UNITED STATES DISTRICT COURT
DISTRICT OF MARYLAND
Southern Division

Ryant Connelly
5006 Cascade Drive
Corpus Christi, Texas 78413

and

Belen Perez
340 W 12th Street
Falfurrias TX 78355

individually and on behalf of others similarly situated,

Plaintiffs,

v.

Berkshire Hathaway, Inc.,
3555 Farnam Street
Omaha, NE 68131

Government Employees Insurance Company
(a/k/a GEICO)
5260 Western Ave
Chevy Chase, MD 20815
(Montgomery County)

GEICO Casualty Company,
5260 Western Ave,
Chevy Chase, MD 20815
(Montgomery County)

GEICO Indemnity Company
5260 Western Ave.
Chevy Chase, MD 20815
(Montgomery County)

GEICO General Insurance Company,
5260 Western Ave.
Chevy Chase, MD 20815
(Montgomery County)

Defendants.

CASE NO. 8:21-cv-1152

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiffs Ryant Connelly and Belen Perez ("Plaintiffs"), individually and on behalf of all others similarly situated (the "Class" or "Class Members"), bring this Class Action Complaint against Defendants Berkshire Hathaway, Inc., Government Employees Insurance Company (a/k/a GEICO), GEICO Casualty Company, GEICO Indemnity Company, and GEICO General Insurance Company (collectively "GEICO" or "Defendants"), based on their individual experiences and personal information, and investigation by their counsel.

INTRODUCTION

1. Plaintiffs, individually and on behalf of all others similarly situated, bring this class action suit against Defendants because of Defendants' failure to safeguard the Personal Identifying Information ("PII") of millions of current and former GEICO customers. The compromised PII appears to be, at a minimum, information typically contained on Class Members' drivers' licenses, including drivers' license numbers.

2. GEICO is a nationwide automobile insurance company headquartered in Chevy Chase, Maryland that is a wholly owned subsidiary of Berkshire Hathaway, Inc., a conglomerate holding company headquartered in Omaha, Nebraska. With at least seventeen million policy holders, GEICO is one of the largest auto insurers in United States. GEICO collects a significant amount of data from its current and former policy holders, often including sensitive personal information obtained in the context of an insurance relationship, including Social Security numbers, addresses, telephone numbers, date of birth, bank account numbers, credit card numbers, financial transaction records, credit ratings and driver's license numbers. Due to its size and the nature of its business, GEICO stores what hackers would consider a veritable treasure trove of PII from GEICO customers, including Plaintiffs and Class Members.

3. On or about April 9, 2021, GEICO announced by letters entitled "Notice of Data Disclosure" to its policy holders that between November 24, 2020 and March 1, 2021, GEICO's website had provided unauthorized access to policyholders' driver's license numbers and that said information could be used to fraudulently apply for unemployment benefits in such policyholders' names (the "Data Disclosure"). The information accessed appears to have been information on Plaintiffs' and Class Members' driver's licenses.

4. The confidential information that GEICO revealed in the Data Disclosure can be used to gain unlawful access to the users' home addresses, legal names, and other online accounts. It can also be used to carry out identity theft or commit other fraud. And, it can be sold to those who broker and traffic in stolen PII and be disseminated on the internet.

5. Drivers' licenses are particularly valuable PII. According 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. In this case, GEICO stated that 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."

6. Drivers' license numbers have been taken from auto-insurance providers by hackers in other circumstances, indicating both that this particular form of PII is in high demand and also that GEICO knew or had reason to know that its security practices were of particular importance to safeguard consumer data.[1]

7. The Data Disclosure could have been avoided through basic security measures, authentications, and training.

8. At all relevant times, Defendants promised and agreed in various documents to safeguard and protect Plaintiffs' and Class Members' PII in accordance with federal, state, and local laws, and industry standards. Defendants made these promises and agreements on their websites and other written notices and also extended this commitment to situations in which third parties handled PII on their behalf.

9. Contrary to these promises, and despite the fact that the threat of a Data Disclosure has been a well-known risk to Defendants, especially due to the valuable and sensitive nature of the data Defendants collect, store and maintain, Defendants failed to take reasonable steps to adequately protect the PII of GEICO's current and former policyholders. The Data Disclosure was

[1] *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).

a direct result of Defendants' failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect PII.

10. As a result of Defendants' failure to take reasonable steps to adequately protect the PII of current and former GEICO policyholders, Plaintiffs' and Class Members' PII was readily available on the internet for anyone and everyone to acquire, access, and use for unauthorized purposes for the foreseeable future.

11. Defendants' failure to implement and follow basic security procedures has resulted in ongoing harm to Plaintiffs and Class Members who will continue to experience a lack of data security for the indefinite future and remain at serious risk of identity theft and fraud that would result in significant monetary loss and loss of privacy.

12. Accordingly, Plaintiffs seek to recover damages and other relief resulting from the Data Disclosure, including but not limited to, compensatory damages, reimbursement of costs that Plaintiffs and others similarly situated will be forced to bear, and declaratory judgment and injunctive relief to mitigate future harms that are certain to occur in light of the scope of this breach.

JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction 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 Plaintiffs and Defendants are citizens of different states. The Court also has federal question jurisdiction under 28 U.S.C. § 1331 for the Drivers' Privacy Protection Act claims. Subject matter jurisdiction is also based upon the Federal Trade Commission Act (FTCA). This Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

14. This Court has personal jurisdiction over Defendants as they conduct substantial business in this State and in this District and/or the conduct complained of occurred in and/or emanated from this State and District because the confidential information compromised in the Data Disclosure was likely stored and/or maintained in accordance with practices emanating from this District.

15. Venue is proper pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to the conduct alleged in this Complaint occurred in, were directed to, and/or emanated from this District, and because Defendants reside within this District.

THE PARTIES

16. Plaintiff Ryant Connelly is a GEICO policyholder residing in Corpus Christi, Texas, who received a notice that his data may have been disclosed and used by someone to apply for unemployment.

17. Plaintiff Belen Perez is a GEICO policyholder residing in Falfurrias, Texas, who received a notice that her data may have been disclosed and used by someone to apply for unemployment.

18. Defendant GEICO is an insurance company, a wholly owned subsidiary of Defendant Berkshire, with its headquarters located in Chevy Chase, Maryland. Defendants GEICO Casualty Company, GEICO Indemnity Company, GEICO General Insurance Company, and Government Employees Insurance Company are Maryland corporations with their principal places of business in Chevy Chase, Maryland.

19. Defendant Berkshire is a domestic business corporation, organized and existing by virtue of the laws of the State of New York, headquartered in Omaha, Nebraska.

20. At all relevant times, Defendants were and are engaged in business in the District of Maryland and throughout the United States of America.

FACTUAL ALLEGATIONS

21. At all pertinent times, Plaintiffs were policyholders of insurance written by GEICO. In the course of purchasing insurance, Plaintiffs were required to provide certain personal and financial information to GEICO, including name, address, Social Security number, vehicle information, and driver's license number.

22. On or about **April 9, 2021**, Defendant GEICO advised Plaintiffs by letter (the "Notice") that personal information illegally obtained from other sources had been used to obtain unauthorized access to their driver's license numbers through the online sales system on GEICO's website, and that said information could be used to fraudulently apply for unemployment benefits in such policyholders' names (the "Data Disclosure"). The information accessed appears to have been the plaintiffs' driver's licenses, drivers' license number, legal names, addresses, etc.

23. On April 15, 2021, GEICO filed a redacted copy of the Notice with the California Office of the Attorney General revealing that its customers' PII was subject to a data security breach between January 21, 2021 and March 1, 2021.[2] More specifically, in the Notice, GEICO revealed that fraudsters used information about GEICO's customers to hack into GEICO's online sales systems and access their driver's license number. GEICO further stated in its Notice that it believed the fraudsters could use the stolen information to fraudulently apply for unemployment benefits in the names of GEICO's customers. In the Notice, GEICO advised its customers to carefully review any mail they receive from state unemployment agencies or departments and to

[2] Notice of Data Disclosure (Apr. 9, 2021), https://oag.ca.gov/system/files/DL3_IndNoticeLttr_CA_Redacted.pdf (last accessed Apr. 29, 2021).

contact that agency or department if there is any chance fraud is being committed. GEICO further advised its customers to "be vigilant for incidents of fraud or identity theft by reviewing your account statements and credit reports for any unauthorized activity."

24. Because of the extensive confidential and personal information that GEICO stores, GEICO has a privacy policy that makes specific representations to GEICO Customers regarding its affirmative duty to protect its customers' PII. In its Privacy Policy, GEICO represents to its customers that "We restrict access to your Information to employees who we have determined need it to provide products or services to you. We train our employees to safeguard customer information, and we require them to sign confidentiality and non-disclosure agreements. We maintain a variety of physical, electronic, and procedural safeguards to protect your Information from unauthorized access by third parties."[3]

25. GEICO continues that its Privacy Policy applies equally to current and former policyholders: "Information about our former customers and about individuals who have obtained quotes from us is safeguarded to the same extent as Information about our current policyholders."

26. GEICO further represents in its Privacy Policy that "Your Security is Important" and guides its customers to review GEICO's Confidentiality and Security Policy, which is linked directly to GEICO's Privacy Policy.[4] In that Confidentiality and Security Policy, GEICO represents that: "At GEICO.com, the privacy and security of customer data is as important to us as it is to you. Physical safeguards, procedural controls and data access controls protect your data

[3] GEICO's Privacy Policy (effective July 1, 2020), https://media.geico.com/legal/privacy_policy.htm (last accessed Apr. 29, 2021).
[4] *See* GEICO's Confidentiality and Security Policy (effective July 1, 2020), https://media.geico.com/legal/privacy_policy.htm#conf_security (last accessed Apr. 29, 2021).

from unauthorized access. We continually monitor our systems to prevent unauthorized attempts at intrusion."

27. Plaintiffs and Class Members were required to agree to GEICO's Privacy Policy, Terms of Use, Payment Authorization, and Consent to Electronic Transactions and Disclosures.

28. GEICO's customers expect GEICO to maintain strict confidentiality of PII in its possession. Throughout the course of its business, GEICO has collected and maintained an extensive amount of its customers' PII. GEICO's customers provide their PII to GEICO in reliance on GEICO's assurances in its Privacy Policy, Confidentiality and Security Policy and elsewhere that it will protect their PII from unauthorized access.

29. GEICO has failed to maintain the confidentiality of PII, failed to prevent cybercriminals from access and use of PII, failed to avoid accidental loss, disclosure, or unauthorized access to PII, failed to prevent the unauthorized disclosure of PII, and failed to provide security measures consistent with industry standards for the protection of PII, of its current and former policyholders.

30. GEICO's Notice does not state when the breach was discovered except that it was "recently determined."

31. As a result of GEICO's failure to maintain adequate security measures, GEICO's customers' personal and private information has been compromised and remains vulnerable, including the PII of Plaintiffs and Class Members.

32. This Data Disclosure was foreseeable, in light of the much-publicized wave of data breaches in recent years. Since at least 2015, the Federal Bureau of Investigation ("FBI") has specifically advised private industry about the threat of "Business E-Mail Compromise" ("BEC"). The FBI calls BEC "a growing financial fraud that is more sophisticated than any similar scam the

FBI has seen before and one—in its various forms—that has resulted in actual and attempted losses of more than a billion dollars to businesses worldwide." The FBI notes that "scammers' methods are extremely sophisticated," and warns companies that "the criminals often employ malware to infiltrate company networks."[5]

33. Identity thieves can also use the PII to harm Plaintiffs and Class Members through embarrassment, blackmail, or harassment either in person or online, or to commit other types of fraud including fraudulently obtaining tax returns and refunds, and government benefits such as unemployment insurance or access to other benefits and services -- as GEICO understands to be the case with respect to this Data Disclosure.

34. To put this identity theft into context, the 2013 Norton Report – based on one of the largest consumer cybercrime studies ever conducted – estimated that at that time, the global price tag of cybercrime was around $113 billion with the average cost per victim being $298 dollars.[6]

35. Accordingly, GEICO knew or should have known, given the vast amount of PII it collects, manages, and maintains, that it was the target of security threats, and therefore understood the risks posed by unsecure data security practices and systems. Defendants' failure to heed warnings and to otherwise maintain adequate security practices resulted in this Data Disclosure.

36. Defendants, at all relevant times, had a duty to Plaintiffs and Class Members to properly secure their PII, encrypt and maintain such information using industry standard methods, train their employees, utilize available technology to defend their systems from invasion, act

[5] Federal Bureau of Investigation, *Business E-Mail Compromise: An Emerging Global Threat*, https://www.fbi.gov/news/stories/business-e-mail-compromise (last visited Apr. 29, 2021).
[6] 2013 Norton Report, Norton by Symantec, *available at* https://yle.fi/tvuutiset/uutiset/upics/liitetiedostot/norton_raportti.pdf (last accessed Apr. 29, 2021).

reasonably to prevent foreseeable harm to Plaintiffs and Class Members, and promptly notify Plaintiffs and Class Members when Defendants became aware of the potential that its current and former policyholders' PII may have been compromised.

37. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between Defendants, on the one hand, and Plaintiffs and the Class Members, on the other hand. The special relationship arose because Plaintiffs and the members of the Class entrusted Defendants with their PII as part of receiving insurance coverage from GEICO. Defendants had the resources necessary to prevent the Data Disclosure but neglected to adequately invest in security measures, despite their obligation to protect such information. Accordingly, Defendants breached their common law, statutory, and other duties owed to Plaintiff and Class Members.

38. Defendants' duty to use reasonable security measures also arose under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data by entities such as Defendants.

39. The Federal Trade Commission has established data security principles and practices for businesses as set forth in its publication, Protecting Personal Information: A Guide for Business.[7] Among other things, the FTC states that companies should encrypt information stored on computer networks and dispose of consumer information that is no longer needed. The FTC also says to implement policies for installing vendor-approved patches to correct problems, and to identify operating systems. The FTC also recommends that companies understand their

[7] https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_protecting-personal-information.pdf (last visited Apr. 18, 2020).

network's vulnerabilities and develop and implement policies to rectify security deficiencies. Further, the FTC recommends that companies utilize an intrusion detection system to expose a Data Disclosure as soon as it occurs; monitor all incoming traffic for activity that might indicate unauthorized access into the system; monitor large amounts of data transmitted from the system, and have a response plan ready in the event of a Data Disclosure. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." (17 C.F.R. § 248.201 (2013)).

40. The FTC has prosecuted a number of enforcement actions against companies for failing to take measures to adequately and reasonably protect consumer data. The FTC has viewed and treated such security lapses as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45.

41. Defendants failed to maintain reasonable data security procedures and practices.

42. The Data Disclosure enabled successful attempts by a malicious third parties to steal GEICO's customers' PII on a mass scale. The only reason a hacker would steal PII on a mass scale would be to use that information to commit future acts of cyber-fraud and identity theft -- in this case, according to GEICO, to, among other things, fraudulently apply for unemployment benefits in GEICO's customers' names. It is a virtual certainty that the hackers will engage in future acts of fraud or identity theft either directly, or indirectly by selling the GEICO customers' PII on the dark web to other malicious actors. Thus, Plaintiffs and Class Members are at an exceptionally high risk of future acts of identity theft. Moreover, the ill-gotten PII could be

combined with information stolen during other computer hacks and data breaches to create increasingly complex and convincing scams.

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

44. Defendants were at all times fully aware of their obligations to protect the PII of current and former policyholders. Defendants were also aware of the significant consequences that would result from its failure to do so.

45. To date, Defendants have merely offered identity theft and credit monitoring services at no charge for 12 months. The offer, however, is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and it entirely fails to provide any compensation for the unauthorized release and disclosure of Plaintiffs' and Class Members' PII.

46. Furthermore, Defendants' credit monitoring offer to Plaintiffs and Class Members squarely places the burden on Plaintiffs and Class Members, rather than upon the Defendants, to investigate and protect themselves from Defendants' tortious acts resulting in the Data Disclosure. Rather than automatically enrolling Plaintiffs and Class Members in credit monitoring services upon discovery of the breach, Defendants merely sent instructions offering the services to potentially affected policyholders with the recommendation that they sign up for the services.

47. Plaintiffs' and Class Members' ascertainable losses in undertaking additional security measures is consistent with Javelin Strategy & Research's 2017 compilation of consumer complaints to the FTC showing that the average out-of-pocket cost to consumers for identity theft was $429.00.

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

49. As a direct and proximate result of Defendants' wrongful actions and inaction, Plaintiffs and Class Members have suffered injury and damages, including the increased risk of identity theft and identity fraud, improper disclosure of PII, the time and expense necessary to mitigate, remediate, and sort out the increased risk of identity theft and to deal with governmental agencies, including all those administering unemployment benefits, as a result of fraudulent claims ostensibly made on their behalf.

50. In addition, as a direct and proximate result of Defendants' wrongful actions and inaction, GEICO's customers have suffered an ascertainable loss in that they must undertake additional security measures, some at their own expense, to minimize the risk of future data breaches.

51. Plaintiffs' and Class Members' ascertainable losses in undertaking additional security measures is consistent with Javelin Strategy & Research's 2017 compilation of consumer complaints to the FTC showing that the average out-of-pocket cost to consumers for identity theft was $429.00.

52. Moreover, as a direct result and a necessary consequence of the Data Disclosure, GEICO's customers have suffered an ascertainable loss in that they have incurred otherwise-

unnecessary out-of-pocket expenses and suffered opportunity loss due to the time they have been required to spend in attempts to mitigate the damages caused by the Data Disclosure.

53. Furthermore, GEICO essentially granted unauthorized third parties/hackers access to Plaintiffs' and Class Members' PII without compensation. The value of their PII, in part derived from its privacy, should be exclusively controlled by GEICO's customers, which is precisely what Plaintiffs expected. As a result of GEICO's failure to maintain adequate security measures, Plaintiffs and Class Members continue to suffer an ongoing and escalating accumulation of damages, as the Data Disclosure has rendered them more susceptible to future data breaches, identity theft, and other kinds of online fraud.

CLASS ACTION ALLEGATIONS

54. Plaintiffs bring this action and seek to certify and maintain it as a class action under Federal Rules of Civil Procedure 23(a), (b)(2), (b)(3), and/or (c)(4), on behalf of themselves, and the following proposed Class (collectively, the "Class").

55. The Nationwide Class is defined as follows: All individuals residing in the United States whose PII was compromised as a result of the Data Disclosure initially disclosed by GEICO on or about April 9, 2020.

56. Excluded from the above proposed Class are: Defendants, any entity in which Defendants have a controlling interest, is a parent or subsidiary, or which is controlled by Defendants, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendants; and judicial officers to whom this case is assigned and their immediate family.

57. Plaintiffs reserve the right to re-define the Class definitions after conducting discovery and add any necessary subclasses if further investigation reveals that the Class should be expanded or otherwise modified.

58. The proposed Class meets the criteria for certification under Rule 23(a), (b)(2), (b)(3) and/or (c)(4).

59. **Fed. R. Civ. P. 23(a)(1): Numerosity**. Pursuant to Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that the joinder of all members is impractical. While the exact number of Class Members is unknown to Plaintiff at this time, the proposed Class includes potentially millions of individuals whose PII was compromised in the Data Disclosure. Class Members may be readily identified through objective means, including by and through Defendants' business records. The disposition of the claims of these Class Members in a single action will provide substantial benefits to Plaintiffs, Class Members, Defendants, and the Court. Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

60. **Fed. R. Civ. P. 23(a)(2) and (b)(3): Commonality**. Pursuant to Rule 23(a)(2) and in conjunction with Rule 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class Members. The common questions include, but are not limited to, the following:

a. Whether Defendants had a legal duty to implement and maintain reasonable security procedures and practices for the protection of Class Members' personal and financial information, including by vendors;

b. Whether Defendants breached their legal and/or contractual duty to implement and maintain reasonable security procedures and practices for the protection of Plaintiffs and Class Members' PII;

c. Whether Defendants took reasonable steps and measures to safeguard Plaintiffs' and Class Members' PII;

d. Whether Defendants' conduct, practices, actions, and omissions, resulted in or were the proximate cause of the Data Disclosure, resulting in the loss of PII of Plaintiffs and Class Members;

e. Whether Defendants' acts and omissions described herein give rise to class claims of negligence or other statutory violations;

f. Whether Defendants had a legal duty to provide timely and accurate notice of the Data Disclosure to Plaintiffs and Class Members;

g. Whether Defendants breached their duty to provide timely and accurate notice of the Data Disclosure to Plaintiffs and Class Members;

h. Whether and when Defendants knew or should have known that their computer systems were vulnerable to attack;

i. Whether Defendants failed to implement and maintain reasonable and adequate security measures, procedures, and practices to safeguard Plaintiffs' and Class Members' PII, including by vendors;

j. Whether Defendants breached express or implied contracts with Plaintiffs and the Class in failing to have adequate data security measures despite promising to do so;

k. Whether Defendants' conduct was negligent;

l. Whether Defendants' conduct was *per se* negligent;

m. Whether Defendants' practices, actions, and omissions constitute unfair or deceptive business practices;

n. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendants' conduct, including increased risk of identity theft and loss of value of their personal and financial information; and

o. Whether Plaintiffs and Class Members are entitled to relief, including damages and equitable relief.

61. **Fed. R. Civ. P. 23(a)(3): Typicality**. Pursuant to Rule 23(a)(3), Plaintiffs' claims are typical of the claims of Class Members. Plaintiffs, like all members of the Class, were injured through Defendants' uniform misconduct described above and asserts similar claims for relief. The same events and conduct that give rise to Plaintiffs' claims also give rise to the claims of every other Class Member because Plaintiffs and each Class Member are persons that have suffered harm as a direct result of the same conduct engaged in by Defendants and resulting in the Data Disclosure. In addition, the representative Plaintiffs and Class Members have been damaged by GEICO's misconduct in that they have had to undertake additional security measures, at their own time and expense, to minimize the risk of future data breaches, and/or will be required to do so.

62. **Fed. R. Civ. P. 23(a)(4): Adequacy of Representation**. Pursuant to Rule 23(a)(4), Plaintiffs and their counsel will fairly and adequately represent the interests of the Class Members. Plaintiffs have no interest antagonistic to, or in conflict with, the interests of the Class Members. Plaintiffs have retained attorneys experienced in the prosecution of complex class actions, including consumer Data Disclosure class actions, and Plaintiffs intend to prosecute this action vigorously.

63. **Superiority**. **Fed. R. Civ. P. 23(b)(3)**. Pursuant to Rule 23(b)(3), a class action is superior to individual adjudications of this controversy. Litigation is not economically feasible for individual members of the Class because the amount of monetary relief available to individual Plaintiffs is insufficient in the absence of the class action procedure. Absent a class action, most Class Members would likely find the cost of litigating their claims prohibitively high and would therefore have no effective remedy at law. The value of the individual Class Members' claims, when compared to the costs of investigation and prosecution of those claims, makes it more probable than not that only a few Class Members could afford to seek legal redress for GEICO's misconduct. Absent a class action, Class Members will continue to incur damages, and GEICO's misconduct will continue without remedy. Separate litigation could yield inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. A class action presents fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

64. **Fed. R. Civ. P. 23(b)(1) and (2): Risk of Inconsistent or Dispositive Adjudications and the Appropriateness of Final Injunctive or Declaratory Relief**. In the alternative, this action may properly be maintained as a class action, because:

a. The prosecution of separate actions by individual members of the Class would create a risk of inconsistent or varying adjudication with respect to individual members of the Class, which would establish incompatible standards of conduct for Defendants; or

b. The prosecution of separate actions by individual members of the Class would create a risk of adjudications with respect to individual members of the Class which would, as a practical matter, be dispositive of the interests of other members of the Class not

parties to the adjudications, or substantially impair or impede their ability to protect their interests; or

c. Defendants have acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive or corresponding declaratory relief with respect to the Class as a whole.

65. **Fed. R. Civ. P. 23(c)(4): Issue Certification**. In the alternative, the common questions of fact and law, set forth above, are appropriate for issue certification on behalf of the proposed Class.

COUNT ONE
Negligence

66. Plaintiffs repeat, reiterate and reallege each and every allegation set forth in previous paragraphs above as if set forth in full herein.

67. Defendants required Plaintiffs and Class Members to submit non-public, sensitive PII for purposes of obtaining insurance through GEICO.

68. Defendants had, and continue to have, a duty to Plaintiffs and Class Members to exercise reasonable care in safeguarding and protecting their PII. Defendants also had, and continue to have, a duty to use ordinary care in activities from which harm might be reasonably anticipated, such as in the storage and protection of PII within their possession, custody and control and that of its vendors.

69. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between GEICO and its policyholders. Only Defendants were in a position to ensure that their systems were sufficient to protect against the harm to Plaintiffs and the Class Members from the Data Disclosure.

70. Defendants violated these standards and duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect the PII entrusted to it, including Plaintiffs' and Class Members' PII, and including driver's license numbers. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiffs' and Class Members' PII.

71. Defendants knew or should have known that their computer systems and data storage architecture were vulnerable to unauthorized access and targeting by hackers for the purpose of stealing and misusing confidential PII.

72. Defendants, by and through their negligent actions, inaction, omissions, and want of ordinary care, unlawfully breached its duties to Plaintiffs and Class Members by, among other things, failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' PII within their possession, custody and control.

73. Defendants, by and through their negligent actions, inactions, omissions, and want of ordinary care, further breached its duties to Plaintiffs and Class Members by failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit their processes, controls, policies, procedures, protocols, and software and hardware systems for complying with the applicable laws and safeguarding and protecting their PII.

74. But for Defendants' negligent breach of the above-described duties owed to Plaintiffs and Class Members, their PII would not have been released, disclosed, and disseminated without their authorization.

75. Plaintiffs' and Class Members' PII was transferred, sold, opened, viewed, mined and otherwise released, disclosed, and disseminated to unauthorized persons without their authorization as the direct and proximate result of Defendants' failure to design, adopt, implement, control, direct, oversee, manage, monitor and audit its processes, controls, policies, procedures and protocols for complying with the applicable laws and safeguarding and protecting Plaintiffs' and Class Members' PII.

76. As a direct and proximate result of Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Disclosure, Plaintiffs and Class Members have suffered, and will continue to suffer, ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

77. Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused this Data Disclosure constitute negligence.

COUNT TWO
Negligence *Per Se*

78. The Plaintiffs repeat, reiterate and reallege each and every allegation set forth in previous paragraphs above as if set forth in full herein.

79. Pursuant to the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security to safeguard the personal and financial information of Plaintiffs and Class Members.

80. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect the PII of Plaintiffs and Class Members. The pertinent FTC publications and orders form part of the basis of Defendants' duty in this regard.

81. Defendants required, gathered, and stored personal and financial information of Plaintiffs and Class Members for insurance purposes.

82. Defendants violated the FTCA by failing to use reasonable measures to protect the PII of Plaintiffs and Class Members and not complying with applicable industry standards, as described herein.

83. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

84. The harm that occurred as a result of the Data Disclosure is the type of harm the FTCA was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and Class Members.

85. As a direct and proximate result of Defendants' negligence per se, Plaintiffs and Class Members have suffered, and continue to suffer, injuries, damages arising from identify theft; from their needing to contact agencies administering unemployment benefits; potentially defending themselves from legal action base upon fraudulent applications for unemployment benefits made in their name; contacting their financial institutions; loss of use of funds; closing or modifying financial accounts; damages from lost time and effort to mitigate the actual and potential impact of the Data Disclosure on their lives; closely reviewing and monitoring their accounts for unauthorized activity which is certainly impending; placing credit freezes and credit alerts with credit reporting agencies; and damages from identify theft, which may take months or years to discover and detect.

86. Defendants' violation of the FTCA constitutes negligence *per se*.

COUNT THREE
Breach of Contract

87. The Plaintiffs repeat, reiterate and reallege each and every allegation set forth in previous paragraphs above as if set forth in full herein.

88. Plaintiffs and Class Members entered into express contracts with GEICO that included GEICO's promise to protect nonpublic PII provided to GEICO from disclosure.

89. At all relevant times, GEICO and Plaintiffs and the Class mutually assented to and therefore were bound by the version of GEICO's Privacy Policy and Confidentiality and Security Policy (the "Contract") that was operative at the time Plaintiffs and each of the Class members purchased products from GEICO.

90. There was offer, acceptance and consideration, the consideration being the premiums paid by Plaintiffs and Class Members in exchange for insurance coverage pursuant to

the terms of said agreements, including the provisions of those agreements pertaining to the protection of PII.

91. Plaintiffs and Class Members have performed and satisfied all of their obligations to GEICO, pursuant to their insurance agreements, except for those obligations they were prevented or excused from performing or satisfying.

92. Defendants breached their contractual obligations to protect the nonpublic PII they possessed and with which they were entrusted with when the information was accessed by unauthorized persons as part of the Data Disclosure. Defendants also breached the Contract by failing to have proper safeguards to protect Plaintiffs and the Class Members' PII and allowing a malicious third party to access that information without permission. GEICO violated its commitment to maintain the confidentiality and security of the PII of Plaintiffs and the Class and failed to comply with their own polices and industry standards related to data security.

93. As a direct and proximate result of Defendants' breach of contract, Plaintiffs and Class Members have suffered, and continue to suffer, injuries, damages arising from identify theft; from their needing to contact agencies administering unemployment benefits; potentially defending themselves from legal action base upon fraudulent applications for unemployment benefits made in their name; contacting their financial institutions; loss of use of funds; closing or modifying financial accounts; damages from lost time and effort to mitigate the actual and potential impact of the Data Disclosure on their lives; closely reviewing and monitoring their accounts for unauthorized activity which is certainly impending; placing credit freezes and credit alerts with credit reporting agencies; and damages from identify theft, which may take months or years to discover and detect.

94. The above constitutes breach of contract by Defendants.

COUNT FOUR
Breach of Implied Contract

95. Plaintiffs repeat, reiterate and reallege each and every allegation set forth in previous paragraphs above as if set forth in full herein.

96. Defendants required Plaintiffs and Class Members to provide PII, including their driver's license, driver's license numbers, legal name and address, as a condition of issuing insurance. In so doing, Plaintiffs and Class Members entered into implied contracts with Defendants by which Defendants agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and Class Members if their data had been breached and compromised, or stolen.

97. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendants.

98. Defendants breached the implied contracts it made with Plaintiffs and Class Members by failing to safeguard and protect their PII, including driver's license numbers, and by failing to provide timely and accurate notice to them that PII was compromised as a result of the Data Disclosure.

99. Plaintiffs and Class Members would not have provided and entrusted their PII to GEICO or would have paid less for GEICO's services in the absence of the implied contract or implied terms between them and GEICO. The safeguarding of the PII of Plaintiffs and Class Members was critical to realize the intent of the parties.

100. As a direct and proximate result of Defendants' breach of implied contract, Plaintiffs and Class Members have suffered, and continue to suffer, injuries, damages arising from identify theft; from their needing to contact agencies administering unemployment benefits; potentially defending themselves from legal action base upon fraudulent applications for

unemployment benefits made in their name; contacting their financial institutions; loss of use of funds; closing or modifying financial accounts; damages from lost time and effort to mitigate the actual and potential impact of the Data Disclosure on their lives; closely reviewing and monitoring their accounts for unauthorized activity which is certainly impending; placing credit freezes and credit alerts with credit reporting agencies; and damages from identify theft, which may take months or years to discover and detect.

101. The above constitutes breach of implied contract by Defendants.

COUNT FIVE

Breach of the Drivers Privacy Protection Act ("DPPA")

102. Plaintiffs repeat, reiterate and reallege each and every allegation set forth in previous paragraphs above as if set forth in full herein.

103. 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.

104. 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). Drivers' license numbers are motor vehicle records under the DPPA.

105. Defendant obtains motor vehicle records from its customers.

106. Defendant also obtains motor vehicle records directly from state agencies or through resellers who sell such records.

107. Through the Data Disclosure, Defendants disclosed motor vehicle records for purposes not authorized by the DPPA.

108. Such disclosure was willful and reckless.

109. Plaintiffs and putative class members are entitled to actual damages, liquidated damages, punitive damages, and attorneys' fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the members of the Class defined above, respectfully request that this Court:

A. Certify this case as a class action under Federal Rule of Civil Procedure 23, appoint Plaintiffs as the Class representatives, and appoint the undersigned as Class counsel;

B. Order appropriate relief to Plaintiffs and the Class;

C. Awarding Plaintiffs and the Class Members actual, compensatory, liquidated, and consequential damages;

D. Awarding Plaintiffs and the Class Members statutory damages and penalties, as allowed by law;

E. Awarding Plaintiffs and the Class Members restitution and disgorgement;

F. Requiring Defendants to provide appropriate credit monitoring services to Plaintiffs and the other class members;

G. Awarding Plaintiffs and the Class Members punitive damages;

H. Entering injunctive and declaratory relief as appropriate under the applicable law;

I. Awarding Plaintiffs and the Class pre-judgment and/or post-judgment interest as prescribed by law;

J. Awarding reasonable attorneys' fees and costs as permitted by law; and

K. Entering such other and further relief as may be just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury of all claims so triable.

Dated: May 11, 2021

/s/ Kristi C. Kelly

Kristi C. Kelly, Esq., (No. 07244)
KELLY GUZZO, PLC
3925 Chain Bridge Road, Suite 202
Fairfax, VA 22030
(703) 424-7572 – Telephone
(703) 591-0167 – Facsimile
Email: kkelly@kellyguzzo.com

E. Michelle Drake*
John Albanese*
BERGER MONTAGUE PC
43 S.E. Main Street, Suite 505
Minneapolis, MN 55414
(612) 594-5999
emdrake@bm.net
jalbanese@bm.net

Karen Hanson Riebel*
Kate M. Baxter-Kauf*
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Avenue South, Suite 2200
Minneapolis, MN 55401
Telephone: (612) 339-6900
Facsimile: (612) 339-0981
khriebel@locklaw.com
kmbaxter-kauf@locklaw.com
Counsel for Plaintiffs
**pro hac vice* forthcoming