UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

BRIAN CONWAY, individually and on behalf of all similarly situated persons, Plaintiff, v. MAPFRE U.S.A. CORP. and THE COMMERCE INSURANCE COMPANY, Defendants.	Case No. **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Brian Conway ("Plaintiff") individually and on behalf the proposed Class, by and through undersigned counsel, brings this Class Action Complaint against Defendants MAPFRE U.S.A. Corp. ("MAPFRE") and The Commerce Insurance Company ("Commerce") (collectively, "MAPFRE" or "Defendants"), and allege as follows:

INTRODUCTION

1. Every year, millions of Americans have their most valuable personal information disclosed and their privacy intruded upon because corporations seeking to maximize profits misuse their personal information, making the public vulnerable to fraudsters.

2. In an effort to stem the tide of such misuses and disclosures, and in recognition of the sensitivity of drivers' license information (and its utility to identity thieves), Congress passed the Drivers' Privacy Protection Act ("DPPA"), which restricts access to drivers' license information, and mandates that private companies may only use it for limited, enumerated, purposes. Under the DPPA, private companies are legally required to protect from unauthorized

access and exfiltration the personal information ("PI") that they obtain and use. In the DPPA, Congress specifically defines PI to include driver's license numbers. *See* 18 U.S.C. 2725(3).

3. Unauthorized third parties harvest driver's license numbers because they are highly valuable pieces of PI. A driver's license can be a critical part of a fraudulent, synthetic identity, with reports indicating that the going rate for a stolen identity is about $1,200 on the dark web, and that a stolen or forged driver's license, alone, can sell for around $200.[1] Driver's license numbers are particularly useful to identity thieves for applying for unemployment or other government benefits.

4. Defendants MAPRE and Commerce write property and casualty insurance policies in fourteen states across the country and claim to be the 19th largest private auto insurer and 33rd largest homeowner's insurer in the country. MAPFRE markets its policies mainly by direct response methods whereby customers apply for coverage directly to the company via the internet or over the telephone. MAPFRE provides online insurance quotes to consumers through its online sales system on its publicly accessible insurance website.

5. Despite warnings about the severe impact of identity theft on Americans of all economic strata, companies—including Defendants—still put their own economic interests ahead of consumers' privacy interests.

6. Turning a blind eye to the limitations imposed by the DPPA, MAPFRE knowingly chose to obtain, use, and disclose federally protected drivers' license numbers and other motor vehicle record information to grease the wheels of its online insurance sales. MAPFRE chose to

[1] Lee Mathews, *Hackers Stole Customers' License Numbers From MAPFRE In Months-Long Breach,* Forbes (Apr. 20, 2021, 11:57 A.M. EDT), https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/.

add a feature to its existing online sales platform whereby an individual's driver's license number would auto-populate for anyone that would enter a bare minimum of publicly available information about that individual.

7. MAPFRE had offered online insurance quotes to applicants before it incorporated this auto-population feature but added the auto-population feature to its online sales system in order to gain competitive advantage in its sales process. MAPFRE's conduct is motivated by its desire to entice customers to complete applications for insurance.

8. By adding the auto-population feature to its online quoting process, which MAPFRE knowingly chose to do, MAPFRE intended to make the displayed information, which it obtained and used to create the feature, easily accessible to anyone who entered basic information into its system. MAPFRE did not impose any security protocols to ensure that website visitors entered and accessed PI only about themselves. MAPFRE did not impose effective security protocols to prevent automated bots from accessing consumers' PI. Thus, MAPFRE effectively published consumers' driver's license numbers, including Plaintiff's and the class members', on the internet's "windshield," for all digital passers-by with a few bits of others' PI to see.

9. MAPFRE's decision quickly caught the attention of identity thieves, who mined MAPFRE's website and obtained private drivers' license information for hundreds of thousands of consumers, including Plaintiff.

10. In a document entitled "Data Security Incident Report of MAPFRE Insurance" dated August 22, 2023 (the "Notice"), MAPFRE informed affected victims "of an incident that involved your personal information and, possibly, information about your vehicle(s)," and that the so-called "incident" had occurred between July 1 and 2, 2023 (the "Data Disclosure"). According to the Notice, "an unknown party used information about [class members]—which was already in

the unknown party's possession—to obtain access to additional information about you through MAPFRE's Massachusetts online quoting platform in Massachusetts," and MAPFRE has determined that its disclosure involved driver's license numbers obtained "through MAPFRE's Massachusetts online quoting platform" and may have included the following vehicle information: "make, model, year, and vehicle identification number." MAPFRE acknowledged that information could be used to conduct "incidents of identity theft and fraud" and has acknowledged that it "took down our Massachusetts online quoting platform" following the Data Disclosure. The Notice further instructed those affected to "remain vigilant" to prevent identity theft and fraud, and "to monitor your free credit reports for suspicious activity and to detect errors." The Notice did not identify the information "which was already in the unknown party's possession" but, on information and belief, this information is publicly available "phone book" information that can be retrieved through a simple internet search or accumulated in data bases and widely available on the internet. Through the Notice, MAPFRE also acknowledged that it had obtained and used the information in the design and creation of the online sales feature.

11. MAPFRE sent a Notice to Plaintiff Conway. Thus, his sensitive driver's license number and other personal information were disclosed to unauthorized persons. Plaintiff has also experienced credit card fraud following MAPFRE's Data Disclosure. This fraud is logically and temporally related to Defendants' disclosure of Plaintiff's driver's license number.

12. While the Notice indicated that MAPFRE "took down" the affected website "[a]s soon as [it] became aware of the issue" and that it has "implemented additional controls . . . to protect against reoccurrence of the incident," unfortunately for Plaintiff, the damage to privacy had already been done. As a result of MAPFRE's Data Disclosure, Plaintiff's privacy has been invaded, his sensitive drivers' license information is now in the hands of criminals, and he faces a

substantially increased risk of identity theft and fraud. Accordingly, Plaintiff and other victims now must take immediate and time-consuming action to protect themselves from identity theft and fraud.

13. To redress MAPFRE's illegal profit-seeking conduct, Plaintiff brings this class action individually and on behalf and all other individuals ("Class Members") who had their driver's license information disclosed because of MAPFRE's sales efforts and during MAPFRE's Data Disclosure. Plaintiff, individually and on behalf of the Class Members, seeks remedies, including monetary damages and injunctive relief (including relief under the federal Declaratory Judgment Act), for MAPFRE's violations of the DPPA and its negligence.

PARTIES

Plaintiff Brian Conway

14. Plaintiff Brian Conway is a citizen of the Commonwealth of Massachusetts and resides in South Hadley, Massachusetts.

15. In or about August 2023, MAPFRE sent, and Plaintiff Conway subsequently received, a data disclosure notification letter, confirming that he was impacted by MAPFRE's Data Disclosure, and that his driver's license number was obtained, used, and disclosed by MAPFRE.

16. The notice letter stated that "[b]etween July 1 and July 2, 2023, an unknown party used information about you-which was already in the unknown party's possession—to obtain access to additional information about you through MAPFRE's Massachusetts online quoting platform in Massachusetts." It further stated: "We have determined that the unknown party obtained access to your driver's license number through MAPFRE's Massachusetts online quoting platform. The unknown party may also have obtained access to information regarding vehicles you own, including make, model, year, and vehicle identification number." Thus, the Notice

acknowledges that the unauthorized persons also had other information about Plaintiff Conway that they had acquired elsewhere, and that they used to access and link Plaintiff Conway's driver's license number to that other information.

17. Following the Data Disclosure, Plaintiff Conway experienced an approximately $400.00 fraudulent charge on his Mastercard. This fraud occurred after MAPFRE's Data Disclosure. This fraud and identity theft is temporally and logically connected to the data derived from MAPFRE's Data Disclosure in the same way that data breach and other privacy cases have found to be "fairly traceable." MAPFRE disclosed Plaintiff Conway's driver's license number and, potentially, other personal information, shortly before he experienced the fraud.

18. Plaintiff Conway has taken (and continues to take) considerable precautions to protect the unauthorized dissemination of his PI. To date, he has spent approximately 15 hours monitoring accounts and otherwise dealing with the fallout of the Data Disclosure. Unfortunately, because of MAPFRE's disclosure of his PI, Plaintiff Conway's sensitive driver's license number and other sensitive information was disseminated without his consent, has already been fraudulently used by unauthorized third parties, and the value of that information was quantifiably reduced.

19. As a result of MAPFRE's Data Disclosure, Plaintiff Conway suffered injury and/or damages, including but not limited to actual identity theft; time and expenses interacting with government agencies, 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; 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.

Additionally, because of MAPFRE's Data Disclosure, Plaintiff Conway now faces a substantial risk that unauthorized third parties will further misuse his PI.

Defendants

20. Defendants MAPFRE U.S.A. Corp. and The Commerce Insurance Company are Massachusetts corporations with a principal place of business in Webster, Massachusetts. Defendants write property and casualty insurance policies in 14 states across the country and claim to be the 19th largest private auto insurer and 33rd largest homeowners insurer in the country. The Commerce Insurance Company is a subsidiary of MAPFRE U.S.A. Corp.

JURISDICTION AND VENUE

21. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds $5 million, exclusive of interest and costs; the number of members of the proposed Class exceeds 100; and diversity exists because there is minimal diversity in that one member of the class resides in a state different than where Defendants are citizens. The Court also has federal question jurisdiction under 28 U.S.C. § 1331 for the DPPA claim. This Court has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

22. The Court has personal jurisdiction over Defendants because Defendants have their principal places of business in Massachusetts and conduct significant business in the commonwealth of Massachusetts, thus availing themselves of Massachusetts markets by selling insurance policies; have sufficient minimum contacts with the commonwealth of Massachusetts; and a substantial part of the conduct giving rise to Plaintiff's claims occurred in Massachusetts.

23. Venue properly lies in this judicial district pursuant to 28 U.S.C. § 1391 because, *inter alia*, a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in,

were directed to, and/or emanated from this district; Defendants have principal places of business in this district, transact substantial business and have agents in this district; and a substantial part of the conduct giving rise to Plaintiff's claims occurred in this judicial district.

FACTUAL ALLEGATIONS

A. MAPFRE Collects Vast Amounts of Sensitive PI from Consumers and Third Parties

24. MAPFRE primarily offers private passenger automobile and homeowner's insurance to individuals in 14 states.[2]

25. MAPFRE collects and stores vast amounts of personal information and sensitive data from prospective clients, current and former customers, and other consumers, as part of its regular business practices. Included in this information are highly sensitive driver's license numbers. For example, during the quoting, application, claims, and other insurance processes, MAPFRE informs customers and potential customers of the following:

> We collect and use information that we believe is necessary to serve you effectively and to permit us to meet your needs, such as information that we receive from your insurance application and through correspondence and communications from you, including name, address, and telephone number; information about your transactions with us; information that you provide to us on our web site; information from your insurance agent or broker (if applicable); information that we receive from consumer reporting agencies; information from website usage (or traffic); information from customer lists provided by other organizations and marketing data providers; information from governmental agencies and insurance-support organizations; and information relating to insurance claims, which may include medical information.[3]

26. Discovery will show that during the insurance claims process, MAPFRE also requires submission of similar personal information in connection with insurance processing

[2] MAPFRE, *About Us*, https://www.mapfreinsurance.com/where-we-are/ (last visited Sept. 7, 2023).

[3] MAPFRE, *Privacy Policy*, https://www.mapfreinsurance.com/privacy-policy/ (last visited Sept. 7, 2023).

claims, including from individuals who are not MAPFRE policyholders but who are involved in a claim being handled by MAPFRE, such as drivers involved in accidents with MAPFRE insureds.

27. MAPFRE's marketing is primarily through direct response methods in which consumers submit applications for insurance directly to Defendants via the internet or by telephone, and to a lesser extent, through captive agents.

28. Competition for private passenger automobile insurance, which is substantial, tends to focus on price and level of customer service provided.

29. Like other insurance providers, MAPFRE has an online sales system available to all persons capable of accessing it via the internet. Visitors to MAPFRE's insurance website can get a quote instantly after providing some PI.

30. Defendants' now-removed quoting feature used the information entered by the website visitor, combined it with additional information Defendants had or that Defendants could access from third-party prefill services, and then automatically displayed the additional information to the visitor as part of the quote process.

31. Specifically, Defendants' quoting feature may ask any visitor to the site for their name, date of birth, and address. Once a visitor enters that information, Defendants' system auto-populates the quotation with driver's license information from Defendants' own databases or from third-party prefill service providers (e.g., Lexis) and makes that information visible to the person entering the information on the MAPFRE quote website.

32. "Phone book" information—such as a person's name, date of birth, or address—is data that is publicly available and easily attained. It is common knowledge and MAPFRE knew that this information is compiled in multitudes of different databases available on the internet,

often at no cost.[4]

33. An automated process, or "bot," was used on the instant quote feature to obtain Plaintiff's and Class Members' driver's license numbers, which includes many people who never applied for insurance with Defendants or were even necessarily aware of Defendants' existence. In other words, unauthorized parties availed themselves of the PI Defendants made publicly available via their instant quote feature on a wholesale basis.

34. Defendants' online sales system did not require verification that the person or automated process accessing the system was *actually* the individual for whom the information was being entered. In addition, Defendants' online sales system did not employ effective, industry-standard security measures to detect whether the website visitor was, in fact, a "bot" or automated process rather than an individual person. Instead, Defendants configured their online sales system to provide PI—including driver's license numbers—when anyone, including bots, just entered commonly known information. Thus, Defendants' online sales system was purposefully and knowingly set up to disclose to any site visitor, including bots, PI (including driver's license numbers) of anyone about whom Defendants had collected or could access that PI simply so that MAPFRE could more easily sell its insurance products.

B. Defendants Contravened the Purpose of the Driver's Privacy Protection Act

35. Prior to the enactment of the Driver's Privacy Protection Act, Congress found that most states freely turned over DMV information to whomever requested it with only few

[4] 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 its website, www.mylife.com. … On its 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.*, No. CV 20-6692-JFW(PDX), 2021 WL 4891776, at *2 (C.D. Cal. Oct. 19, 2021) (citations omitted) (emphasis added).

restrictions. 137 Cong. Rec. 27,327 (1993).

36. Due to this 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).

37. 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 upcoming 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).

38. In light of 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).

39. Additionally, in enacting the DPPA, Congress was motivated by its "[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 like driver's license numbers and other motor vehicle records was the exact impetus for the DPPA's passage.

40. As such, 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). Driver's license numbers are thus explicitly listed as "personal information" from "motor vehicle records" under the DPPA. *See* 18 U.S.C. 2725(1).

41. By knowingly using the PI of Plaintiff 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 Plaintiff and Class Members, that would not have happened but for Defendants' failure to adhere to the DPPA. Plaintiff was harmed by the public disclosure of Plaintiff's private facts in addition to the other harms enumerated herein.

C. The Data Use and Disclosure, and Its Impact

42. In the Notice dated August 22, 2023, MAPFRE notified consumers that their sensitive PI—namely, driver's license numbers—was compromised in the Data Disclosure, which it described as follows:

> **What Happened**
>
> Between July 1 and July 2, 2023, an unknown party used information about you- which was already in the unknown party's possession—to obtain access to additional information about you through MAPFRE's Massachusetts online quoting platform in Massachusetts.

What Information Was Involved

> We have determined that the unknown party obtained access to your driver's license number through MAPFRE's Massachusetts online quoting platform. The unknown party may also have obtained access to information regarding vehicles you own, including make, model, year, and vehicle identification number.[5]

43. While the Notice indicates that "[a]s soon as MAPFRE became aware of the issue" MAPFRE "took down our Massachusetts online quoting platform and conducted an investigation," the Notice does not provide the date when MAPFRE learned of or "became aware of" the incident.

44. MAPFRE's obtaining, use, and disclosure of the driver's license numbers, its Data Disclosure through its online sales platform, and its violation of the law, assisted an ongoing and concerted campaign by unauthorized third parties to engage with insurers' online quoting platforms to obtain driver's license numbers. For example, on February 16, 2021 the New York State Department of Financial Services issued an alert regarding an ongoing systemic and aggressive campaign to engage with public-facing insurance websites—particularly those that offer instant online automobile insurance quotes—to obtain non-public information, in particular unredacted driver's license numbers.[6] According to the alert, the unauthorized collection of driver's license numbers appears 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 driver's license

---

[5] MAPFRE, *Data Security Incident Report of MAPFRE Insurance* (Aug. 22, 2023), Commonwealth of Massachusetts Office of Consumer Affairs and Business Regulation, https://www.mass.gov/doc/assigned-data-breach-number-30358-the-commerce-insurance-company-mapfre-insurancer/download.

[6] Department of Financial Services, *Industry Letter* (Feb. 16, 2021), https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210216_cyber_fraud_alert#_edn.

numbers. Defendants should have been aware of these campaigns and the alerts issued by DFS and other state actors.

45. 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.[7] 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 driver's license numbers without going any further in the process and abandoned the quote."[8] Of-course, MAPFRE need not use driver's license numbers on a sales platform, or disclose this information to the public, to underwrite any auto insurance policy. Its use of driver's license numbers is purely intended to reduce quoting time, speeding up the quoting process and driving volume of quotes and, thus, sales and profits.

46. The increase in interest in driver's license numbers 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 expired driver's licenses for various purposes for an extended period, due to difficulty in securing the in-person DMV appointments necessary to renew them.[9]

---

[7] *Id.*

[8] *Id.*

[9] CPO Magazine, *Geico Data Breach Leaks Driver's License Numbers, Advises Customers to Watch Out for Fraudulent Unemployment Claims*, https://www.cpomagazine.com/cyber-

47. Unsurprisingly, fraudulent unemployment claims spiked during the pandemic, as more money has become available to displaced workers and the requirements for filing have eased. Many states have paid out tens of millions of dollars to scammers, a phenomenon largely driven by the unauthorized use of fraudulently obtained PI. Hackers 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.[10]

48. The United States Department of Labor estimates that pre-pandemic fraudulent unemployment claims accounted for about 10% of all filings.[11] 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.

49. MAPFRE knew that it was using driver's license information on its online sales platform. MAPFRE also knew that this platform was created and maintained in a way that allowed unauthorized third parties to plug in readily and publicly available basic personal information of other persons, and that the website would auto-populate driver's license information into its quoting tool (i.e., publish it) once that basic information is entered. Indeed, MAPFRE was responsible for its website, including its design and design features. MAPFRE thus knew that its

---

security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/ (last visited Sept. 7, 2023).

[10] *Id.*

[11] Megan DeMatteo, *Unemployment fraud costs victims $200 billion annually in the U.S. – here's how to protect yourself*, CNBC (Apr. 27, 2021), https://www.cnbc.com/select/how-to-protect-yourself-from-unemployment-fraud/.

website and the website's auto-populate feature disclosed consumers' driver's license number to anyone, and worked just as it was designed.

50. Not only did MAPFRE know that it was using driver's license numbers to sell insurance, and that it was disclosing driver's license numbers to the public, but it also failed to assess 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. By adding the auto-population feature to its online quoting process, which MAPFRE knowingly chose to do, MAPFRE intended to use the driver's license numbers and make the displayed information easily accessible to anyone who entered basic information into its system. MAPFRE did not impose any security protocols to ensure that website visitors entered and accessed PI only about themselves. MAPFRE did not impose effective security protocols to prevent automated bots from accessing consumers' PI. Thus, MAPFRE knowingly used and posted consumers' driver's license numbers directly to all members of the public.

D. Defendants' Use of Data and the Data Disclosure Create a Substantial Risk of Identity Theft and Fraud

51. The extent, scope, and impact of MAPFRE's use of the data and its Data Disclosure on its customers and other consumers remains uncertain. Nevertheless, the harm caused to Plaintiff and Class Members by MAPFRE's use of the information and its Data Disclosure is already apparent. Criminals now possess Plaintiff's and Class Members' driver's license numbers, 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.

52. Defendants' Notice specifically admonished Plaintiff and Class Members to take mitigation steps:

What You Can Do

> We encourage you to remain vigilant against incidents of identity theft and fraud, and to monitor your free credit reports for suspicious activity and to detect errors. Enclosed with this letter are some steps you can take to protect your information.[12]

53. The Notice includes an attachment recommending vigilance for incidents of fraud or identity theft, explaining how to report such incidents to the Federal Trade Commission and/or to one's state attorney general, and explaining how to obtain one's credit reports and utilize credit freezes.

54. Having received the Notice about MAPFRE's Data Disclosure, it is reasonable for Plaintiff 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 Notice relate to the fact that criminals obtained the disclosed driver's license numbers for the purpose of committing fraud in the name of the person whose license number is taken.

E. The PI MAPFRE Obtained, Used, and Then Disclosed in Its Data Disclosure Is Highly Valuable to Fraudsters

55. It is well known among companies that store or have access to sensitive PI that driver's license numbers are valuable and frequently targeted by criminals. The PI that Defendants voluntarily disclosed via their online sales system in violation of state and federal law is very valuable to phishers, identity thieves, cyber criminals, and other fraudsters, and driver's license information is uniquely connected to the ability to commit financial fraud. Unsecured sites that

[12] MAPFRE, *Data Security Incident Report of MAPFRE Insurance* (Aug. 22, 2023), Commonwealth of Massachusetts Office of Consumer Affairs and Business Regulation, https://www.mass.gov/doc/assigned-data-breach-number-30358-the-commerce-insurance-company-mapfre-insurancer/download.

contain or transmit PI such as driver's license numbers require notice to consumers when the data is stolen because it can be used to commit identity theft and other types of fraud.

56. The driver's license numbers disclosed in MAPFRE's 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 disclosed in MAPFRE's Data Disclosure can be used to *open* fraudulent bank accounts and credit and debit cards or take out loans. The driver's license numbers disclosed in MAPFRE's Data Disclosure are also more valuable because they are long lasting, and difficult to change.

57. 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 driver's license number during an arrest, resulting in an arrest warrant being issued in the victim's name.[13] 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.

58. Fraudsters often aggregate information taken from data security incidents to build profiles on individuals. These profiles combine publicly available information with information

[13] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited on Sept. 7, 2023).

discovered in previous data security incidents and exploited vulnerabilities. There are few data security incidents that provide a comprehensive snapshot of any one individual person. Unique and persistent identifiers such as Social Security numbers, driver's license numbers, usernames, and financial account numbers (e.g., credit cards, insurance policy numbers, etc.) are critical to forging an identity. 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"[14] profile can be obtained.

59. There is no legitimate or legal reason for anyone to use Defendants' website to acquire driver's license information on Plaintiff and the Class Members. Dark Net Markets ("DNM(s)"), 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 malicious actors buy and sell that information for profit.[15] "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).

60. Any non-public data, especially government issued identification numbers like a driver's license or non-driver's identification number, has criminal value.[16] For example, a fake

---

[14] "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.

[15] *Shining a Light on the Dark Web with Identity Monitoring*, Identity Force (Dec. 28, 2020), https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring.

[16] Identity Theft Resource Center, *Can Someone Steal Your Identity From Your Driver's License?* (Feb. 19, 2021) https://www.idtheftcenter.org/can-someone-steal-your-identity-from-your-drivers-license/ (last visited Sept. 8, 2023).

U.S. citizenship kit for sale: passport, SSN, 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.[17]

61. Prices can vary depending on the point in the chain – verified identities may sell for higher prices early in the chain, then for the lower prices when they reach the "flea market sites." DNMs are a downstream "flea market" for data to be sold, usually not by the original threat actor or criminal group. It is a dumping ground, usually after the data has been exploited. The value of stolen driver's license information currently has a DNM value of $1 per license. This was re-verified on March 3, 2022, accessing several DNM using a trusted identity. Social Security numbers, once considered the "gold standard" of identity fraud, are also selling for $1 per number in those same markets. This illustrates the value of driver's license information to cybercriminals and people committing identity fraud. According to popular DNMs, cyber criminals value driver's license numbers equally to Social Security numbers.

62. In some ways, driver's license numbers are even more attractive than Social Security numbers to threat actors and more dangerous to the consumer when disclosed. Unlike a Social Security number, a driver's license number is not monitored as closely, so it can potentially be used in ways that will not immediately alert the victim. Threat actors know this as well. Because driver's licenses contain, or can be used to gain access to, uniquely qualifying and comprehensive identifying information such as eye color, height, weight, sex, home address, medical or visual restrictions, and living will/health care directives, most insurance and credit agencies highly

[17] Daniel Shkedi, *Heart of Darkness: Inside the Darknet Markets that Fuel Financial Cybercrime*,BioCatch, https://web.archive.org/web/20210905231044/https://www.biocatch.com/blog/financial-cybercrime-darknet-markets (last visited Sept. 7, 2023).

recommend immediate notice and replacement, and that identity theft protections are put in place for a minimum of 3 years. Most cyber experts, including Enterprise Knowledge Partners, recommend five years or more.

63. Blogger Gayle Sato from the national credit reporting company Experian emphasized the value of driver's license information to thieves and cautioned:

> Your driver's license may not seem like a jackpot for thieves, but it can be used to create fake driver's licenses, open accounts in your name, avoid traffic tickets or collect government benefits such as unemployment checks. Worse, if your license data has been stolen in a data breach, you may not even know it's being misused.[18]

64. 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 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.[19]

65. 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

---

[18] Gayle Sato, *What Should I Do If My Driver's License Number Is Stolen?* Experian (Nov. 3, 2021) https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/.

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

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."[20]

66. The process that was used to extract the data from Defendants' website was likely automated. The identity thieves have demonstrated the value they place on the driver's license numbers by engaging in a systematic and businesslike process for collecting them from MAPFRE's Data Disclosure and from additional insurers' websites offering instant quotes.

67. 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.[21] 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."[22]

---

[20] Zach Whittaker, *MAPFRE Admits Fraudsters Stole Customers' Driver's License Numbers for Months*, TechCrunch (Apr. 19, 2021), https://techcrunch.com/2021/04/19/MAPFRE-driver-license-numbers-scraped/#:~:text=To%20get%20a%20driver's%20license,benefits%20in%20another%20person's%20name.

[21] *See* United States Government Accountability Office, *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.

[22] *Id.*

F. Defendants Failed to Comply with Federal Trade Commission Requirements

68. 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 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.[23]

69. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[24] Among other things, the guidelines note businesses should properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct 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.[25]

70. Also, the FTC recommends companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for

---

[23] Federal Trade Commission, *Start With Security: A Guide for Business*, (June 2015) https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[24] *See* Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

[25] *Id.*

suspicious activity on the network; and verify third-party service providers have implemented reasonable security measures.[26]

71. 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 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.[27]

72. Through negligence in designing and implementing their online quoting platform and securing Plaintiff's and Class Members' PI, Defendants knowingly allowed the public—and thieves—to utilize their online sales system to obtain access to and collect individuals' PI. Defendants failed to employ reasonable and appropriate measures to protect against unauthorized disclosure and access to Plaintiff's 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, and the DPPA, 18 U.S.C. § 2724, *et seq*.

G. Plaintiff's Injuries—Attempts to Secure PI After MAPFRE's Data Disclosure

73. Defendants admitted in the Notice that there was disclosure of Plaintiff's and Class Members' driver's license numbers to third parties. Defendants also concede that this disclosure created imminent harm to Plaintiff and Class Members, specifically acknowledging that the Data

[26] *Start With Security*, *see supra* n.23.

[27] *See* Federal Trade Commission, *Privacy and Security Enforcement Press Releases*, available at https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement.

Disclosure can lead to "incidents of identity theft and fraud." MAPFRE tasked Plaintiff and Class Members with various mitigation steps and offered a year of credit monitoring. These measures are woefully inadequate and do not absolve MAPFRE of its violations of the DPPA and other laws alleged herein.

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

H. Plaintiff and Class Members Suffered Additional Damages

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

76. 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.[28]

77. Plaintiff's and Class Members' driver's license numbers are private, valuable, and sensitive in nature as they can be used to commit a lot of different harms and fraud in the hands of the wrong people. Defendants did not obtain Plaintiff's and Class Members' consent to disclose such PI to any other person, as required by applicable law and industry standards.

78. Defendants' decision to expose Plaintiff and Class Members to the possibility that anyone, especially thieves with various pieces of individuals' PI, could obtain any individual's

[28] *2014 LexisNexis True Cost of Fraud Study*, (August 2014), https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf.

driver's license number by utilizing Defendants' front-facing online instant quote platform left Plaintiff and Class Members with no ability to protect their sensitive and private information.

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

80. Despite the known risk of data disclosures including ones involving disclosure of drivers' license numbers, and the widespread publicity and insurance industry alerts regarding other similar data security events involving auto-fill features on online insurance quoting tools, Defendants failed to take reasonable steps to adequately secure MAPFRE's website and publish it in a manner that did not hand over Class Members' driver's license numbers to unauthorized third parties, leaving MAPFRE customers and other consumers, including Plaintiff and Class Members, exposed to risk of fraud and identity theft.

81. Defendants were, and at all relevant times have been, aware that the PI MAPFRE handles and stores in connection with its services is highly sensitive. Because MAPFRE is a company that provides insurance services involving highly sensitive and identifying information, Defendants were aware of the importance of safeguarding that information and protecting its websites, systems, and products from security vulnerabilities.

82. 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 driver's license numbers to members of the public on MAPFRE's website.

83. Defendants knowingly obtained, used, disclosed, and compromised Plaintiff's and Class Members' PI by creating the online quoting platform with the auto-populate feature, and voluntarily transmitting it directly to members of the public, including fraudulent actors. MAPFRE

failed to take reasonable steps against an obvious threat. MAPFRE designed and implemented its own website using driver's license information, including the instant quote feature that auto-populated Class Members' drivers' license numbers in response to the input of very basic publicly available consumer information. MAPFRE knowingly included this instant quote feature on its website. The website and this feature operated exactly as Defendants intended and designed it to work.

84. Had Defendants never used the information to sell insurance or never included this feature on its sales platform, it would have prevented the disclosure, unauthorized access, and ultimately, the fraudulent use and possible fraudulent use of the PI.

85. As a direct and proximate result of Defendants' actions and inactions, Plaintiff 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 MAPFRE's Data Disclosure on their lives.

86. 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."[29]

87. As a result of Defendants' Data Disclosure, Plaintiff 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,

[29] U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012*, (December 2013) https://www.bjs.gov/content/pub/pdf/vit12.pdf.

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

c. Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of MAPFRE's 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 MAPFRE's Data Disclosure for the remainder of the lives of Plaintiff and Class Members.

88. In addition to a remedy for the economic harm, Plaintiff 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.

89. To date, other than providing 12 months of credit monitoring and identity protection services, Defendants do not appear to be taking any measures to assist Plaintiff and Class Members other than simply telling them to "remain vigilant against incidents of identity theft and fraud"; "monitor your free credit reports for suspicious activity and to detect errors"; obtain a copy of your free credit report; contact the FTC and/or the state Attorney General's office to report misuse of your personal information; or to obtain additional information about avoiding identity theft. None of these recommendations, however, require Defendants to expend any effort to protect Plaintiff's

and Class Members' PI, and they all fail to provide monetary compensation or any protection whatsoever after 12 months.

90. Defendants' disclosure of driver's license numbers directly to members of the public has resulted in Plaintiff and Class Members having to undertake these tasks, which require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money. Instead, as Defendants' Notice confirms, they are putting the burden on Plaintiff and Class Members to discover possible fraudulent activity and identity theft.

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

92. 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.

93. 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.[30]

94. Industry experts are clear that a data security incident is indicative of data security failures. Indeed, though MAPFRE's knowing Data Disclosure is more egregious than a data breach

[30] *Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown*, at 29, *see supra* at n.21 (emphasis added).

because it knowingly handed drivers' license numbers and other PI over to bad actors without any breach or intrusion, industry-leading research and advisory firm Aite Group has identified that: "If your data was stolen through a data breach that means you were somewhere out of compliance . . . ."[31]

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

CLASS ALLEGATIONS

96. Plaintiff brings this action on behalf of himself and the following Classes pursuant to Federal Rule of Civil Procedure 23(a) and (b):

Nationwide Class

> All residents of the United States whose driver's license and other personal information and was disclosed in the MAPFRE Data Disclosure occurring in or around the period between July 1 and July 2, 2023, including all persons who received notice of the MAPFRE Data Disclosure.

[31] Lisa Baertlein, *Chipotle Says Hackers Hit Most Restaurants in Data Breach*, Reuters (May 26, 2017), http://www.reuters.com/article/us-chipotle-cyber-idUSKBN18M2BY.

Massachusetts Class

All residents of Massachusetts whose driver's license and other personal information and was disclosed in the MAPFRE Data Disclosure occurring in or around the period between July 1 and July 2, 2023, including all persons who received notice of the MAPFRE Data Disclosure.

97. The above defined classes are collectively referred to as the "Class" or "Classes." Plaintiff reserves the right to re-define the Class(es) prior to class certification. Plaintiff reserves the right to modify these class definitions as discovery in this action progresses.

98. Excluded from the Class are Defendants and their affiliates, officers, directors, assigns, successors, and the Judge(s) assigned to this case.

99. **Numerosity**: While the precise number of Class Members has not yet been determined, members of the Classes are so numerous that their individual joinder is impracticable, as the proposed Classes appear to include at least 266,142 customers of Defendants.[32]

100. **Typicality**: Plaintiff's claims are typical of Class Members' claims. Plaintiff and all Class Members were injured through Defendants' uniform misconduct, and Plaintiff's claims are identical to the claims of the Class Members he seeks to represent. Accordingly, Plaintiff's claims are typical of Class Members' claims.

101. **Adequacy**: Plaintiff is an adequate representative of the Class because Plaintiff's interests are aligned with the Classes Plaintiff seeks to represent and Plaintiff has no conflicts of interest with the Classes. Plaintiff's counsel are competent with significant experience prosecuting complex class action cases, including cases involving alleged privacy and data security violations. The law firm of Ahdoot & Wolfson, P.C. is appointed as co-lead counsel in similar litigation

[32] *See* https://www.mass.gov/doc/data-breach-report-2023/download.

involving the same type of data disclosure with a pre-fill feature on another insurer's insurance quoting website. *See In re GEICO Customer Data Breach Litig.*, No. 1:21-cv-02210-KAM-SJB (E.D.N.Y.). Plaintiff and Plaintiff's counsel intend to prosecute this action vigorously. The Classes' interests are well-represented by Plaintiff and Plaintiff's counsel.

102. **Superiority**: A class action is the superior—and only realistic—mechanism to fairly and efficiently adjudicate Plaintiff's 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 presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented 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.

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

- whether Defendants engaged in the wrongful conduct alleged herein;
- whether Defendants knowingly used Plaintiff's and the Class Members' driver's license numbers to sell auto insurance;
- whether Defendants knowingly disclosed Plaintiff's and the Class Members' driver's license numbers;
- whether Defendants violated the DPPA;

- whether Defendants' data security practices and the vulnerabilities of MAPFRE's systems resulted in the disclosure of Plaintiff's and other Class Members' sensitive information;
- whether Defendants violated privacy rights;
- whether Defendants were negligent when they disclosed the sensitive information of Plaintiff and other Class Members; and
- whether Plaintiff and Class Members are entitled to damages, equitable relief, or other relief and, if so, in what amount.

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

CAUSES OF ACTION

COUNT I
Violation of the Drivers' Privacy Protection Act, 18 U.S.C. § 2724, *et seq.*
(On behalf of Plaintiff and the Nationwide Class, or in the alternative, the Massachusetts Class)

105. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

106. Plaintiff brings this cause of action individually and on behalf of the Nationwide Class or, in the alternative, the Massachusetts Class.

107. 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.

108. The DPPA also restricts the resale and redisclosure 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).

109. 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). Drivers' license numbers are motor vehicle records and "personal information" under the DPPA. 18 U.S.C. § 2725(3).

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

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

112. Defendants knowingly used the above-described information to sell auto insurance on their free online sales system and website(s).

113. Defendants knowingly published the above-described information to the public on their free online sales system and website(s).

114. Defendants knowingly linked their respective public websites to systems and/or networks storing, maintaining, and/or obtaining Plaintiff's and Class Members' PI.

115. MAPFRE had a practice of offering online insurance quotes to applicants before it incorporated this auto-population feature but added the auto-population feature to its online sales system in order to gain competitive advantage in its sales process. By adding the auto-population feature to its online quoting process, which MAPFRE knowingly chose to do, MAPFRE knew that it was using the driver's license information to sell insurance and making the displayed information easily accessible to anyone who entered basic information into its system. MAPFRE did not impose any security protocols to ensure that website visitors entered and accessed PI only about

themselves. MAPFRE did not impose effective security protocols to prevent automated bots from accessing consumers' PI.

116. During the time period up until, at earliest, July 2023, PI, including drivers' license numbers, of Plaintiff and Class Members, were publicly available and viewable on Defendants' online sales system, and Defendants knowingly obtained, used, and disclosed and/or redisclosed Plaintiff's 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).

117. Pursuant to the allegations herein, MAPFRE knew, inferably knew, or should have known that it obtained, disclosed, and used personal information, from a motor vehicle record, for a purpose not permitted under the DPPA.

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

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

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

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

COUNT II
Negligence
(On Behalf of Plaintiff and the Nationwide Class, or in the alternative, the Massachusetts Class)

122. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

123. Plaintiff brings this cause of action individually and on behalf of the Nationwide Class or, in the alternative, the Massachusetts Class.

124. Defendants owed a duty to Plaintiff and the Class Members to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiff's 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 Plaintiff's and Class Members' PI in Defendants' possession, or that could be accessed by Defendants, was adequately secured and protected.

125. Defendants owed a duty to Plaintiff 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 an unauthorized use of data knowingly disclosed on Defendants' website.

126. Defendants owed a duty of care to Plaintiff 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 PI they stored, maintained, used, accessed, and/or obtained.

127. Defendants further assumed the duty to implement reasonable security measures as a result of their general conduct, internal policies, and procedures, in which MAPFRE states, among other things, that Defendants "always made it a priority to protect your personal and privileged information"; "We limit access to your personal and privileged information to those persons who need to know it to perform their jobs and to provide service to you, and as required or permitted by law"; "We maintain physical and electronic safeguards to protect such information from unauthorized use or disclosure"; "We maintain physical, electronic, and procedural

safeguards to secure your personal information."[33] 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.

128. Unbeknownst to Plaintiff 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 who sell such records. Defendants had an obligation to safeguard Plaintiff's and Class Members' PI and were able to protect against the harm suffered by Plaintiff and Class Members. Instead, Defendants chose to disclose Plaintiff's and Class Members' driver's license numbers and other PI so they could sell more auto insurance.

129. Defendants owed a duty of care to Plaintiff 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 notifying or obtaining consent or authorization from the person whose PI was being provided. Only Defendants were able to ensure that their systems were sufficient to protect against harm to Plaintiff and the Class resulting from a data security incident, instead they chose to disclose Plaintiff's and Class Members' driver's license numbers so they could sell more auto insurance.

130. Defendants' own conduct also created a foreseeable risk of harm to Plaintiff and Class Members and their PI. Defendants' misconduct included failing to adopt, implement, and

[33] MAPFRE, *Privacy Policy*, https://www.mapfreinsurance.com/privacy-policy/ (last visited Sept. 7, 2023).

maintain the systems, policies, and procedures necessary to prevent disclosure of PI. Instead, MAPFRE chose to disclose Plaintiff's and Class Members' driver's license numbers.

131. Defendants acknowledge their conduct created actual harm to Plaintiff and Class Members because Defendants warned of potential fraudulent unemployment benefits claims in their names as a result of their Data Disclosure and offered one year of credit monitoring.

132. 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.

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

134. Defendants breached their duties to Plaintiff and Class Members, and thus were negligent, by failing to adopt, implement, and maintain fair, reasonable, or adequate security measures to safeguard Plaintiff's and Class Members' PI, failing to adequately monitor the security of MAPFRE's online sales system and website, knowingly providing Plaintiff's and Class Members' driver's license information directly to members of the public with small amounts of their PI, failing to recognize in a timely manner that Plaintiff's and Class Members' PI had been disclosed, and failing to warn Plaintiff and Class Members in a timely manner that their PI had been disclosed.

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

136. Defendants acted with wanton disregard for the security of Plaintiff's and Class Members' PI.

137. The injury and harm suffered by Plaintiff 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 that Defendants' breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the disclosure of their PI.

138. Neither Plaintiff nor the other Class Members contributed to MAPFRE's Data Disclosure.

139. As a direct and proximate result of Defendants' conduct, Plaintiff 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 MAPFRE's 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.

140. Defendants acted with wanton disregard for the security of Plaintiff's and Class Members' PI.

141. Plaintiff 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 Plaintiff and the Nationwide Class
or, in the alternative, the Massachusetts Class)

142. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

143. Plaintiff brings this claim individually and on behalf of the Nationwide Class, or in the alternative, the Massachusetts Class.

144. As previously alleged, Plaintiff 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.

145. Defendants owe a duty of care to Plaintiff and Class Members requiring it to adequately secure PI.

146. Defendants still possess and can still access PI regarding Plaintiff and Class Members.

147. Since their Data Disclosure, Defendants have confirmed few changes to their decision to disclose the PI, their data security infrastructure, processes, or procedures to fix the vulnerabilities in their computer systems or online sales system.

148. Defendants' Data Disclosure caused actual harm because of Defendants' failure to fulfill their duties of care to provide security measures to Plaintiff and Class Members. Further,

Plaintiff 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.

149. 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.

150. Plaintiff therefore seeks a declaration (1) that Defendants' existing security measures do not comply with their duties of care to provide adequate security, and (2) that to comply with their duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to:

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 cyber-attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors,

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 instant quote webpage,

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 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.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of the Classes, by and through undersigned counsel, respectfully requests that the Court grant the following relief:

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

B. Award Plaintiff and Class Members actual and statutory damages, punitive damages, and monetary 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 Plaintiff and Class Members pre-judgment and post-judgment interest to the maximum extent allowable;

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

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

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: September 8, 2023

Respectfully submitted,

By: /s/ David Pastor

DAVID PASTOR (BBO 391000)
dpastor@pastorlawoffice.com
PASTOR LAW OFFICE PC
63 Atlantic Avenue, 3rd Floor
Boston, MA 02110
Tel: 617.742.9700
Fax: 617.742.9701

TINA WOLFSON (*pro hac vice* to be filed)
ROBERT AHDOOT (*pro hac vice* to be filed)
AHDOOT & WOLFSON, PC
2600 W. Olive Avenue, Suite 500
Burbank, CA 91505
Telephone: (310) 474-9111
Facsimile: (310) 474-8585
twolfson@ahdootwolfson.com
rahdoot@ahdootwolfson.com

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