosure and access to Plaintiffs' and Class Members' PI. Defendants' data security policies and practices constitute unfair acts or practices prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45, and violate the Gramm-Leach-Bliley Act ("GLB Act"), 15 U.S.C. § 6801.

G. Lemonade falsely assured Plaintiffs, Class Members, and the public that their information would be private and their DLNs would not be disclosed.

86. Defendants advertise that Lemonade is "America's top-rated insurance company," protecting "your family and your belongings—at home, and everywhere else."

87. On its publicly available car insurance page, Defendants pose the hypothetical question, "Can I trust you guys?" In response, they assure the public: "Of course. Unlike most of the new insurance startups out there, Lemonade is an insurance carrier, reinsured by some of the most trusted names in the industry . . . .[35]"

---

[34] *See* FED. TRADE COMM'N, *Privacy and Security Enforcement: Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (follow "Press Releases" link).

[35] LEMONADE, https://www.lemonade.com/car (last visited Aug. 28, 2025) [https://web.archive.org/web/20240303120756/https://www.lemonade.com/car (March 3, 2024)].

88. On its "FAQs" page, Defendants claim they were "built to provide the best, most delightful, and most transparent insurance experience in the world."[36]

89. Their FAQs say: "we care about the community and environment, and not just business results."

90. In addition, their FAQs pose the question: "How do you keep my information private?" In response, they claim: "We highly value and respect your privacy (see our Privacy Policy). We will never sell your information, or share it with anyone except for the purposes of providing our services and promoting our business."

91. Their FAQs also make further promises of confidentiality, claiming to be "obsessed" with privacy:

> Is my information kept confidential?
>
> We're obsessed with our customers' privacy (see our Privacy Pledge). We will never sell your information to any third party. Note that, in order to provide our service, we may need to transfer information to our partners and providers, solely for the purposes of regulatory and financial audits; running our service and resolving an incident; or obtaining a term life policy and settling claim benefits.

92. Defendants further explain that they are a "B Corp," "a certification granted to for-profit companies that meet rigorous standards of social and environmental performance, accountability, and transparency."

[36] LEMONADE, *FAQS,* https://www.lemonade.com/faq (last visited Aug. 28, 2025) [https://web.archive.org/web/20231203183514/https://www.lemonade.com/faq (Dec. 3, 2023)].

93. Defendants do not just have a privacy policy—they make a public-facing "Data Privacy Pledge," and they did so throughout the duration of the Data Disclosure.[37]

94. In those Pledges, Defendants publicly promised transparency, privacy, and security; safekeeping and nondisclosure of DLNs; and that DLNs were only used in limited circumstances.

95. For example, the Pledges promise: "No matter what we change, we will always maintain our commitment to protecting your privacy. . . ."

96. The June 2023, April 2024, and June 2024 Pledges, for example, like other Lemonade Pledges, assure the public of Lemonade's commitment to privacy:

> Lemonade's Data Privacy Pledge
>
> TL;DR: We will never, ever, sell your data to anyone.
>
> In light of growing concerns about companies selling customers' private data, we thought this would be a good opportunity to tell you about what types of data we collect, why we collect it, and what we do with it.

97. The June 2023 and April 2024 Pledges, for example, said that DLNs were only "collected and required to provide our services" for "car users" and "rarely during claims," and that they "may send it to one of our service providers" for "authentication" or "claim support." They promised it would "never" be sold to a third party.

---

[37] *E.g.,* LEMONADE, *Data Privacy Pledge*, https://www.lemonade.com/privacy-policy (effective July 19, 2025) (last visited Aug. 28, 2025) ("July 2025 Pledge")

[https://web.archive.org/web/20250206231706/https://www.lemonade.com/privacy-policy (effective June 27, 2024) (last visited Aug. 28, 2025) ("June 2024 Pledge")];

[https://web.archive.org/web/20240601034441/https://www.lemonade.com/privacy-policy (effective April 2, 2024) (last visited Aug. 28, 2025) ("April 2024 Pledge")];

[https://web.archive.org/web/20230402113801/https://www.lemonade.com/privacy-policy (effective March 28, 2023) (last visited Aug. 28, 2025) ("March 2024 Pledge"]; and

[https://web.archive.org/web/20231011154334/https://www.lemonade.com/privacy-policy (effective June 30, 2023) (last visited Aug. 28, 2025) ("June 2023 Pledge")].

98. In the July 2025 Pledge, Defendants claim they only disclose "Driver's License Details" for "Car and Life Insurance policies and claim handling" and with "Authentication providers and claims service providers."

99. According to the June 2023, April 2024, and July 2025 Pledges, for example, Defendants collect certain information for "Obtaining insurance quotes." They acknowledge that DLNs are not always required to generate quotes. And they make no disclosure that DLNs can be obtained by the public or are being used for prefill or other marketing and sales purposes.

100. In fact, the July 2025 Pledge claims that Defendants only disclosed "name" and "date of birth" to third-party "vendors" acting as "claim service providers and advertisers."

101. Similarly, the June 2023 Pledge claims names may be sent to "claim support service providers." (It also states that Lemonade would "never" sell such data to a third party, though it suggests that it is provided to advertising and social networks).

102. The July 2025 Pledge further claims that "Postal address" is only disclosed to third-party "vendors" acting as "Claim service providers, insurance background check providers, identification and authentication service providers, and advertisers." *See also, e.g.,* June 2023 Pledge (similar).

103. Defendants' Pledges claim to undertake certain steps with the goal of "Fighting fraud" and "detect[ing] potential fraud attempts," but failed to disclose they had inadequate security systems to allow it to do so.

104. Likewise, the Pledges claim Defendants may use data for security purposes but fail to disclose that Defendants were not taking adequate steps to protect consumer data—let alone that they were voluntarily disclosing it:

> [W]e use data in the following ways: . . . To detect and protect against malicious, deceptive, fraudulent, or illegal activity, including violation of our policies and terms and conditions, security incidents, and harm to the rights, property, or safety of our company and our users, employees, or others.

105. Lemonade also claims in their Pledges to protect consumer data and that it will notify consumers of a data breach:

> In the unlikely event of a data breach, which results in your personal information being compromised, we will make sure to notify you via email, regular mail, or phone, as required by law.
>
> We retain your personal information for only as long as necessary to fulfill the purposes outlined in this Privacy Pledge. . . .
>
> We use security measures that comply with applicable laws in order to protect your personal information from unauthorized access and use. These measures include modern cloud security standards, as well as computer safeguards, secured files, and buildings. In addition, we restrict access to personal customer data to those who need it to provide insurance services or to conduct our normal business operations.

July 2025 Pledge. *See also, e.g.,* June 2023 Pledge (similar).

106. Defendants' Pledges unfairly and deceptively misled Plaintiffs, Class Members, and the public in numerous ways. Not only did they fail to disclose that they made DLNs publicly available, but Defendants further omitted that they were obtaining DLNs from a third party and using the DLNs for marketing and sales purposes; i.e., for prefill, and that they were disclosing other PI (like name, date of birth, and address) to third-party vendors for these undisclosed purposes. They also misrepresented their commitment to privacy, data security, fraud detection, and timely notification of any data breach.

H. Plaintiffs and Class Members were injured by the Data Disclosure.

107. Defendants admitted in the Notices that they disclosed Plaintiffs' and Class Members' DLNs to unauthorized third parties. Defendants tasked Plaintiffs and Class Members with various mitigation steps, and offered a year of credit monitoring. These measures are woefully inadequate and do not absolve Defendants of their violations of the DPPA and other laws alleged herein.

108. Plaintiffs and Class Members have been, and will continue to be, injured because Defendants disclosed their PI, and—per Defendants' instructions— they are now forced to spend time monitoring their credit and governmental communications guarding against identity theft, and resolving fraudulent claims and charges because of Defendants' actions and/or inactions.

I. Plaintiffs and Class Members suffered damages as a result of the Data Disclosure.

109. The ramifications of Defendants' disclosure and failure to keep individuals' PI secure are long lasting and severe. Once PI is disseminated to unauthorized parties, fraudulent use of that information and damage to victims may continue for years.[38]

110. Plaintiffs' and Class Members' DLNs are private, valuable, and sensitive in nature as they can be used to commit an array of harms and fraud in the hands of the wrong people.

111. Defendants did not obtain Plaintiffs' and Class Members' consent to obtain or use their DLNs, or to disclose their DLNs to any other person, as required by applicable law and industry standards.

112. Plaintiffs and Class Members are at risk for actual identity theft in addition to all other forms of fraud.

---

[38] LEXISNEXIS RISK SOLUTIONS, *True Cost of Fraud Studies*, https://risk.lexisnexis.com/insights-resources/research/us-ca-true-cost-of-fraud-study (last visited Aug. 28, 2025).

113. Defendants' decision to enable anyone, especially thieves with various pieces of individuals' PI, to obtain any Plaintiff's or Class Member's DLN by utilizing Defendants' Quote Platform, left Plaintiffs and Class Members with no ability to protect their sensitive and private PI.

114. Defendants had the resources necessary to prevent their Data Disclosure, but did not implement data security measures, despite their obligations to protect Plaintiffs' and Class Members' PI from unauthorized disclosure.

115. Defendants failed to take reasonable steps to adequately secure Defendants' website and publish it in a manner that did not hand over Plaintiffs' and Class Members' DLNs to unauthorized third parties, leaving Defendants' customers and other consumers, including Plaintiffs and Class Members, exposed to risk of fraud and identity theft.

116. Defendants were, and at all relevant times have been, aware that the PI they obtain, use, handle, and store in connection with their services is highly sensitive. Because Defendants are companies that provide insurance services involving highly sensitive and identifying information, Defendants were aware of the importance of safeguarding that information and protecting their websites, systems, and products from security vulnerabilities.

117. Defendants were aware, or should have been aware, of regulatory and industry guidance regarding data security, and they were alerted to the risk associated with knowingly providing DLNs to members of the public on Defendants' website.

118. Defendants knowingly obtained, used, disclosed, and compromised Plaintiffs' and Class Members' PI by prefilling DLNs on their Quote Platform without ever verifying users' identities, and voluntarily transmitting DLNs to any member of the public, including fraudulent actors.

119. Defendants failed to take reasonable steps against an obvious threat. Defendants designed and implemented their own website Quote Platform, which included the instant quote feature that auto-populated Plaintiffs' and Class Members' DLNs in response to the input of basic publicly available consumer information. Defendants knowingly and intentionally included the quote feature on their website. Had Defendants not prefilled DLNs, publicly disclosed them, or failed to verify user identities, they could have prevented the disclosure, unauthorized access, and, ultimately, the prospective fraudulent use and possible fraudulent use of consumers' PI.

120. As a direct and proximate result of Defendants' actions and inactions, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands, such as work and family, in an effort to mitigate the actual and potential impact of Defendants' Data Disclosure on their lives.

121. The U.S. 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" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[39]

122. As a result of Defendants' Data Disclosure, Plaintiffs and Class Members have suffered, will suffer, and are at imminent risk of suffering:

a. the compromise, publication, fraudulent, and/or unauthorized use of their PI;

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

[39] Erika Harrell and Lynn Langton, *Victims of Identity Theft, 2012*, NCJ 243779, U.S. DEP'T OF JUSTICE, OFF. OF JUSTICE PROGRAMS, BUREAU OF JUSTICE STATISTICS (Dec. 2013), https://bjs.ojp.gov/content/pub/pdf/vit12.pdf.

c. lost opportunity costs and wages and loss of productivity associated with efforts expended from addressing and attempting to mitigate the actual and future consequences of Defendants' Data Disclosure, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

d. the continued risk to their PI, which remains in the possession of Defendants and is subject to further compromise so long as Defendants fail to undertake appropriate measures to protect the PI in their possession; and

e. current and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, remediate, and repair the impact of Defendants' Data Disclosure for the remainder of the lives of Plaintiffs and Class Members.

123. In addition to a remedy for the economic harm, Plaintiffs and Class Members maintain an undeniable interest in ensuring that their PI is secure, remains secure, and is not subject to further disclosure, misappropriation, and theft.

124. To date, other than providing 12 months of credit monitoring and identity protection services, Defendants do not appear to be taking any additional measures to assist Plaintiffs and Class Members, other than simply telling them to "remain vigilant with respect to reviewing your account statements and credit reports." This recommendation, however, does not require Defendants to expend any effort to protect Plaintiffs' and Class Members' PI, instead shifting that burden to Plaintiffs and the Class. Moreover, Defendants fail to provide monetary compensation and provide no protection whatsoever after 12 months.

125. Defendants' disclosure of Plaintiffs' and Class Members' DLNs directly to members of the public has resulted in Plaintiffs and Class Members having to undertake these tasks, which requires extensive time, calls, and, for many of the credit and fraud protection services, payment of money. Indeed, as Defendants' Notice indicates, they are explicitly *instructing*—and putting the burden on—Plaintiffs and Class Members to monitor and discover possible fraudulent activity and identity theft.

126. Defendants' offer of 12 months of identity monitoring and identity protection services to Plaintiffs and Class Members is woefully inadequate. While some harm has manifested already, the worst may be yet to come.

127. Identity theft victims are frequently required to spend many hours and large amounts of money repairing the impact to their credit. Identity thieves use stolen PI for a variety of crimes, including credit card fraud, tax fraud, phone or utilities fraud, and bank/finance fraud.

128. There may be a time lag between when additional harm occurs versus when it is discovered, and also between when PI is acquired and when it is used. 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.[40]

129. As a result of the events detailed herein, Plaintiffs and Class Members suffered harm and loss of privacy, and will continue to suffer future harm, because of Defendants' Data Disclosure and the fact that their DLNs are now in the hands of criminals, including, but not limited to: loss of privacy; loss of control over PI and identities; fraud and identity theft; unreimbursed

[40] *See* GAO-07-737, *supra* note 28, at 29 (emphasis added).

losses relating to fraud and identity theft; loss of value and loss of possession and privacy of PI; harm resulting from damaged credit scores and credit information; a substantially increased risk of future identity theft and fraud; loss of time and money preparing for and resolving fraud and identity theft; loss of time and money obtaining protections against future identity theft; and other harm resulting from the unauthorized use or threat of unauthorized disclosure of PI.

J. Plaintiff Klein was injured and experienced damages.

130. Prior to April 2025, Plaintiff Klein was a homeowner's insurance customer of Lemonade for over five years.

131. Lemonade sent Klein a letter in or about April 2025, informing Klein that Lemonade disclosed his DLN to unauthorized third parties through Lemonade's Quote Platform.

132. Klein has spent considerable time and effort and taken (and continues to take) considerable precautions to monitor for and protect against the unauthorized dissemination of his DLN and PI. To date, Klein has spent hours researching the breach, freezing credit through Experian and Equifax, monitoring financial accounts, sorting through significant spam, and otherwise dealing with the fallout of the Data Disclosure. Unfortunately, because of Defendants' practice of unlawfully obtaining, using, and disclosing his PI, Klein's sensitive PI was disseminated without his consent, is at high risk of being fraudulently used by unauthorized third parties, and the value of that information was quantifiably reduced.

133. Klein is very careful about sharing PI and has never knowingly transmitted unencrypted PI over the internet or any other unsecured source. Further, Klein stores documents containing PI in a secure location and takes steps to ensure all online accounts are secure and password protected.

134. As a result of Defendants' Data Disclosure, Klein has suffered—or is at an increased risk of suffering—injury and/or damages, including, but not limited to, the unauthorized

use of the disclosed PI, heightened threat of identity theft and general mitigation efforts spent on monitoring credit and for identity theft; time and expenses spent scrutinizing bank statements, credit card statements, and credit reports for fraudulent transactions/conduct; time and expenses spent monitoring bank accounts for fraudulent activity; loss in value of personal data; lost property in the form of the compromised PI; and injury to Plaintiff's privacy.

135. Additionally, because of Defendants' Data Disclosure, Klein now faces a substantial risk that unauthorized third parties will further misuse his PI. Indeed, (1) the Data Disclosure involved unauthorized third parties specifically targeting Defendants' systems (i.e., the online Quote Platform); (2) the dataset of PI the unauthorized third parties obtained from Defendants' disclosure through their Quote Platform is likely to be misused for fraudulent and/or unauthorized conduct; and (3) the type of PI Defendants disclosed and that unauthorized third parties obtained in the Data Disclosure—i.e., mainly DLNs—are highly sensitive and can be misused for substantially injurious forms of identity and/or fraud, such as (*inter alia*) fraudulently applying for and obtaining unemployment benefits or loans and opening bank accounts. As a result, Klein has (1) suffered, or is at an increased risk of suffering, unauthorized use of his disclosed PI such that Klein has suffered concrete injury; (2) suffered concrete injury in fact based on the material risk of future misuse of Klein's PI and concrete harm by exposure to this risk; and (3) experienced separate concrete, present harm caused by Plaintiff's exposure to the risk of future harm due to lost time Klein spent taking protective measures that would have otherwise been put to other productive use and lost opportunity costs associated with the time and effort Plaintiff expended addressing future consequences of the Data Disclosure.

136. Klein experienced all the foregoing harm and injury as a direct result of Defendants' knowing and voluntary disclosure of his PI in the Data Disclosure. The monetary relief sought

herein by Klein would compensate for the foregoing redressable injuries. Further, Klein seeks injunctive relief to redress the foregoing injuries and harm, including, but not limited to, requiring Defendants to take steps to monitor for, protect, and/or prevent misuse of the PI that Defendants disclosed in the Data Disclosure, as well as enact adequate data privacy/security practices.

K. Plaintiff Rich was injured and experienced damages.

137. Plaintiff Rich does not currently (and has never had) any insurance policies with Lemonade, nor has he ever applied for insurance—or engaged in other business—with Lemonade.

138. Nevertheless, Lemonade sent Rich a letter dated April 10, 2025, informing him that Lemonade disclosed his DLN to unauthorized third parties through Lemonade's Quote Platform. The letter stated as follows:

> Through certain of their subsidiaries, Lemonade offers car insurance policies through an online application process at www.lemonade.com/car (the "Online Flow"). Using the Online Flow to obtain an insurance quote and purchase a policy, an individual enters certain information—name, date of birth, and residential address. Using this information, Lemonade calls for and returns from their third-party vendor that individual's driver's license number. On March 14, 2025, we learned that due to a vulnerability in our Online Flow, certain driver's license numbers for identifiable individuals were likely exposed. Lemonade believes that the unauthorized exposures spanned from approximately April 2023 through September 2024. . . . Based on our investigation, your driver's license number may have been accessed without authorization.

139. In October and November 2024, Rich learned that cybercriminals fraudulently applied for multiple auto loans, on multiple occasions, with multiple lenders, all in his name.

140. Specifically, Ally Bank sent Rich a letter dated October 24, 2024, informing him that an application for an auto loan with CarMax was made in his name, but it was denied. Plaintiff Rich contacted CarMax on or about November 5, 2024, and was informed that they would investigate the matter, but he never heard anything further from Ally Bank or CarMax.

141. Further, Rich received seven separate letters from Capital One, dated October 18 and 25, 2024 and November 7, 2024, each of which stated that an auto loan application had been submitted in his name. All seven letters contained separate reference numbers, indicating that cybercriminals made seven separate applications for auto loans in his name—four of which were made on the same day. Plaintiff Rich contacted Capital One on or about October 28, 2024, to report the fraud, and Capital One informed him that it would investigate the situation, but Plaintiff Rich never heard anything further from Capital One.

142. Global Lending Services sent Plaintiff Rich two separate letters dated November 4 and 12, 2024, informing him that two separate applications for auto loans were made in his name, but both applications were declined. Plaintiff Rich had never applied for either of those auto loans or otherwise heard of Global Lending Services. On November 13, 2024, Rich contacted Global Lending Services to inform the company that the loan applications made in his name were fraudulent. Global Lending Services instructed Plaintiff Rich to contact Capital One, which is the lender that declined the auto loan applications (Global Lending Services is a third-party intermediary that matches loan applicants with lenders). Plaintiff Rich then contacted Capital One to dispute the loan applications.

143. On or about December 12, 2024, Rich experienced a fraudulent charge for Uber, in the amount of $9.99, on his Chase Freedom Visa credit card. Rich does not use Uber, so he contacted Chase to dispute the charge, which Chase promptly reversed. Chase also issued Plaintiff Rich a replacement credit card.

144. On or about November 6, 2024, Rich discovered that a series of fraudulent trades were made on his IRA account with Fidelity. Specifically, on November 7, 2024, unauthorized individuals sold Plaintiff Rich's investments in the S&P 500 Mutual Fund and used the proceeds

of the sale to make a series of trades in penny stocks. Rich was forced to take a day off from work on November 6, 2024, to investigate the fraud and contact Fidelity to report and troubleshoot it. Although Plaintiff Rich did not lose any wages as a result, he would have spent that paid day off on more valuable endeavors. On or about December 20, 2024, Fidelity reversed those trades.

145. The foregoing fraudulent misuse of Rich's sensitive information is temporally and logically connected to the data derived from Lemonade's Data Disclosure in the same way that data breach and other privacy cases have found to be "fairly traceable." Lemonade disclosed Plaintiff Rich's DLN shortly before he experienced this fraud.

146. Rich has spent and continues to spend considerable time and effort, and has taken and continues to take considerable precautions, to monitor for and protect against the unauthorized dissemination of his DLN. To date, he has spent approximately 20-30 hours monitoring accounts and otherwise dealing with the fallout of the Data Disclosure. Unfortunately, because of Lemonade's practice of unlawfully obtaining, using, and disclosing his DLN, Rich's sensitive information was disseminated without his consent, is at high risk of being fraudulently used by unauthorized third parties, and the value of that information was quantifiably reduced.

147. Rich is very careful about sharing his DLN and has never knowingly transmitted his DLN (or other sensitive information) unencrypted over the internet or any other unsecured source. Further, Rich stores documents containing his sensitive information (including his driver's license number) in a secure location and takes steps to ensure his online accounts are secure and password protected.

148. As a result of Lemonade's Data Disclosure, Rich has suffered—or is at an increased risk of suffering—injury and/or damages, including, but not limited to, the unauthorized use of his disclosed DLN, heightened threat of identity theft and general mitigation efforts spent on

monitoring his credit and for identity theft; time and expenses spent scrutinizing bank statements, credit card statements, and credit reports for fraudulent transactions/conduct; time and expenses spent monitoring bank accounts for fraudulent activity; loss in value of his personal data; lost property in the form of his compromised PI; and injury to his privacy.

149. Additionally, because of Lemonade's Data Disclosure, Rich now faces a substantial risk that unauthorized third parties will further misuse his DLN. Indeed, (1) the Data Disclosure involved unauthorized third parties specifically targeting Lemonade's systems (i.e., the online Quote Platform); (2) the dataset of DLNs the unauthorized third parties obtained from Lemonade's disclosure through their Quote Platform has already been actually misused for fraudulent and/or unauthorized conduct; and (3) the type of PI Defendants disclosed and that unauthorized third parties obtained in the Data Disclosure are highly sensitive and can be misused for substantially injurious forms of identity and/or fraud such as (*inter alia*) fraudulently applying for and obtaining unemployment benefits or loans and opening bank accounts. As a result, Rich has (1) suffered, or is at an increased risk of suffering, unauthorized use of his disclosed DLN such that he has suffered concrete injury; (2) suffered concrete injury in fact based on the material risk of future misuse of his DLN and concrete harm by exposure to this risk; and (3) experienced separate concrete, present harm caused by Plaintiff's exposure to the risk of future harm due to lost time Rich spent taking protective measures that would have otherwise been put to other productive use and lost opportunity costs associated with the time and effort Plaintiff expended addressing future consequences of the Data Disclosure.

150. Rich experienced all the foregoing harm and injury as a direct result of Lemonade's knowing and voluntary disclosure of his DLN in the Data Disclosure. The monetary relief sought herein by Rich would compensate him for the foregoing redressable injuries. Further, Rich seeks

injunctive relief to redress the foregoing injuries and harm, including, but not limited to, requiring Lemonade to take steps to monitor for, protect, and/or prevent misuse of his DLN that Lemonade disclosed in the Data Disclosure, as well as enact adequate data privacy/security practices.

L. Plaintiff Murray was injured and experienced damages.

151. Plaintiff Murray, a customer of Lemonade, provided his PI to Defendants—including his DLN—and, upon information and belief, that PI was stored and maintained by Defendants.

152. Lemonade sent Murray a letter dated April 10, 2025, informing him that Lemonade disclosed his DLN to unauthorized third parties through Lemonade's Quote Platform.

153. Murray is now forced to live with the anxiety that his PI is being disclosed to the entire world, thereby subjecting Plaintiff to embarrassment and depriving him of any right to privacy whatsoever.

154. Since the Data Disclosure, Murray has experienced a significant increase in the frequency of spam telephone calls and emails from individuals who have clearly obtained his PII.

155. Murray remains at a substantial and imminent risk of future harm given the highly sensitive nature of the information stolen. Murray faces a substantial risk of out-of-pocket fraud losses, such as loans opened in his name, medical services billed in his name, tax return fraud, utility bills opened in his name, credit card fraud, and similar identity theft.

156. The exposure of Murray's sensitive information is temporally and logically connected to the data derived from Lemonade's Data Disclosure in the same way that data breach and other privacy cases have found to be "fairly traceable." Lemonade disclosed Murray's DLN shortly before he experienced this fraud.

157. Murray has spent and continues to spend considerable time and effort, and has taken and continues to take considerable precautions, to monitor for and protect against the unauthorized

dissemination of his DLN. To date, Plaintiff has spent approximately five hours monitoring his accounts to detect suspicious and fraudulent activity, to mitigate against potential harm, verify whether incoming phone calls, text messages, and emails are legitimate or spam, and otherwise dealing with the fallout of the Data Disclosure. Unfortunately, because of Lemonade's practice of unlawfully obtaining, using, and disclosing his DLN, Murray's sensitive information was disseminated without his consent, is at high risk of being fraudulently used by unauthorized third parties, and the value of that information was quantifiably reduced.

158. Murray is very careful about sharing his DLN and has never knowingly transmitted his DLN (or other sensitive information) unencrypted over the internet or any other unsecured source. Further, Murray stores documents containing his sensitive information (including his DLN) in a secure location and takes steps to ensure his online accounts are secure and password protected.

159. As a result of Lemonade's Data Disclosure, Murray has suffered—or is at an increased risk of suffering—injury and/or damages, including, but not limited to, the unauthorized use of his disclosed DLN, heightened threat of identity theft and general mitigation efforts spent on monitoring his credit and for identity theft; time and expenses spent scrutinizing bank statements, credit card statements, and credit reports for fraudulent transactions/conduct; time and expenses spent monitoring bank accounts for fraudulent activity; loss in value of his personal data; lost property in the form of his compromised PI; and injury to his privacy.

160. Additionally, because of Lemonade's Data Disclosure, Murray now faces a substantial risk that unauthorized third parties will further misuse his DLN. Indeed, (1) the Data Disclosure involved unauthorized third parties specifically targeting Lemonade's systems (i.e., the online Quote Platform); (2) the dataset of DLNs the unauthorized third parties obtained from

Lemonade's disclosure through their Quote Platform has already been actually misused for fraudulent and/or unauthorized conduct; and (3) the DLNs Lemonade disclosed and that unauthorized third parties obtained in the Data Disclosure are highly sensitive and can be misused for substantially injurious forms of identity and/or fraud such as (*inter alia*) fraudulently applying for and obtaining unemployment benefits or loans and opening bank accounts. As a result, Murray (1) is at an increased risk of suffering, unauthorized use of his disclosed DLN such that he has suffered concrete injury; (2) suffered concrete injury in fact based on the material risk of future misuse of his DLN and concrete harm by exposure to this risk; and (3) experienced separate concrete, present harm caused by his exposure to the risk of future harm because he lost time he spent taking protective measures that would have otherwise been put to other productive use and lost opportunity costs associated with the time and effort he expended addressing future consequences of the Data Disclosure.

161. Murray experienced all the foregoing harm and injury as a direct result of Lemonade's knowing and voluntary disclosure of his DLN in the Data Disclosure. The monetary relief sought herein by Murray would compensate him for the foregoing redressable injuries. Further, Murray seeks injunctive relief to redress the foregoing injuries and harm, including, but not limited to, requiring Lemonade to take steps to monitor for, protect, and/or prevent misuse of his DLN that Lemonade disclosed in the Data Disclosure, as well as enact adequate data privacy/security practices.

V. CLASS ALLEGATIONS

162. Plaintiffs bring this action on behalf of themselves and the following class and subclasses[41] (collectively, the "Class") pursuant to Federal Rule of Civil Procedure 23(a) and (b):

> **Nationwide Class**:
> All residents of the United States whose driver's license numbers were obtained, used, and/or disclosed by Defendants through their Quote Platform or otherwise displayed on their website, including, but not limited to, during the Data Disclosure.
>
> **Arizona Class**:
> All residents of Arizona whose driver's license numbers were obtained, used, and/or disclosed by Defendants through their Quote Platform or otherwise displayed on their website, including, but not limited to, during the Data Disclosure.
>
> **Connecticut Class**:
> All residents of Connecticut whose driver's license numbers were obtained, used, and/or disclosed by Defendants through their Quote Platform or otherwise displayed on their website, including, but not limited to, during the Data Disclosure.
>
> **New York Class**:
> All residents of New York whose driver's license numbers were obtained, used, and/or disclosed by Defendants through their Quote Platform or otherwise displayed on their website, including, but not limited to, during the Data Disclosure.

163. Plaintiffs reserve the right to re-define the Class prior to class certification. Plaintiffs further reserve the right to modify these class definitions as discovery in this action progresses.

164. Excluded from the Class are Defendants and their affiliates, officers, directors, assigns, successors, and the judges assigned to this case.

165. **Numerosity**: While the precise number of Class Members has not yet been determined, Defendants' filing with the United States Securities and Exchange Commission states

[41] The Arizona, Connecticut, and New York classes are referred to collectively herein as the "State Classes."

that the Data Disclosure impacted "approximately 190,000 individuals"[42]; therefore, members of the Class are so numerous that their individual joinder is impracticable, as the proposed Class appears to include at least hundreds of thousands of members who are geographically dispersed.

166. **Typicality**: Plaintiffs' claims are typical of Class Members' claims. Plaintiffs and all Class Members were injured through Defendants' uniform misconduct, and Plaintiffs' claims are identical to the claims of the Class Members they seek to represent. Accordingly, Plaintiffs' claims are typical of Class Members' claims.

167. **Adequacy**: Plaintiffs are adequate representatives of the Class because their interests are aligned with the Class they seek to represent, and they have no conflicts of interest with the Class. Plaintiffs' Counsel are competent with significant experience prosecuting complex class action cases, including cases involving alleged privacy and data security violations. Plaintiffs and Plaintiffs' counsel intend to prosecute this action vigorously. The Class's interests are well-represented by Plaintiffs and Plaintiffs' counsel.

168. **Superiority**: A class action is the superior—and only realistic—mechanism to fairly and efficiently adjudicate Plaintiffs' and other Class Members' claims. The injury suffered by each individual Class Member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for Class Members individually to effectively redress Defendants' wrongdoing. Even if Class Members could afford such individual litigation, the court system could not. Individualized litigation also presents a potential for inconsistent or contradictory judgments. Individualized litigation further increases the delay and expense to all parties, and to the court system, presented

[42] LEMONADE, INC., Current Report (Form 8-K) (SEC filed Apr. 4, 2025), https://d18rn0p25nwr6d.cloudfront.net/CIK-0001691421/bd19d2fb-41d1-4e83-a381-c246044d769b.pdf.

by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

169. **Commonality and Predominance**: The following questions common to all Class Members predominate over any potential questions affecting individual Class Members:

a. whether Defendants engaged in the wrongful conduct alleged herein;

b. whether Defendants knowingly used Plaintiffs' and the Class Members' DLNs to promote and sell auto insurance;

c. whether Defendants knowingly obtained Plaintiffs' and the Class Members' DLNs;

d. whether Defendants knowingly disclosed Plaintiffs' and the Class Members' DLNs;

e. whether Defendants violated the DPPA;

f. whether Defendants violated the New York General Business Act;

g. whether Defendants violated the Connecticut Unfair Trade Practices Act;

h. whether Defendants' data security practices and the vulnerabilities of Defendants' systems resulted in the disclosure of Plaintiffs' and other Class Members' sensitive information;

i. whether Defendants violated Plaintiffs' and the Class Members' privacy rights;

j. whether Defendants were negligent when they disclosed the sensitive information of Plaintiffs and other Class Members; and

k. whether Plaintiffs and Class Members are entitled to damages, equitable relief, or other relief and, if so, in what amount.

170. Given that Defendants engaged in a common course of conduct as to Plaintiffs and the Class, similar or identical injuries and common law and statutory violations are involved, and common questions outweigh any potential individual questions.

VI. CAUSES OF ACTION

COUNT I
Violation of the Driver's Privacy Protection Act, 18 U.S.C. §§ 2724, *et seq.*
(On Behalf of Plaintiffs and the Nationwide Class Against Defendants)

171. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

172. Plaintiffs bring this claim individually and on behalf of the Nationwide Class.

173. The DPPA provides that "[a] person who knowingly obtains, discloses or uses personal information, from a motor vehicle record, for a purpose not permitted under this chapter shall be liable to the individual to whom the information pertains. . . ." 18 U.S.C. § 2724.

174. The DPPA also restricts the resale and re-disclosure of personal information, and requires authorized recipients to maintain records of each individual and the permitted purpose of the disclosure for a period of five years. 18 U.S.C. § 2721(c).

175. Under the DPPA, a "'motor vehicle record' means 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). Driver's license numbers are motor vehicle records and "personal information" under the DPPA. 18 U.S.C. § 2725(3).

176. Defendants obtain, use, and disclose motor vehicle records from their customers.

177. Defendants also obtain motor vehicle records directly from state agencies or through resellers (third-party prefill services) that sell such records.

178. Defendants knowingly used the above-described information to sell auto insurance on their free online Quote Platform, accessible from www.lemonade.com.

179. Defendants knowingly published the above-described information to the public on their free online Quote Platform, accessible from www.lemonade.com.

180. Defendants knowingly linked their public website to systems and/or networks storing, maintaining, and/or obtaining Plaintiffs' and Class Members' PI.

181. Defendants had a practice of offering online insurance quotes to applicants long before they incorporated this auto-population feature but added the auto-population feature to their online Quote Platform to gain competitive advantage in their sales process. By adding the auto-population feature to their online Quote Platform, which Defendants knowingly chose to do, Defendants knew that they were using the driver's license information to sell insurance and make the displayed information easily accessible to anyone who entered basic information into their system. Defendants did not impose any security protocols to ensure that website visitors entered and accessed PI only about themselves. Defendants did not impose effective security protocols to prevent automated bots from accessing consumers' PI.

182. During the time period starting, at the latest, in April 2023 through September 2024, the PI, including DLNs, of Plaintiffs and Class Members was publicly available and viewable, unencrypted, on Defendants' Quote Platform, and Defendants knowingly obtained, used, and disclosed and/or redisclosed Plaintiffs' and Class Members' motor vehicle records and PI to the general public, which is not an authorized use permitted by the DPPA pursuant to 18 U.S.C. §§ 2724, 2721(b), and 2721(c).

183. Pursuant to the allegations herein, Defendants knew or should have known that they obtained, disclosed or redisclosed, and used PI from a motor vehicle record for a purpose not permitted under the DPPA.

184. By engaging in the conduct described above, Defendants knowingly obtained personal information for a purpose not permitted under the DPPA.

185. By engaging in the conduct described above, Defendants knowingly used personal information for a purpose not permitted under the DPPA.

186. By engaging in the conduct described above, Defendants knowingly disclosed or redisclosed personal information for a purpose not permitted under the DPPA.

187. As a result of Defendants' acquisition, use, subsequent Data Disclosure, and violations of the DPPA, Plaintiffs and putative Class Members are entitled to statutory damages to maximum allowable, actual damages, liquidated damages, and attorneys' fees and costs.

COUNT II
Negligence
(On Behalf of Plaintiffs and the Nationwide Class or, in the Alternative, the State Classes)

188. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

189. Plaintiffs bring this claim individually and on behalf of the Nationwide Class or, in the alternative, the State Classes.

190. Defendants owed a duty to Plaintiffs and the Class Members to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiffs' and Class Members' PI from being compromised, lost, stolen, and accessed by unauthorized persons. This duty includes, among other things, designing, implementing, maintaining, and testing their Data

security systems to ensure Plaintiffs' and Class Members' PI in Defendants' possession, or that could be accessed by Defendants, was adequately secured and protected.

191. Defendants owed a duty to Plaintiffs and the Class Members to adopt, implement, and maintain a process by which they could detect vulnerabilities in their websites and systems in a reasonably expeditious period of time and to give prompt notice in the case of a data security incident, including any unauthorized use of data knowingly disclosed on Defendants' website.

192. Defendants owed a duty of care to Plaintiffs and Class Members to provide security, consistent with industry standards, to ensure that their systems and networks—and the personnel responsible for them—adequately protected the PI they stored, maintained, used, accessed, and/or obtained.

193. Defendants further assumed the duty to implement reasonable security measures as a result of their general conduct, internal policies, and procedures, in which Defendants state, among other things, that Defendants have a "commitment to protecting your privacy."[43] Through these and other statements, Defendants specifically assumed the duty to comply with industry standards in protecting their customers' and other consumers' PI; and to adopt, implement, and maintain internal standards of data security that met those industry standards.

194. Defendants owed a duty by, on information and belief, entering into agreements with various state DMVs, which required them to certify that they will not use motor vehicle records in manners inconsistent with the DPPA and will secure the information appropriately.

195. Unbeknownst to Plaintiffs and Class Members, they were entrusting Defendants with their PI when Defendants obtained their PI from motor vehicle records directly from state agencies or through resellers or third-party prefill services that sell such records. Defendants had

[43] LEMONADE, *Privacy Pledge*, *supra* note 37.

an obligation to safeguard Plaintiffs' and Class Members' PI and were able to protect against the harm suffered by Plaintiffs and Class Members. Instead, Defendants chose to disclose Plaintiffs' and Class Members' DLNs so they could sell more auto insurance.

196. Defendants owed a duty of care to Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices. Defendants knew or should have known of the inherent risks in having their systems auto-populate online quote requests with private PI, without the consent or authorization of the person whose PI was being provided. Only Defendants were in a position to ensure that their systems were sufficient to protect against harm to Plaintiffs and the Class resulting from a data security incident; instead, Defendants chose to disclose Plaintiffs' and Class Members' DLNs so they could sell more auto insurance.

197. Defendants' own conduct also created a foreseeable risk of harm to Plaintiffs and Class Members and their PI. Defendants' misconduct included failing to adopt, implement, and maintain the systems, policies, and procedures necessary to prevent disclosure of PI.

198. Defendants acknowledged their conduct created actual harm to Plaintiffs and Class Members because Defendants instructed them to monitor their accounts for fraudulent conduct and identity theft, and offered one year of credit monitoring.

199. Defendants knew, or should have known, of the risks inherent in disclosing, collecting, storing, accessing, and transmitting PI, and the importance of adequate security. Defendants knew about—or should have been aware of—numerous, well-publicized unauthorized data disclosures affecting businesses, especially insurance and financial businesses, in the United States.

200. Because Defendants knew that their disclosure of sensitive PI would damage thousands of individuals, including Plaintiffs and Class Members, Defendants had a duty to adequately protect their data systems and the PI contained and/or accessible therein.

201. Defendants breached their duties to Plaintiffs and Class Members, and thus were negligent, by designing the Quote Platform and website so that it automatically provided Plaintiffs' and Class Members' driver's license information directly to members of the public, failing to recognize in a timely manner that Plaintiffs' and Class Members' PI had been disclosed, and failing to warn Plaintiffs and Class Members in a timely manner that their PI had been disclosed.

202. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

203. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known they were failing to meet their duties, and the Defendants' breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the disclosure of their PI.

204. Neither Plaintiffs nor the other Class Members contributed to Defendants' Data Disclosure.

205. As a direct and proximate cause of Defendants' conduct, Plaintiffs and Class Members have suffered and/or will suffer injury and damages, including, but not limited to: (i) the loss of the opportunity to determine for themselves how their PI is used; (ii) the publication and/or fraudulent use of their PI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PI; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of Defendants' Data Disclosure, including, but not limited to, efforts spent

researching how to prevent, detect, contest, and recover from unemployment and/or tax fraud and identity theft; (v) costs associated with placing freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PI, which remains in Defendants' possession (and/or to which Defendants continue to have access) and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PI in their continued possession; and, (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of disclosed PI.

206. Defendants acted with wanton disregard for the security of Plaintiffs' and Class Members' PI.

207. Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT III
Declaratory and Injunctive Relief
(On Behalf of Plaintiffs and the Nationwide Class or, in the Alternative, the State Classes)

208. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

209. Plaintiffs bring this claim individually and on behalf of the Nationwide Class or, in the alternative, the State Classes.

210. As previously alleged, Plaintiffs and Class Members have a reasonable expectation that companies such as Defendants, who could access their PI through automated systems, would provide adequate security for that PI.

211. Defendants owe a duty of care to Plaintiffs and Class Members requiring them to adequately secure PI.

212. Defendants still possess and can still access PI regarding Plaintiffs and Class Members.

213. Since their Data Disclosure, Defendants have announced few, if any, changes to their decision to disclose the PI, their Data security infrastructure, or the processes or procedures to fix the vulnerabilities in their computer systems or Quote Platform.

214. Defendants' Data Disclosure caused actual harm because of Defendants' failure to fulfill their duties of care to provide security measures to Plaintiffs and Class Members. Further, Plaintiffs and Class Members are at risk of additional or further harm due to the exposure of their PI and Defendants' failure to address the security failings that led to such exposure.

215. There is no reason to believe that Defendants' security measures are more adequate now to meet Defendants' legal duties than they were before their Data Disclosure.

216. Plaintiffs therefore seek an order (1) declaring that Defendants' existing security measures do not comply with their duties of care to provide adequate security, and (2) directing Defendants to comply with their duties of care by implementing and maintaining reasonable security measures by:

a. ordering Defendants not to disclose PI, including driver's license information, to the general public through their website or sales platforms;

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

c. ordering Defendants to engage third–party security auditors and internal personnel to run automated security monitoring, including risk analysis on Defendants' decision making;

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

e. ordering Defendants not to make PI available on their Quote Platform;

f. ordering Defendants not to store PI or make PI accessible in any publicly facing website;

g. ordering Defendants to purge, delete, and destroy, in a reasonably secure manner, customer and consumer data not necessary for their provisions of services;

h. ordering Defendants to conduct regular computer system scanning and security checks; and

i. ordering Defendants to routinely and continually to conduct internal training and education to inform employees and officers on PI security risks, internal security personnel how to identify and contain a disclosure when it occurs, and what to do in response to a data security incident.

COUNT IV
Violations of New York General Business Law
N.Y. Gen. Bus. Law § 349 ("GBL")
(On Behalf of Plaintiffs and the Nationwide Class Against Defendants)

217. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

218. Plaintiffs bring this cause of action individually and on behalf of the Nationwide Class.

219. Section 349 of the New York GBL provides that "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state are hereby declared unlawful." N.Y. Gen. Bus. Law § 349(a).

220. Defendants, while operating in New York, engaged in deceptive acts and practices in the conduct of business, trade and commerce, and the furnishing of services, in violation of N.Y. Gen. Bus. Law § 349(a). This includes, but is not limited to, the following:

a. disclosing Plaintiffs' and Class Members' PI;

b. failing to enact adequate privacy and security measures to protect Plaintiffs' and Class Members' PI from unauthorized disclosure, release, and theft;

c. failing to take proper action following known security risks and prior cybersecurity incidents;

d. knowingly and fraudulently providing Plaintiffs' and Class Members' driver's license information directly to members of the public with small amounts of their PI;

e. omitting, suppressing, and concealing the inadequacy of Defendants' security protections;

f. knowingly and fraudulently misrepresenting that Defendants would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of PI; and

g. failing to disclose their Data Disclosure to the victims in a timely and accurate manner, in violation of the duties imposed by, *inter alia*, N.Y. Gen Bus. Law § 899-aa(2).

221. As a direct and proximate result of Defendants' practices, including their Data Disclosure, Plaintiffs and other Class Members suffered injury and/or damages, including, but not limited to, actual misuse of their PI, fraud, and identity theft; lost time and expenses related to monitoring their accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PI.

222. The above unfair and deceptive practices and acts by Defendants was immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs and other Class Members that they could not reasonably avoid, and which outweighed any benefits to consumers or to competition.

223. In view of their decision to disclose the PI in their Data Disclosure, Defendants knew or should have known that their systems and data security practices were inadequate to safeguard PI entrusted to it, and that risk of fraudsters obtaining the PI was highly likely.

224. Defendants' actions in engaging in the above-named unfair practices and deceptive acts, including Defendants' Data Disclosure, were negligent, knowing and willful.

225. Plaintiffs and Class Members seek relief under N.Y. Gen. Bus. Law § 349(h), including, but not limited to, actual damages (to be proven at trial), treble damages, statutory damages, injunctive relief, and/or attorneys' fees and costs.

226. Plaintiffs and Class Members seek to enjoin such unlawful deceptive acts and practices described above. Each Class Member will be irreparably harmed unless the Court enjoins Defendants' unlawful, deceptive actions, in that Defendants will continue to fail to protect the PI entrusted to them, as detailed herein.

227. Plaintiffs and Class Members seek declaratory relief, restitution for monies wrongfully obtained, disgorgement of ill-gotten revenues and/or profits, injunctive relief

prohibiting Defendants from continuing to disseminate their false and misleading statements, and other relief allowable under N.Y. Gen. Bus. Law § 349.

COUNT V
Violation of the Connecticut Unfair Trade Practices Act
Conn. Gen. Stat. § 42-110a, *et seq*.
(On Behalf of Plaintiff Murray and the Connecticut Class Against Defendants)

228. Plaintiff Murray ("Plaintiff" for purposes of this count) re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

229. Defendants, Plaintiff, and the Connecticut Class Members are "persons" within the meaning of the Connecticut Unfair Trade Practices Act ("Conn. UTPA"), Conn. Gen. Stat. § 42-110a(3).

230. The Conn. UTPA states: "No person shall engage in unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce." Conn. Gen. Stat. § 42-110b(a).

231. Defendants engaged in unfair or deceptive acts or practices in violation of Conn. Gen. Stat. § 42-110b(a) by, among other things:

a. failing to adopt reasonable data security procedures to adequately safeguard consumers' DLNs and/or other PI;

b. retaining DLNs and/or other PI for much longer than necessary for their business purposes;

c. omitting and concealing the material fact that they did not employ reasonable measures to secure consumers' DLNs and/or other PI. Defendants could and should have made a proper disclosure reasonably calculated to inform consumers of their inadequate data security;

d. making implied or implicit representations that their data security practices were sufficient to protect consumers' DLNs and/or other PI. Defendants intentionally obtained and disclosed Plaintiff's and Connecticut Class Members' DLNs and/or other PI during the quoting process of their Quote Platform. In doing so, Defendants made implied or implicit representations that their data security practices were sufficient to protect consumers' DLNs and/or other PI. By virtue of obtaining and disclosing Plaintiffs' DLNs and/or other PI during the quoting process, Defendants implicitly represented that their data security processes were sufficient to safeguard the DLNs and/or other PI; and

e. failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Connecticut Class Members' DLNs and/or other PI.

232. The Conn. UTPA states that their construction shall be "guided by interpretations given by the Federal Trade Commission and the federal courts to Section 5(a)(1) of the Federal Trade Commission Act (15 USC 45(a)(1))." Conn. Gen. Stat. § 42-110b(b). As discussed *supra*, the FTC treats the failure to employ reasonable data security safeguards as an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

233. Defendants conducted business in Connecticut for purposes of this claim. Connecticut Class Members and Plaintiff transacted with Defendants in Connecticut by, among other things, Defendants obtaining and intentionally disclosing their DLNs on their Quote Platform, and contracting with Plaintiff for insurance, in Connecticut. Plaintiff and the Connecticut Class Members were deceived in Connecticut when they were not informed of Defendants' deficient data security practices.

234. The Conn. UTPA states the following at Conn. Gen. Stat. § 42-110g(a):

> Any person who suffers any ascertainable loss of money or property, real or personal, as a result of the use or employment of a method, act or practice prohibited by section 42-110b, may bring an action . . . to recover actual damages. . . . The court may, in their discretion, award punitive damages and may provide such equitable relief as it deems necessary or proper.

Conn. Gen. Stat. § 42-110g(a).

235. Plaintiff and the Connecticut Class suffered an "ascertainable loss of money or property" based on the various types of damages alleged herein, including the loss of their DLNs and/or other PI.

236. Plaintiff and the Connecticut Class suffered "actual damages" based on the various types of damages alleged herein.

237. Plaintiffs are entitled to punitive damages under Conn. Gen. Stat. § 42-110g(a). Defendants knew or should have known that their data security practices were deficient. This is true because, among other things, Defendants was aware that the insurance industry was a frequent target of sophisticated cyberattacks, including the exact attack perpetrated here, because (as alleged above) the New York State Department of Financial Services warned all insurance companies, including Defendants, that cybercriminals were unlawfully obtaining DLNs prefilled on quote websites such as Defendants' Quote Platform. Defendants knew or should have known that their data security was insufficient to guard against those attacks. Also, given the size of Defendants' database and the sensitivity of the DLNs and other PI therein, Defendants should have taken adequate measures to protect that data. Defendants not only intentionally failed to encrypt the DLNs and other PI while it was stored on Defendants' systems, but also knowingly and intentionally disclosed this PI through the Quote Platform.

238. Plaintiff and the Connecticut Class are entitled to the injunctive relief sought herein because, among other things, Defendants continue to retain their DLNs and other PI and may subject those DLNs and other PI to further disclosures and/or unauthorized access unless the requested injunctive relief is granted.

239. The Conn. UTPA permits claims to be brought as class actions. Conn. Gen. Stat. § 42-110g(b).

240. The Conn. UTPA states the following at Conn. Gen. Stat. § 42-110g(d):

> [T]he court may award, to the plaintiff . . . costs and reasonable attorneys' fees based on the work reasonably performed by an attorney and not on the amount of recovery. . . . In any action brought under this section, the court may, in their discretion, order, in addition to damages or in lieu of damages, injunctive or other equitable relief.

Conn. Gen. Stat. § 42-110g(d).

241. Plaintiff and the Connecticut Class are entitled to recovery of their costs and reasonable attorneys' fees.

242. As a result of Defendants' unfair or deceptive acts or practices, Plaintiff and the Connecticut Class have suffered and will continue to suffer ascertainable losses of money or property, as well as non-monetary damages, all as alleged herein.

243. Plaintiff and the Connecticut Class seek all monetary, non-monetary, and injunctive relief allowed by the Conn. UTPA.

COUNT VI
Negligence Per Se
(On Behalf of Plaintiffs and the Nationwide Class or, in the Alternative, the State Classes)

244. Plaintiffs re-allege and incorporate by reference all preceding allegations as if fully set forth herein.

245. Plaintiffs bring this claim individually and on behalf of the Nationwide Class or, in the alternative, the State Classes.

246. Defendants had independent duties under state and federal laws requiring Defendants to reasonably safeguard Plaintiffs' and Class Members' PI. Pursuant to the FTC Act (15 U.S.C. § 45) and the GLB Act (15 U.S.C. § 6801, *et seq*.), Defendants had a duty to provide adequate data security practices in connection with safeguarding Plaintiffs' and Class Members' PI. Further, pursuant to the FTC Act (15 U.S.C. § 45), Defendants had a duty to provide fair, reasonable, or adequate data security in connection with the sale of insurance policies and use of the Defendants' website in order to safeguard Plaintiffs' and Class Members' PI.

247. Further, pursuant to DPPA, 18 U.S.C. § 2724, *et seq.*, Defendants had a duty to protect and also refrain from knowingly obtaining, disclosing, or using protected motor vehicle record information for impermissible purposes, and reselling, redisclosing, or—as recipients of the information—improperly maintaining protected motor vehicle record information. 18 U.S.C. §§ 2721, 2724. 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). 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).

248. Defendants failed to abide by, and thus violated, the DPPA by intentionally configuring and designing their insurance quote application portal on their website to disclose Plaintiffs' and Class Members' PI to anyone who requested an insurance quote. Defendants installed no protections or security measures to protect this information and willingly disclosed it to cybercriminals through the intentional configuration and design of its insurance quote

application portal. Defendants violated the DPPA by knowingly obtaining, using, and disclosing and/or redisclosing Plaintiff's and Class Members' motor vehicle records and PI to the general public in a manner that did and does not constitute authorized use permitted by the DPPA pursuant to 18 U.S.C. §§ 2724, 2721(b), and 2721(c), among other violations of the DPPA alleged herein. Defendants' conduct was particularly unreasonable given the nature and amount of PI it obtained and disclosed and the foreseeable consequences of a data disclosure.

249. In engaging in the knowing and/or negligent acts and omissions as alleged herein, in which Defendants disclosed Plaintiffs' and Class Members' PI to malicious actors through their online sales system, Defendants also violated Section 5 of the FTC Act, which prohibits "unfair…practices in or affecting commerce," and the GLB Act. This includes failing to have adequate data security measures and failing to protect Plaintiffs' and the Class Members' PI. Defendants also breached their duties to Plaintiffs and Class Members under the FTC Act (15 U.S.C. § 45), among other statutes, by failing to provide fair, reasonable, or adequate data security in order to safeguard Plaintiffs' and Class Members' PI in connection with the use of the Defendants' website and online sales system.

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

251. Plaintiffs and Class Members are within the class of persons that the DPPA, the GLB Act, and the FTC Act were intended to protect. The DPPA was expressly designed to protect a person's personal information contained in motor vehicle records from unauthorized disclosure. The GLB Act was expressly designed to protect private and personal information. The FTC Act is designed to protect consumers.

252. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

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

254. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and Class Members now face an increased risk of future harm. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

VII. PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of the Class, by and through undersigned counsel, respectfully request that the Court grant the following relief:

A. Certify this case as a class action pursuant to Fed. R. Civ. P. 23, and appoint Plaintiffs as the class representatives, Plaintiff Murray as the Connecticut Class representative, and Plaintiffs' counsel as class counsel;

B. Award Plaintiffs and Class Members actual, statutory, punitive, monetary, and nominal damages to the maximum extent allowable;

C. Award declaratory and injunctive relief as permitted by law or equity to assure that Class Members have an effective remedy, including enjoining Defendants from continuing the unlawful practices as set forth above;

D. Award Plaintiffs and Class Members pre-judgment and post-judgment interest to the maximum extent allowable;

E. Award Plaintiffs and Class Members reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Award Plaintiffs and Class Members such other favorable relief as allowable under law or at equity.

VIII. JURY TRIAL DEMANDED

Plaintiffs hereby demand a trial by jury on all issues so triable.

Dated: August 28, 2025

/s/ Melissa Clark

Mark B. DeSanto (admitted *pro hac vice*)
BERGER MONTAGUE PC
1818 Market Street, Suite 3600
Philadelphia, PA 19103
Telephone: (215) 875-3000
Facsimile: (215) 875-4604
mdesanto@bm.net

E. Michelle Drake (admitted *pro hac vice*)
BERGER MONTAGUE PC
1229 Tyler Street NE, Suite 205
Minneapolis, MN 55413
Telephone: (612) 594-5999
Facsimile: (612) 584-4470
emdrake@bm.net

Zachary M. Vaughan
BERGER MONTAGUE PC
1001 G Street, NW
Fourth Floor, Suite 400 East
Washington DC 20001
Telephone: 215.875.4602
Facsimile: 215.875.4604
zvaughan@bm.net

Melissa R. Clark
AHDOOT & WOLFSON, PC
521 5th Avenue, 17th Floor
New York, NY 10175
Telephone: (917) 336-0171
Facsimile: (917) 336-0177
mclark@ahdootwolfson.com

Andrew W. Ferich (admitted *pro hac vice*)
AHDOOT & WOLFSON, PC
201 King of Prussia Road, Suite 650
Radnor, PA 19087
Telephone: (310) 474-9111
Facsimile: (310) 474-8585
aferich@ahdootwolfson.com

Robert Ahdoot (admitted *pro hac vice*)
Alyssa Brown (admitted *pro hac vice*)
AHDOOT & WOLFSON, PC
2600 W. Olive Avenue, Suite 500
Burbank, CA 91505
Telephone: (310) 474-9111
Facsimile: (310) 474-8585
rahdoot@ahdootwolfson.com
abrown@ahdootwolfson.com

Ronald Podolny
John A. Yanchunis (admitted *pro hac vice*)
Antonio Arzola, Jr. (*pro hac vice* to be filed)
MORGAN & MORGAN COMPLEX

LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, FL 33602
Telephone: (813) 275-5272
ronald.podolny@forthepeople.com
jyanchunis@forthepeople.com
ararzola@forthepeople.com

Paul C. Whalen
LAW OFFICE OF PAUL C. WHALEN P.C.
769 Plandome Road
Manhasset, NY 11030
Telephone: (516) 426-6870
pcwhalen@gmail.com

Counsel for Plaintiffs and the Putative Classes