UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

RICHARD MA and FRED DEVEREAUX, individually and on behalf of all others similarly situated,	)	Case No.:
Plaintiffs,	)	
v.	)	**JURY TRIAL DEMANDED**
MAPFRE U.S.A. CORP. and THE COMMERCE INSURANCE COMPANY	)	
Defendants.	)	

CLASS ACTION COMPLAINT

Individually and on behalf of others similarly situated, Plaintiffs Richard Ma and Fred Devereaux bring this action against Defendants MAPFRE U.S.A. Corp. (aka "MAPFRE Insurance", the brand and service mark of MAPFRE U.S.A. Corp. and its affiliates) and The Commerce Insurance Company ("Commerce Insurance") (collectively known here as "Defendants" or "MAPFRE"). Plaintiffs' allegations are based upon personal knowledge and acts, and upon information and belief as to all other matters based on the investigation conducted by and through Plaintiffs' attorneys. Plaintiffs believe that substantial additional evidentiary support for the allegations set forth herein exists and will be revealed after a reasonable opportunity for discovery.

I. INTRODUCTION

1. Every year millions of Americans have their valuable personal information stolen and sold online because of unauthorized data disclosures. Despite dire warnings about the severe

impact of unauthorized data disclosures on Americans of all economic strata, companies still fail to put adequate security measures in place to prevent the unauthorized disclosure of private data.

2. Defendants MAPFRE and Commerce Insurance provide insurance products, including car insurance, to Americans across the country. As a part of that business, Defendants collect sensitive personal information from members of the public when they request a quote for Defendants' car insurance products. MAPFRE's website explicitly advertises the information they collect is to "save time" and "save money."

3. This is a class action for damages against Defendants for their failure to exercise reasonable care in securing and safeguarding highly sensitive consumer data in connection with a massive data breach of approximately 266,142 individuals' personal information[1] that started between July 1 and July 2, 2023 (the "Data Breach") and impacted the highly sensitive data, including Plaintiffs' and putative Class Members' (defined below), resulting in the unauthorized public release and subsequent misuse of their driver's license information, including, but not limited to, names, dates of birth, driver's license numbers, and vehicle information including make, model, year, and vehicle identification number (collectively, the "Private Information").

4. MAPFRE collects information from MAPFRE customers and potential customers in fourteen states through six of its national affiliates.

5. To the world of cybercriminals, MAPFRE's Private Information, including the data that was in possession at the time of the Data Breach, is extremely valuable. By accessing Plaintiffs' and Class Members' Private Information, hackers can simply use a driver's license to steal a Class Member's identity. Stolen driver's licenses wreak financial havoc and identity theft issues for MAPFRE potential customers and customers – like Plaintiffs.

[1] https://www.mass.gov/doc/data-breach-report-2023/download at 76.

6. The security of MAPFRE's Private Information is, therefore, of the utmost importance. MAPFRE understood and appreciated the value of this Information by requesting it. yet chose to ignore it by failing to invest in adequate data security measures that would protect Plaintiffs and the Class from the unauthorized access to, and copying of, their Private Information.

7. Defendants readily provided Plaintiffs' and putative Class Members' driver's license and vehicle information to unknown parties from their online quoting platform. Thus, customers and even members of the public who were not MAPFRE customers, but potential customers, may have had sensitive information compromised.

8. Because Defendants access and store personal information—including driver's license numbers—from motor vehicle records as defined by the Drivers' Privacy Protection Act, Defendants are legally required to protect Private Information from unauthorized access and exfiltration.

9. With their Private Information now in the hands of cybercriminals looking to profit from the theft, Plaintiffs' and Class Members' Private Information is no longer secure, causing Plaintiffs and Members of the Class to suffer (and continue to suffer) economic and non-economic harms, as well as a substantial and imminent risk of future economic and non-economic harms.

10. MAPFRE understands the serious nature of data breaches and the potential theft and misuse of MAPFRE's highly sensitive information resulting therefrom, and purports to address these issues. MAPFRE acknowledges on its website that it "has always made it a priority to protect your personal and privileged information. We do not sell your 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."

11. MAPFRE's business model is built on MAPFRE's "accurate information"[2], which places MAPFRE at a heightened risk when unauthorized third parties have access to accurate information.

12. Plaintiffs and Class Members are no longer in possession of their Private Information, as it is no longer hidden but, instead, in the hands of cybercriminals who have already fraudulently misused such data.

13. While the exact reason(s) for the Data Breach remain unclear, there is no doubt that Defendants failed to adequately protect Plaintiffs' and Class Members' Private Information and incorporate the tools necessary to keep such Private Information safe; such negligent failures resulted in the injuries alleged herein.

14. Had Plaintiffs and the Class known that the Private Information they entrusted to Defendants in exchange for the services offered would not be adequately protected, they would not have entrusted their valuable Private Information to Defendants in order to use its product.

15. Thus, on behalf of the Class of victims also impacted by the Data Breach described herein, Plaintiffs seek, under state common law and consumer protection statutes, to redress Defendants' misconduct.

[2] https://www.mapfreinsurance.com/quote-disclosure/ ("A quote is an estimate of what you will pay for an insurance policy on your vehicle. In order to provide you with an accurate quote, we rely on you to provide accurate information. We will determine your actual premium amount, including applicable discounts, and eligibility for coverage once you have completed an insurance application. We may, to the extent allowed by law, verify the information you have provided through third-party providers, including providers of information relating to your driving history.")

II. PARTIES

A. Plaintiff Richard Ma

16. Plaintiff Ma signed up to use MAPFRE insurance in June 2018. In making the decision to entrust his Private Information to MAPFRE, Plaintiff Ma relied upon the data security services and privacy guarantees advertised by Defendants. Plaintiff Ma is a citizen and resident of Massachusetts in Middlesex County.

17. Prior to July 2023, Plaintiff Ma purchased a MAPFRE insurance policy.

18. On or around August 22, 2023, Plaintiff Ma received a data breach notification that an "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."

19. Upon learning of the Data Breach, Plaintiff Ma spent time reconciling how to protect his private information.

20. Plaintiff Ma is very careful about sharing his highly sensitive Private Information.

21. Plaintiff Ma would not have given MAPFRE his Private Information had he known that the sensitive information collected by MAPFRE would be at risk of compromise and misuse due to Defendants' negligent data security practices.

22. Plaintiff Ma has suffered the damages described herein, including but not limited to, loss of time, loss of value of his Private Information, and remains at a significant risk of additional attacks now that his Private Information has been stolen. In addition, Plaintiff Ma and Class Members have also been harmed from the lost value of their privacy; not receiving the benefit of their bargain with Defendants; losing the difference in the value between the services

with adequate data security that Defendants promised and the services actually received; loss of peace and quiet; and loss of the value of the lost time and effort required to mitigate the actual and potential impact of the Data Breach on their lives.

B. Plaintiff Fred Devereaux

23. Plaintiff Devereaux signed up to use Commerce Insurance about 30 years ago, which was later acquired by MAPFRE. Plaintiff Devereaux terminated his Commerce Insurance policy approximately 5 years ago. In making the decision to entrust his Private Information decades ago, Plaintiff Devereaux relied upon basic privacy guarantees. Plaintiff Devereaux is a citizen and resident of Massachusetts in Essex County.

24. Prior to July 2023, Plaintiff Devereaux purchased a MAPFRE insurance policy.

25. On August 29, 2023, Plaintiff Devereaux received a data breach notification that an "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."

26. Upon learning of the Data Breach, Plaintiff Devereaux spent time reconciling how to protect his private information.

27. Plaintiff Devereaux is very careful about sharing his highly sensitive Private Information.

28. Plaintiff Devereaux did not have knowledge that MAPFRE continued to retain his Private Information.

29. Plaintiff Devereaux has suffered the damages described herein, including but not limited to, loss of time, loss of value of his Private Information, and remains at a significant risk

of additional attacks now that his Private Information has been stolen. In addition, Plaintiff Devereaux and Class Members have also been harmed from the lost value of their privacy; not receiving the benefit of their bargain with Defendants; losing the difference in the value between the services *with* adequate data security that Defendants promised and the services actually received; loss of peace and quiet; and loss of the value of the lost time and effort required to mitigate the actual and potential impact of the Data Breach on their lives.

C. Defendant MAPFRE U.S.A Corp.

30. Defendant MAPFRE U.S.A. Corp. (formerly known as The Commerce Group, Inc.) is a domestic profit corporation company organized under the laws of Massachusetts, with its principal place of business in Webster, Massachusetts. MAPFRE insures private passenger automobiles and provides homeowner and other types of insurance for qualified applicants. MAPFRE's affiliates are American Commerce Insurance Company℠ (Columbus, Ohio); Citation Insurance Company℠ (Webster, MA); The Commerce Insurance Company℠ (Webster, MA); Commerce West Insurance Company℠ (California COA No. 06715; San Ramon, CA): MAPFRE Insurance Company℠ (California COA No. 18643; Florham Park, NJ); and MAPFRE Insurance Company of Florida℠ (Miami, FL). MAPFRE had access to users' Private Information and failed to secure the received Private Information or implement data security measures sufficient to ensure the sensitive customer data it stored would be securely handled.

D. Defendant The Commerce Insurance Company

31. The Commerce Insurance Company is a domestic profit corporation company organized under the laws of Massachusetts, with its principal place of business in Webster, Massachusetts. The Commerce Insurance Company is an affiliate of MAPFRE. The Commerce Insurance Company was primarily responsible for the data breach. The Commerce Insurance

Company had access to users' Private Information and failed to secure the received Private Information or implement data security measures sufficient to ensure the sensitive customer data it stored would be securely handled.

III. JURISDICTION AND VENUE

32. Jurisdiction of this Court is founded upon 28 U.S.C. § 1332(d) because the matter in controversy exceeds the value of $5,000,000, exclusive of interests and costs, there are more than 100 class Members, and the matter is a class action in which any member of a class of plaintiffs is a citizen of a different state from any defendant.

33. This Court has personal jurisdiction over this action because Defendants are headquartered in Massachusetts and have thus availed themselves of the rights and benefits of the Commonwealth of Massachusetts by engaging in activities including (i) directly and/or through their parent companies, affiliates and/or agents providing services throughout the United States and in this judicial district and abroad; (ii) conducting substantial business in this forum; (iii) having a registered agent to accept service of process in the Commonwealth of Massachusetts; and/or (iv) engaging in other persistent courses of conduct and/or deriving substantial revenue from services provided in Massachusetts and in this judicial District.

34. Venue is proper in this District under 28 U.S.C. § 1391(b)(1) because Defendants reside within this District and have purposefully engaged in activities, including transacting business in this District and engaging in the acts and omissions alleged herein, in this District.

IV. FACTUAL ALLEGATIONS

A. Defendants' Security Practices "Best Practices" Were Woefully Insufficient to Protect its Users' Private Information from Compromise and Misuse

35. MAPFRE and its affiliates collect customer's Private Information like driver's license numbers, names, vehicle information including make, model, year, and vehicle

identification number, as well as other information.

36. MAPFRE collects both potential customer and customer's Private Information primarily for its business model, including to profit off customer information via behavioral advertising.

37. Potential customer information collected includes name, date of birth, email, phone number, and more.

38. In order to simply obtain a quote, MAPFRE uses potential customer information from third parties to obtain customer's credit, driving claims, and insurance histories.[3]

39. Information collected about potential customers is excessive compared to the history of insurance companies' business practices.

40. MAPFRE collects customers' information including driver's license information. Driver's licenses are crucial identity documents individuals need to have for day to day life, like driving for any reason, obtaining a job, buying a home, accessing healthcare or entering any facility that requires documentation.

41. Despite the sensitivity of driver's license information, MAPFRE's customer information is shared with third parties via behavioral advertising, i.e. commercial information; internet or other similar network activity; geolocation data; sensory data; professional or employment-related information; non-public education information; and/or inferences drawn from other personal information.[4]

42. MAPFRE retains customer Private Information for commercial operations and advertising purposes.[5]

[3] https://quote.mapfreinsurance.com/#contactinfo ("To provide you the most accurate quote possible, we will obtain from third parties information such as your consumer credit, driving, claims and insurance histories.")
[4] MAPFRE Notice to California Consumers mapfreinsurance.com/getnoticecollection/?lang=EN
[5] MAPFRE Notice to California Consumers mapfreinsurance.com/getnoticecollection/?lang=EN

43. MAPFRE held customer information in unsafe and unsecure environments.

B. The Data Breach

44. On August 22, 2023, MAPFRE issued the following notice:

> We are writing to inform you of an incident that involved your personal information and, possibly, information about your vehicle(s). Please read this letter carefully for information about the incident and to learn how you can take steps to help protect yourself against possible misuse of the information, including by means of services being offered through MAPFRE Insurance ("MAPFRE")* for your benefit.
>
> **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.
>
> **What We Are Doing**
>
> As soon as MAPFRE became aware of the issue, we took down our Massachusetts online quoting platform and conducted an investigation to determine what happened. We have implemented additional controls within our system to protect against a reoccurrence of the incident. In addition, MAPFRE has reported the unknown party's illegal activity to law enforcement.
>
> **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.
>
> As a measure of added security and to help protect your identity, we are offering a complimentary 12-month Membership to Experian's® IdentityWorksSM. This product provides you with credit monitoring, identity theft resolution services, and $1,000,000 of identity theft insurance.

> Please review the enclosed instructions to learn how to activate your Membership to Experian's® IdentityWorksSM.
>
> We regret that this incident occurred and any concern it may cause you. If you have additional questions, please call our dedicated, toll-free call center at 833-318-2776, Monday through Friday between 9:00 a.m. and 11:00 p.m. and Saturday and Sunday between 11:00 am and 8:00 pm Eastern Time, excluding major U.S. holidays.
>
> Sincerely,
>
> Steven Shiner
> Senior Vice President, Operations
> MAPFRE U.S.A. Corp.

45. Upon information and belief, the Data Breach involved the data of approximately 266,142 MAPFRE customers.[6]

46. Hackers were able to copy highly sensitive information that included names, driver's license number, make, model, year, and vehicle identification number.

47. During the delay between the data breach in early July and notification in late August, the risks and damages to Plaintiffs and Class Members were only increasing. A prompt and proper response from Defendants, including full disclosure to all MAPFRE customers involved in the Data Breach of the extent of the Breach and the specific information impacted as a result of the Breach, as well as the risks users faced, would have mitigated those risks and resulting damages substantially, as users would have been able to change their impacted drivers' information.

48. Thus, Defendants' disclosure, in addition to being unreasonably delayed, has been woefully inadequate and directly contributed to the damages suffered by Plaintiffs and the Class thus far, and Defendants has yet to offer any remedy to assist Plaintiffs and Class Members

[6] https://www.mass.gov/doc/data-breach-report-2023/download at 76.

through the aftermath of its Breach.

49. Furthermore, the Data Breach exposed the make, model, year, and vehicle identification number. This information is specific enough to find any individual's physical location at any public location the individual chooses to go to, unless they buy or lease a new car.

50. Defendants not only failed to adequately disclose the Data Breach to impacted MAPFRE, but it also failed to explain the extent of the Data Breach, where the information was lost, and to whom it may have been lost.

C. Defendants Violated the FTC Act and Failed to Observe Reasonable and Adequate Data Security Measures

51. Defendants were prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 (the "FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

52. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[7]

53. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses.[8] The guidelines note that businesses should protect the personal customer information that they keep; properly

[7] *Start With Security: A Guide for Business*, FED. TRADE. COMM'N (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf [hereinafter *Start with Security*].
[8] *Protecting Personal Information: A Guide for Business*, FED. TRADE. COMM'N (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

54. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[9]

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

56. Defendants were aware (or should have been aware), at all times, of their obligation to protect the Private Information of Plaintiffs and Class Members because of their position as possessors and controllers of such data. Defendants were also aware of the significant repercussions that would result from its failure to do so.

57. Plaintiffs and Class Members provided their Private Information to Defendants with the reasonable expectation and mutual understanding that Defendants would comply with their obligation to keep such information confidential and secure from unauthorized access.

58. Prior to and during the Data Breach, Defendants understood their practices were not secure, yet collected more information than required anyway for business practices.

[9] *Start with Security*, *supra* note 32.

59. Defendants posted on their website conflicting terms and conditions that they would protect confidential information without guaranteeing security. "While we provide certain internet security technologies and use other reasonable precautions to protect confidential information and provide suitable security, we do not guarantee or warrant that information transmitted through the internet is secure, or that such transmissions will be free from delay, interruption, interception or error."[10]

60. Defendants did not follow industry standard security or data minimization policies.

61. Further, Defendants have been on notice for years that Plaintiffs' and Class Members' Private Information was a target for malicious actors due to, among other reasons, the high value to these bad actors of the Private Information stored in MAPFRE's system. In fact, MAPFRE experienced a data breach in 2021. Additionally, MAPFRE offers cyber insurance to help businesses respond to cyber incidents.[11] Despite such knowledge, Defendants failed to implement and maintain reasonable and appropriate administrative and data security measures to protect Plaintiffs' and Class Members' Private Information from unauthorized access that Defendants should have anticipated and guarded against.

62. Stolen driver's licenses can be used (alone or in combination with other information) by malicious actors to accomplish the following:

• Apply for credit cards

• Apply for financial loans (especially student loans)

• Open bank accounts

[10] https://www.mapfreinsurance.com/terms-conditions/.
[11] https://www.mapfreinsurance.com/blog/why-your-business-needs-cyber-insurance/. (*last accessed September 6, 2023)*.

- Obtain or create fake driver's licenses
    - o Given to police for tickets
    - o Provided to accident victims
    - o Collect government unemployment benefits
    - o Create and sell underage fake IDs
- Replace/access account information on:
    - o LinkedIn
    - o Facebook/Meta
    - o WhatsApp
    - o Instagram
- Obtain a mobile phone
- Dispute or prove a SIM swap
- Redirect U.S. mail
- Apply for unemployment benefits
- Undocumented aliens may use them as a method to gain access to the U.S., and claim a lost or stolen passport
- Create a fake license as a baseline to obtain a Commercial Driver's License
- File tax returns or gain access to filed tax returns
- Engage in phishing and other social engineering scams

63. Almost half of data breaches globally are caused by internal errors relating to either human mismanagement of sensitive information or system errors.[12] Cybersecurity firm Proofpoint reports that since 2020, there has been an increase of internal threats through the

[12] COST OF A DATA BREACH REPORT, *supra* note 8, at 30.

misuse of security credentials or the negligent release of sensitive information.[13] To mitigate these threats, Proofpoint recommends that firms take the time to train their employees about the risks of such errors.[14]

64. As explained by the FBI, "[p]revention is the most effective defense against ransomware and it is critical to take precaution for protection."[15]

65. To prevent and detect unauthorized access to its system, Defendants could have, and should have, implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

> **Secure internet-facing assets**
> - Apply the latest security updates
> - Use threat and vulnerability management
> - Perform regular audit; remove privilege credentials;
>
> **Include IT Pros in security discussions**
> - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;
>
> **Build credential hygiene**
> - use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords
>
> **Apply principle of least-privilege**
> - Monitor for adversarial activities
> - Hunt for brute force attempts
> - Monitor for cleanup of Event Logs
> - Analyze logon events
>
> **Harden infrastructure**
> - Use Windows Defender Firewall

[13] *The Human Factor 2021*, PROOFPOINT (July 27, 2021), https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-human-factor-report.pdf.
[14] *Id.*
[15] *See How to Protect Your Networks from RANSOMWARE*, FBI (2016) https ://www. fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[16]

66. These are basic, common-sense security measures that every business, not only those who handle sensitive information, should be taking. Defendants, with the highly sensitive personal information in its possession and control, should be doing even more. By adequately taking these common-sense solutions, Defendants could have prevented this Data Breach from occurring.

67. Charged with handling sensitive Private Information, Defendants knew, or should have known, the importance of safeguarding the Private Information that was entrusted to them and of the foreseeable consequences of a lapse in their data security. This includes the significant costs that would be imposed on Defendants' users because of a breach. Defendants failed, however, to take adequate administrative cybersecurity measures to prevent the Data Breach from occurring.

68. The Private Information was maintained in a condition vulnerable to misuse. The mechanism of the unauthorized access and the potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Defendants, and thus Defendants were on notice that failing to take reasonable steps necessary to secure the Private Information from those risks left the Private Information in a vulnerable position.

69. As evidenced by these failures by Defendants to comply with their legal obligations established by the FTC Act, as well as their failures to maintain the reasonable and

[16] *See Human-operated ransomware attacks: A preventable disaster*, MICROSOFT (Mar. 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-apreventable-disaster/.

adequate data security measures set forth herein, Defendants failed to properly safeguard Plaintiffs' and Class Members' Private Information, allowing hackers to access and subsequently misuse it.

70. But for Defendants' unlawful conduct, hackers would not have accessed Plaintiffs' and the putative Class Members' Private Information. Defendants' unlawful conduct has directly and proximately resulted in widespread attacks against Plaintiffs and the Class.

71. In addition to these types of threats, Plaintiffs' and Class Members' make, model, year, vehicle identification number, and driver's license number ties and individual to any location they may drive to. The power of Plaintiffs to be anonymous in public is now gone.

72. National credit reporting company blogger, Sue Poremba, emphasized the value of driver's license to thieves and cautioned:

> If someone gets your driver's license number, it is also concerning because it's connected to your vehicle registration and insurance policies, as well as records on file with the Department of Motor Vehicles, place of employment (that keep copy of your driver's license on file), doctor's office, government agencies, and other entities. Having access to that one number can provide an identity thief with several pieces of information they want to know about you. Next to your Social Security number, your driver's license is one of the most important pieces to keep safe from thieves.

73. In fact, according to CPO Magazine, which specializes in news, insights, and resources for data protection, privacy, and cyber security professionals, "[t]o 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.

74. Drivers' license numbers have been taken from auto–insurance providers by hackers in other circumstances, including Geico, Noblr, American Family, USAA, and Midvale all in 2021, indicating both that this specific form of PI is in high demand and also that Defendants knew or had reason to know that their security practices were of particular importance to safeguard consumer data.[17]

75. Plaintiffs and Class Members vehicle and personal information are now in the hands of cybercriminals. The Class as a whole is comprised of a group of people who are at an especially high risk of considering the specificity of a vehicle identification number and driver's license number. This access has resulted in, at minimum, an invasion of Plaintiffs' and Class Members' privacy and can lead to even greater damages, including theft or violent physical attacks.

76. The actions described herein have resulted in emotional distress for Plaintiffs and the Class. Plaintiffs and the Class have lost all security and privacy over important account information, as well as their driver's license number, vehicle identification number, and other contact information that eliminates their right to anonymity in public resulting from the targeted attacks in the Data Breach.

---

[17] See United States Securities and Exchange Commission Form 8-K for INSU Acquisition Corp. II (Feb. 1, 2021), https://www.sec.gov/Archives/edgar/data/1819035/000121390021005784/ea134248-8k_insuacquis2.htm?=1819035-01022021 (accessed Apr. 27, 2021) (announcing a merger with auto-insurance company MetroMile, Inc., an auto-insurer, which announced a drivers' license number Data Disclosure on January 19, 2021); Ron Lieber, How Identity Thieves Took My Wife for a Ride, N.Y. TIMES (Apr. 27, 2021) (describing a scam involving drivers' license numbers and Progressive Insurance).

77. Plaintiffs and the Class are anxious and alert as they are at a substantial risk of being bombarded with phishing emails and other scams, in addition to the disclosure they have already suffered. Plaintiffs are also suffering from the mental and emotional distress associated with such insecurity and uncertainty caused by the Data Breach. Plaintiffs and Class Members attempted to request aid from MAPFRE directly with refusal of assistance from MAPFRE. In addition to financial loss, mental anguish, and risk of future harm, continue to suffer from stress and anxiety as a result of the Data Breach.

78. As long as Plaintiffs' and Class Members' Private Information is in the hands of cybercriminals, they will remain at substantial, imminent risk of continued misuse of their Private Information.

79. Defendants have offered substandard solutions to remedy the damages to Plaintiffs and the Class –the notice given to Plaintiffs and Class Members to enroll in credit monitoring and identity theft insurance requests Plaintiffs and Class Members provide more Private Information that they should not have been bothered to share. The Credit monitoring service proposed cannot guarantee Class Members information security despite requesting it to resolve Defendants' Data Breach. Plaintiffs and Class Members remain at permanent risk unless they take on the significant time and expense to change all of the Private Information that was exposed.

D. Damages to Plaintiffs and the Class

80. Plaintiffs have suffered damages from the Data Breach as set forth herein.

81. Defendants offered insufficient resolution with one-year of Experian Identity Works. In order for Plaintiffs to use Experian Identity Works, they must divulge more Private Information. Experian's Terms and Conditions state they do not guarantee protection of

customer Private Information, they will use it for business use, and that they are not a credit repair organization.

82. If Defendants had disclosed the full extent of the Data Breach in August instead of waiting months to do so, Plaintiffs and Class Members would have been on heightened alert and changed their passwords, thus avoiding the thefts that ensued.

83. As to other forms of damages, Plaintiffs' and Class Members' Private Information has been compromised and they have lost significant time having to sort through and change several accounts and passwords, and in addition, Plaintiffs and Class Members have incurred the following types of damages: the lost value of their privacy; not receiving the benefit of their bargain with Defendants; losing the difference in the value between the services *with* adequate data security that Defendants promised and the services actually received; the value of the lost time and effort required to mitigate the actual and potential impact of the Data Breach on their lives, including, *inter alia*, that required to change multiple account passwords, monitor accounts, and investigate how to maintain privacy from loss of driver's license and vehicle identification information.

84. Additionally, Plaintiffs and Class Members have been put at increased, substantial risk of future fraud and/or misuse of their Private Information, which may take years to manifest, discover, and detect, and may not occur until an attempt to purchase another insurance policy or vehicle.

85. The Data Breach has also exposed make, model, year and vehicle identification number of Plaintiffs and Class Members, which inherently impacts their physical security.

86. Had Plaintiffs been made aware of Defendants' lax data security practices, unwillingness to promptly and completely disclose data breaches such as this one, and failure to

provide timely notice and mitigatory assistance, Plaintiffs would not have agreed to allow his Private Information to be held by Defendants.

87. Defendants require Plaintiffs to resolve problems created by Defendants' lack of security. Other than providing 12–months of credit monitoring, Defendants avoid requests to answer loss of privacy related questions. Defendants do not appear to be taking any measures to assist Plaintiffs and Class Members. None of the recommendations described in the Data Breach Notification required Defendants to expend any effort to protect Plaintiffs' and Class Members' Private Information.

E. The Monetary Value of Privacy Protections and Private Information

88. The fact that Plaintiffs' and Class Members' Private Information was inadvertently disclosed to bad actors that should not have had access to it demonstrates the monetary value of the Private Information.

89. At all relevant times, Defendants understood the Private Information they collect from their users is highly sensitive and of significant property value.

90. Preservation of the confidentiality of Private Information is a valuable property right. The value of the Private Information is axiomatic, considering the value of Big Data in corporate America, as evidenced by MAPFRE's overcollection of data beyond necessary business purposes, and that the consequences of cyber thefts include heavy prison sentences.

91. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly $200 billion. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to insurance companies, that

MAPFRE uses to collect data when providing quotes.[18]

92. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. This transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property.

V. CLASS ALLEGATIONS

93. Plaintiffs brings this Action as a class action pursuant to Fed. R. Civ. P. 23 and seeks certification of the following nationwide Class (referred to herein as the "Class"):

> All persons whose personal information was accessed, compromised, copied, stolen, and/or exposed as a result of the MAPFRE (and any of MAPFRE's affiliates) Data Breach.

94. Excluded from the Class are Defendants, its officers and directors, and Members of their immediate families or their legal representatives, heirs, successors or assigns and any entity in which Defendants has or had a controlling interest.

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

96. Numerosity—Federal Rule of Civil Procedure 23(a)(1). The Members of the Class are so numerous that joinder of all Class Members would be impracticable. Upon information and belief, the Class numbers in the millions. Moreover, the Class is composed of an easily ascertainable set of MAPFRE customers who were thus impacted by the Data Breach. The precise number of Class Members can be further confirmed through discovery, which includes Defendants' records. The disposition of Plaintiffs' and Class Members' claims through a class

[18] https://quote.mapfreinsurance.com/#contactinfo.

action will benefit the parties and this Court.

97. **Commonality and Predominance—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all Members of the Class and predominate over questions affecting only individual Members of the Class. Such common questions of law or fact include, *inter alia*:

- Whether Defendants' data security systems and/or protocol prior to and during the Data Breach complied with applicable data security laws and regulations;
- Whether Defendants' data security systems and/or protocol prior to and during the Data Breach were consistent with industry standards and best practices;
- Whether Defendants properly implemented their purported security measures to protect Plaintiffs' and Class Members' Private Information from unauthorized capture, dissemination, and misuse;
- Whether Defendants took reasonable measures to determine the extent of the Data Breach after it first learned of same;
- Whether Defendants disclosed Plaintiffs' and Class Members' Private Information in violation of the understanding that the Private Information was being disclosed in confidence and should be maintained;
- Whether Defendants willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiffs' and the Class Members' Private Information;
- Whether Defendants were negligent in failing to properly secure and protect Plaintiffs' and the Class's Private Information;
- Whether Defendants were unjustly enriched by their actions; and
- Whether Plaintiffs and Class Members are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

98. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs, on behalf of themselves and other Members of the Class. Similar or identical common law violations, business practices, and injuries are involved.

Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that predominate in this action.

99. **Typicality—Federal Rule of Civil Procedure 23(a)(3).** Plaintiffs' claims are typical of the claims of the other Members of the Class because, among other things, all Class Members were similarly injured and sustained similar monetary and economic injuries as a result of Defendants' uniform misconduct described herein and were thus all subject to the Data Breach alleged herein. Further, there are no defenses available to Defendants that are unique to Plaintiffs.

100. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4).** Plaintiffs are an adequate representative of the Class because their interests do not conflict with the interests of the Class they seek to represent, they retained counsel competent and experienced in complex class action litigation, and they will prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiffs and their counsel.

101. **Injunctive Relief—Federal Rule of Civil Procedure 23(b)(2).** Defendants acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. Civ. P. 23 (b)(2).

102. **Superiority—Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiffs and the other Members of the Class are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be impracticable for Members of the Class to individually seek redress for Defendants' wrongful conduct. Even if Members of

the Class could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

103. Class certification is also appropriate under Rules 23(b)(1) and/or (b)(2) because:

- The prosecution of separate actions by the individual Members of the Class would create a risk of inconsistent or varying adjudications establishing incompatible standards of conduct for Defendants;
- The prosecution of separate actions by individual Class Members would create a risk of adjudication that would, as a practical matter, be dispositive of the interests of other Class Members not parties to the adjudications, or would substantially impair or impede their ability to protect their interests; and
- Defendants have acted and refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief with respect to the Members of the Class as a whole.

104. Class certification is also appropriate because this Court can designate particular claims or issues for class-wide treatment and may designate multiple subclasses pursuant to Fed. R. Civ. P. 23(c)(4).

105. No unusual difficulties are likely to be encountered in the management of this action as a class action.

COUNT I
VIOLATION OF THE DRIVERS' PRIVACY PROTECTION ACT ("DPPA"), 18 U.S.C. § 2724
(On behalf of Plaintiffs and the Class)

106. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

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. 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(a). And the DPPA's definition of "personal information" includes an individual's driver identification number, commonly referred to as a driver's license number. 18 U.S.C. § 2725(3). Therefore, drivers' license numbers that are maintained as a part of a database of DMV records are motor vehicle records, and part of the personal information intended to be protected under the DPPA.[19]

109. Defendants also obtain motor vehicle records directly from customers to cross-reference with third parties, state agencies, or through resellers. During the time period up until and including at least August 2023, Private Information, including drivers' license numbers, of Plaintiffs and Class Members, were available to unknown parties. Defendants knowingly both used and disclosed Plaintiffs' and Members of the class's motor vehicle records for a purpose not permitted by the DPPA pursuant to 18 U.S.C. §§ 2724 and 2721(b).

110. Because of Defendants' violations of the DPPA, Plaintiffs and putative Class Members are entitled to actual damages, liquidated damages, punitive damages, attorneys' fees and costs.

[19] "Personal information is 'from' a motor vehicle record when it derives from state DMV sources." (Pub. Int. Legal Found. v. Boockvar, 431 F. Supp. 3d 553, 562 (M.D. Pa. 2019), citing Dahlstrom v. Sun-Times Media, LLC, 777 F.3d 937, 949 (7th Cir. 2015); Whitaker v. Appriss, Inc., No. 3:13-CV-826, 2014 WL 4536559, at *3 (N.D. Ind. Sept. 11, 2014) (citation omitted); Andrews v. Sirius XM Radio Inc., 932 F.3d 1253, 1260 n.5 (9th Cir. 2019); *Siegler v. Best Buy Co. of Minn.*, 519 F. App'x 604, 605 (11th Cir. 2013)). It is irrelevant that the information does not take the form of a "motor vehicle record," and the DPPA protects "information" held by the DMV and supplied in connection with a motor vehicle record. (*Id.*; *see* 18 U.S.C. § 2721.). DPPA applies to personal information acquired from a state DMV. *Hatch v. Demayo*, No. 1:16CV925, 2021 WL 231245, at *6 (M.D.N.C. Jan. 22, 2021).

COUNT II
NEGLIGENCE
(On Behalf of Plaintiffs and the Class)

111. Plaintiffs incorporate the preceding paragraphs as though fully set forth herein.

112. Upon Defendants' acceptance and storage of Plaintiffs' and Class Members' Private Information in its system, Defendants undertook and owed a duty to Plaintiffs and the Class to exercise reasonable care to secure and safeguard that Information and to use commercially reasonable methods to do so. Defendants knew that the Private Information was highly sensitive and confidential and should be protected as such.

113. Defendants owed a duty of care to provide security consistent with federal law and industry standards, to ensure their systems protected Class Members Private Information; and not to subject Plaintiffs' and other Class Members' Private Information to an unreasonable risk of exposure and theft because Plaintiffs and other Class Members were foreseeable and probable victims of any inadequate data security practices.

114. Unbeknownst to Plaintiffs and Class Members, they were entrusting Defendants with their Private Information when Defendants obtained their Private Information—including but not limited to their driver's license numbers—from motor vehicle department records and other businesses. Defendants had an obligation to safeguard their information and was in a position to protect against the harm suffered by Plaintiffs and Members of the Class as a result of the Data Breach.

115. Defendants owed numerous duties to Plaintiffs and the Class, including the following:

- to exercise reasonable care in obtaining, retaining, securing, safeguarding, and protecting Private Information in its possession;

- to protect Private Information using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and
- to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

116. Defendants also breached their duty to Plaintiffs and other Class Members to adequately protect and safeguard Private Information by disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Private Information to unknown parties. Furthering its dilatory practices, Defendants failed to provide adequate supervision and oversight of the Private Information with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of compromise and misuse, which permitted malicious bad actors to gather Plaintiffs' and Class Members' Private Information and intentionally disclose it to others and/or misuse it without consent, resulting in the harms alleged herein.

117. Defendants knew, or should have known, of the risks inherent in collecting and storing Plaintiffs' and Class Members' Private Information and the importance of adequate data security.

118. Defendants knew, or should have known, that its data systems and privacy protocols and procedures would not adequately safeguard Plaintiffs' and Class Members' Private Information.

119. Defendants breached its duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems, networks, and/or data security practices to safeguard Plaintiffs' and Class Members' Private Information.

120. Because Defendants knew that the theft of the highly sensitive data stored in its

systems would damage millions of individuals and businesses, including Plaintiffs and Class Members, Defendants had a duty to implement sufficient privacy practices and procedures and adequately protect its data systems and the Private Information contained therein.

121. Defendants' duty of care to use reasonable data security measures arose as a result of the special relationship that existed between Defendants and Plaintiffs and Class Members, which is recognized by laws and regulations, including but not limited to, common law. Defendants were in a position to ensure that its systems and protocols were sufficient to protect against the foreseeable risk of harm to Class Members from the compromise of the data with which it was entrusted.

122. In addition, Defendants had a duty to employ reasonable data security measures under Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable data security measures to protect confidential data.

123. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described herein, but also because Defendants were bound by industry standards to do more to protect the confidential data that was compromised as a result of the Data Breach.

124. Defendants' own conduct also created a foreseeable risk of harm to Plaintiffs and Class Members and their Private Information. Defendants' misconduct included failing to (1) secure Plaintiffs' and Class Members' Private Information; (2) comply with industry standard security practices; (3) implement adequate system and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent the Data Breach.

125. Defendants breached their duties, and thus were negligent, by failing to use

reasonable measures to protect Class Members' Private Information, and by failing to provide timely notice of the Data Breach. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

- Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;
- Failing to adequately monitor the security of its networks and systems;
- Allowing unauthorized access to Class Members' Private Information;
- Encouraging exposure of Class Members' Private Information by cross-referencing with third-parties as a business model;
- Failing to detect in a timely manner that Class Members' Private Information had been compromised; and
- Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for fraud and other damages.

126. Through Defendants' acts and omissions described in this Complaint, including its failure to provide adequate data security and protect Plaintiffs' and Class Members' Private Information from being foreseeably accessed, stolen, disseminated, and misused, Defendants unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiffs' and Class Members' Private Information during the time it was within Defendants' possession and control.

127. Defendants' conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to, failing to adequately protect the Private Information, and failing to provide Plaintiffs and Class Members with timely notice that their sensitive Private Information had been compromised.

128. Neither Plaintiffs nor Class Members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint. Any and all actions taken by Plaintiffs and Class Members which Defendants may argue contributed to the misuse of the compromised Private Information were reasonable under the circumstances.

129. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members suffered damages as alleged herein.

130. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to (i) strengthen its data security systems and monitoring procedures; and (ii) submit to future bi-annual audits of those systems and monitoring procedures.

COUNT III
BREACH OF CONTRACT/BREACH OF IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING
(On Behalf of Plaintiffs and the Class)

131. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

132. Plaintiffs and Class Members entered into valid and enforceable express contracts with Defendants under which Plaintiffs and Class Members agreed to provide their Private Information to Defendants, and Defendants agreed to provide confidential services that included the implementation of adequate data security standards, protocols, and procedures to ensure the protection of Plaintiffs' and Class Members' Private Information.

133. In every contract entered into between Plaintiffs and Class Members and Defendants, including those at issue here, there is an implied covenant of good faith and fair dealing obligating the parties to refrain from unfairly interfering with the rights of the other party or parties to receive the benefits of the contracts. This covenant of good faith and fair dealing is applicable here as Defendants were obligated to protect (and not interfere with) the privacy and

protection of Plaintiffs' and Class Members' Private Information.

134. To the extent Defendants' obligation to protect Plaintiffs' and Class Members' Private Information was not explicit in those express contracts, the contracts also included implied terms requiring Defendants to implement data security adequate to safeguard and protect the confidentiality of Plaintiffs' and Class Members' Private Information, including in accordance with trade regulations, federal, state and local laws, and industry standards. No customer would have entered into these contracts with Defendants without the understanding that their Private Information would be safeguarded and protected; stated otherwise, data security was an essential term of the parties' contracts.

135. Indeed, Defendants' Terms of Service obfuscate their privacy policy by adding a hyperlink and incorporating the Privacy Policy "by reference."[20]

136. Defendants' Privacy Policy claims, "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."[21]

137. Defendants' Privacy Policy acknowledges, " As we deem appropriate, we use security measures consistent with industry standards, such as firewalls and encryption technology, to protect your information."

138. Plaintiffs and Class Members agreed, among other things, to provide their Private Information in exchange for Defendants' services.

139. The protection of Plaintiffs' and Class Members' Private Information is a

[20] https://www.mapfreinsurance.com/terms-conditions/ (last accessed September 1, 2023).
[21] https://www.mapfreinsurance.com/privacy-policy/ (last accessed September 1, 2023).

material aspect of Plaintiffs' and Class Members' contracts with Defendants.

140. Defendants' promises and representations described above relating to industry standards and Defendants' purported concern about its users' privacy rights are express terms of the contracts between Defendants, including Plaintiffs and Class Members. Defendants breached these promises by failing to comply with reasonable industry practices.

141. Plaintiffs and Class Members read, reviewed, and/or relied on statements made by or provided by Defendants and/or otherwise understood that Defendants would protect its MAPFRE's Private Information if that information were provided to Defendants.

142. Plaintiffs and Class Members fully performed their obligations under their contracts with Defendants; however, Defendants did not.

143. As a result of Defendants' breach of these terms, Plaintiffs and Class Members have suffered a variety of damages including but not limited to: the lost value of their privacy; not receiving the benefit of their bargain with Defendants; losing the difference in the value between the services *with* adequate data security that Defendants promised and the services actually received; the value of the lost time and effort required to mitigate the actual and potential impact of the Data Breach on their lives, including, inter alia, that required to change multiple account passwords, monitor accounts, and investigating how to protect themselves. Additionally, Plaintiffs and Class Members have been put at increased risk of future fraud and/or misuse of their Private Information, which may take years to manifest, discover, and detect.

144. Plaintiffs and Class Members are therefore entitled to damages, including restitution and unjust enrichment, disgorgement, declaratory and injunctive relief, and attorney fees, costs, and expenses.

COUNT IV
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Class)

145. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

146. Plaintiffs bring this claim alternatively to his claim for breach of contract.

147. Through its course of conduct, Defendants entered into implied contracts with Plaintiffs and Class Members for the provision of password and identity management services, as well as implied contracts for Defendants to implement data security practices adequate to safeguard and protect the privacy of Plaintiffs' and Class Members' Private Information.

148. Specifically, Plaintiffs entered into valid and enforceable implied contracts with Defendants when they first began using Defendants' services.

149. The valid and enforceable implied contracts to provide confidential services that Plaintiffs and Class Members entered into with Defendants include Defendants' promise to protect nonpublic Private Information entrusted to it.

150. When Plaintiffs and Class Members provided their Private Information to Defendants in exchange for Defendants' services, they entered into implied contracts with Defendants pursuant to which Defendants agreed to reasonably protect such information.

151. Defendants solicited and invited Plaintiffs and Class Members to provide their Private Information as part of Defendants' regular business practices. Plaintiffs and Class Members accepted Defendants' offer and provided their Private Information to Defendants.

152. By entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendants' data security practices complied with relevant laws and regulations and were consistent with industry standards.

153. Under these implied contracts, Defendants promised and were obligated to: (a) protect Class Members drivers' license and vehicle information (b) provide services inclusive of protecting Private Information to Plaintiffs' and Class Members; and (c) protect Plaintiffs' and the Class Members' Private Information provided to obtain such benefits of such services. In exchange, Plaintiffs and Members of the Class agreed to turn over their Private Information to Defendants.

154. Both the provision of services and the protection of Plaintiffs' and Class Members' Private Information were material aspects of these implied contracts.

155. The implied contracts for the provision of services, including but not limited to, the maintenance of the privacy of Plaintiffs' and Class Members' Private Information, are also acknowledged, memorialized, and embodied in Defendants' Terms of Service for personal users.

156. Defendants' express representations, including, but not limited to, the express representations found in its Terms of Service, memorialize and embody the implied contractual obligations requiring Defendants to implement data security adequate to safeguard and protect the privacy of Plaintiffs and Class Members, and to protect the privacy of Plaintiffs' and Class Members' Private Information.

157. Users of password management services value their privacy and the ability to keep their Private Information associated with obtaining such services. Plaintiffs and Class Members would not have entrusted their Private Information to Defendants and entered into these implied contracts with Defendants without an understanding that their Private Information would be safeguarded and protected; nor would they have entrusted their Private Information to Defendants in the absence of the implied promise by Defendants to monitor the Private Information and to ensure that it adopted reasonable administrative and data security measures.

158. Plaintiffs and Class Members agreed and provided their Private Information to Defendants in exchange for, among other things, both the provision of confidential services and the protection of their Private Information.

159. Plaintiffs and Class Members performed their obligations under the contract when they turned over their Private Information to Defendants.

160. Defendants materially breached its contractual obligation to protect the nonpublic Private Information it gathered when the Private Information was compromised and subsequently misused as a result of the Data Breach.

161. Defendants materially breached the terms of these implied contracts, including, but not limited to, the terms stated in the relevant Terms of Service. Defendants did not maintain the privacy of Plaintiffs' and Class Members' Private Information as evidenced by its recent notices of the Data Breach posted on its blog. Specifically, Defendants did not comply with industry standards, standards of conduct embodied in statutes like Section 5 of the FTCA, or otherwise protect Plaintiffs' and Class Members' Private Information as set forth above.

162. The Data Breach was a reasonably foreseeable consequence of Defendants' data security failures in breach of these contracts.

163. As a result of Defendants' failure to fulfill the data security protections promised in these contracts, Plaintiffs and Class Members did not receive the full benefit of their bargain with Defendants, and instead received services that were of a diminished value to that described in the contracts. Plaintiffs and Class Members therefore were damaged in an amount at least equal to the difference in the value of the insurance accounts *with* data security protection that Defendants agreed to provide and the services Defendants actually provided.

164. Had Defendants disclosed their administrative and data security measures were

inadequate or that it did not adhere to industry-standard security measures, neither Plaintiffs, Class Members, nor any reasonable person would have utilized services from Defendants.

165. As a direct and proximate result of the Data Breach, Plaintiffs and Class Members have been harmed and suffered, and will continue to suffer, actual damages and injuries, including without limitation, the release and disclosure of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the future, out of pocket expenses, and the loss of the benefit of the bargain they struck with Defendants.

166. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

167. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to, *e.g.*, strengthen their data security systems and monitoring procedures, and immediately take on the burden of long-term, adequate credit monitoring to all Class Members.

COUNT V
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class)

168. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

169. Plaintiffs and Class Members conferred a monetary benefit on Defendants. Specifically, they provided Defendants with their Private Information. In exchange, Plaintiffs and Class Members should have received from Defendants the services that were the subject of the transaction and were entitled to have Defendants protect their Private Information with adequate data security.

170. Defendants knew and appreciated that Plaintiffs and Class Members conferred a

benefit on them and accepted and retained that benefit. Defendants profited from Plaintiffs' and Class Members' providing their Private Information for Defendants' business purposes.

171. Defendants failed to secure Plaintiffs' and Class Members' Private Information and, therefore, did not provide full compensation for the benefit that Plaintiffs' and Class Members' Private Information provided.

172. Defendants acquired the Private Information through inequitable means as it failed to disclose the inadequate security practices alleged herein.

173. If Plaintiffs and Class Members knew that Defendants did not have data security safeguards in place that were adequate to secure their Private Information from unauthorized access, they would not have used Defendants' services.

174. Under the circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiffs and Class Members conferred upon it.

175. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds in the amount of the benefits that it unjustly received from them by way of possessing and controlling Plaintiffs' and Class Members' Private Information.

176. This claim is being asserted in the alternative to Plaintiffs' claims for breach of contract.

COUNT VI
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Class)

177. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

178. Plaintiffs and Class Members have an interest, both equitable and legal, in the

Private Information that was conveyed to and collected, stored, and maintained by Defendants and which was ultimately compromised by unauthorized cybercriminals as a result of the Data Breach.

179. Defendants, in taking possession of this highly sensitive information, have a special relationship with Plaintiffs and the Class. As a result of that special relationship, Defendants were provided with and stored private and valuable information belonging to Plaintiffs and the Class, which Defendants were required by law and industry standards to maintain in confidence.

180. In light of the special relationship between Defendants and Plaintiffs and Class Members, whereby Defendants became a guardian of Plaintiffs' and Class Members' Private Information, Defendants became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its cusmoters, including Plaintiffs and Class Members, for the safeguarding of Plaintiffs' and Class Members' Private Information.

181. Defendants had a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of this relationship, in particular, to keep secure Plaintiffs' and Class Members' Private Information and to maintain the confidentiality of their Private Information.

182. Defendants owed a duty to Plaintiffs' and Class Members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Private Information in its possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

183. Plaintiffs and Class Members have a privacy interest in their personal and proprietary matters and Defendants had a duty not to disclose such confidential information.

184. Plaintiffs' and Class Members' Private Information is not generally known to the public and is confidential by nature. Moreover, Plaintiffs and Class Members did not consent to nor authorize Defendants to release or disclose their Private Information to unknown criminal actors.

185. Defendants breached its fiduciary duty to Plaintiffs' and Class Members when Plaintiffs' and Class Members' Private Information was disclosed to unknown criminal hackers by way of Defendants' own acts and omissions, as alleged herein.

186. Defendants knowingly breached its fiduciary duties by failing to safeguard Plaintiffs' and Class Members' Private Information, including by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of the Private Information; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the Breach at the time it began or within a reasonable time thereafter and give adequate notice to Plaintiffs and Class Members thereof; (g) failing to follow its own privacy policies and practices published online; (h) storing Private Information in an unencrypted and vulnerable manner, allowing its disclosure to hackers; and (i) making an unauthorized and unjustified disclosure and release of Plaintiffs' and Class Members' Private Information to a criminal third party.

187. But for Defendants' wrongful breach of its fiduciary duties owed to Plaintiffs and

Class Members, their privacy would not have been compromised and their Private Information would not have been accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by and/or viewed by unauthorized third parties.

188. As a direct and proximate result of Defendants' breach of its fiduciary duties, Plaintiffs and Class Members have suffered or will suffer injuries, including but not limited to, the following: loss of their privacy and confidentiality of their Private Information; theft of their Private Information; costs associated with the detection and prevention of fraud and unauthorized use of their Private Information; costs associated with purchasing credit monitoring and identity theft protection services; loss of time and costs associated with investigating purchase of vehicle or insurance; costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Defendants' Data Breach – including finding fraudulent charges, enrolling in credit monitoring and identity theft protection services, and filing reports with the police and FBI; the imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their Private Information being placed in the hands of criminals; damages to and diminution in value of their Private Information entrusted, directly or indirectly, to Defendants with the mutual understanding that Defendants would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others; continued risk of exposure to hackers and thieves of their Private Information, which remains in Defendants' possession and is subject to further breaches so long as Defendants fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data; and/or mental anguish accompanying the loss of confidence and disclosure of their Private Information.

189. Defendants breached their fiduciary duty to Plaintiffs' and Class Members when they made an unauthorized release and disclosure of their confidential Private Information and, accordingly, it would be inequitable for Defendants to retain the benefits they have received at Plaintiffs' and Class Members' expense.

190. Plaintiffs and Class Members are entitled to damages and/or disgorgement or restitution, in an amount to be proven at trial.

COUNT VII
DECLARATORY JUDGMENT AND INJUNCTIVE RELIEF
(On Behalf of Plaintiffs and the Class)

191. Plaintiffs fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

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

193. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' present and prospective duties to reasonably safeguard users' Private Information and whether Defendants are maintaining data security measures adequate to protect the Class Members, including Plaintiffs, from further data breaches that compromise their Private Information, including but not limited to, their respective customer accounts.

194. Plaintiffs allege that Defendants' data-security measures remain inadequate. In addition, Plaintiffs and the Class continue to suffer injury as a result of the compromise of their Private Information and remain at imminent risk that further compromises of their Private Information and continued fraudulent activity against them will occur in the future.

195. Pursuant to its authority under the Declaratory Judgment Act, Plaintiffs asks the Court to enter a judgment declaring, among other things, the following: (i) Defendants owe a duty to secure consumers' Private Information and to timely notify consumers of a data breach under the common law, the DDPA, and Section 5 of the FTC Act; and (ii) Defendants are in breach of these legal duties by failing to employ reasonable measures to secure consumers' Private Information in their possession and control.

196. Plaintiffs further ask the Court to issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with law and industry standards to protect consumers' Private Information from future data breaches.

197. If an injunction is not issued, the Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at MAPFRE. The risk of another such breach is real, immediate, and substantial. If another breach at MAPFRE occurs, the Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and Class Members will be forced to bring multiple lawsuits to rectify the same misconduct.

198. The hardship to the Class Members if an injunction does not issue exceeds the hardship to Defendants if an injunction is issued. Among other things, if a similar data breach occurs again due to the repeated misconduct of Defendants, the Class Members will likely be subjected to substantial hacking and phishing attempts and other damage, in addition to the damages already suffered. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have pre-existing legal obligations to employ such measures.

199. Issuance of the requested injunction will not disserve the public interest. To the

contrary, such an injunction would benefit the public by preventing additional data breaches at MAPFRE, thus eliminating the additional injuries that would result to the Class Members and the millions of consumers whose personal and confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the Class proposed in this Complaint, respectfully request that the Court enter judgment in favor of Plaintiffs and the Class and against Defendants, as follows:

A. For an Order certifying this action as a class action and appointing Plaintiffs and their counsel to represent the Class;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to Defendants' lax data security practices, procedures, networks, and systems that led to the unauthorized disclosure and subsequent misuse of Plaintiffs' and Class Members' Private Information, and from failing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;

C. For equitable relief compelling Defendants to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity all types of Private Information compromised during the Data Breach;

D. For equitable relief requiring restitution and disgorgement of the benefits wrongfully retained by Defendants as a result of its wrongful conduct;

E. For an award of damages, compensatory damages and/or restitution or disgorgement, in an amount to be determined, as allowable by law;

F. For an award of attorneys' fees and costs, and any other expense, including expert

witness fees;

G. Pre- and post-judgment interest on any amounts awarded; and

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

JURY DEMAND

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

Date: September 6, 2023

Respectfully Submitted,

/s/ *Patrick J. Sheehan*

Patrick J. Sheehan (BBO# 639320)
WHATLEY KALLAS LLP
101 Federal Street, 19th Floor
Boston, Massachusetts 02110
Telephone: (617) 203-8459
Facsimile: (800) 922-4851
psheehan@whatleykallas.com

Nicholas A. Migliaccio*
Jason S. Rathod*
MIGLIACCIO & RATHOD, LLP
412 H Street, NE, Suite 302
Washington, DC 20002
Phone: 202-470-520
Fax: 202-800-2730
nmigliaccio@classlawdc.com
jrathod@classlawdc.com

Counsel for Plaintiffs and the Putative Class

*To apply for admission *pro hac vice*

ClassAction.org
