RACHELE R. BYRD (190634)
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP
750 B Street, Suite 1820
San Diego, CA 92101
Telephone: (619) 239-4599
Facsimile: (619) 234-4599
byrd@whafh.com

M. ANDERSON BERRY (262879)
GREGORY HAROUTUNIAN (330263)
CLAYEO C. ARNOLD, A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829
aberry@justice4you.com
gharoutunian@justice4you.com

GAYLE M. BLATT (122048)
CASEY GERRY SCHENK FRANCAVILLA BLATT & PENFIELD, LLP
110 Laurel Street
San Diego, California 92101
Telephone: (619) 238-1811
Facsimile: (619) 544-9232
gmb@cglaw.com

[Additional counsel appear on signature page]

Counsel for Plaintiffs and the Class

SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF CONTRA COSTA

JOHN HAJNY, RICARDO VILLALOBOS, ANTHONY SERVICE and JEREMY ADAMS, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

VOLKSWAGEN GROUP OF AMERICA, INC., AUDI OF AMERICA, LLC, AND SANCTUS, LLC D/B/A SHIFT DIGITAL,

Defendants.

Case No. _____

CLASS ACTION

CLASS ACTION COMPLAINT FOR:

1. **NEGLIGENCE;**
2. **BREACH OF IMPLIED CONTRACT;**
3. **VIOLATION OF CALIFORNIA'S CONSUMER PRIVACY ACT;**
4. **VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW; AND**
5. **BREACH OF CONTRACT**

Plaintiffs John Hajny ("Hajny"), Ricardo Villalobos ("Villalobos"), Anthony Service ("Service") and Jeremy Adams ("Adams") (collectively, "Plaintiffs"), on behalf of themselves and all others similarly situated, upon personal knowledge of the facts pertaining to them and on information and belief as to all other matters, allege the following against Defendants Volkswagen Group of America, Inc. ("VGoA"), Audi of America, LLC ("Audi"), and Sanctus, LLC d/b/a Shift Digital ("Shift Digital") (collectively, "Defendants").

NATURE OF THE CASE

1. In a recent Executive Order, President Joe Biden reaffirmed that "[t]he United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy."[1] Among other things, the Order noted:

> The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.[2]

2. Plaintiffs bring this class action against Defendants for their failure to properly secure and safeguard personally identifiable information that Plaintiffs entrusted to Defendants. Unfortunately, Defendants violated that trust, leaving Plaintiffs and the putative Class to suffer the consequences. Here, 3.3 million persons had their personal information ("PI") and/or sensitive personal information ("SPI")[3] stolen from Defendants by computer hackers in a cyber-attack (the

---

[1] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ (last visited Aug. 29, 2022).

[2] *Id*.

[3] "PI" means information that is or could be used, whether on its own or in combination with other information, to identify, locate, or contact a person. For purposes of this complaint, PI does not include driver's license numbers, Social Security numbers, credit or debit card numbers, bank account or routing numbers, social insurance numbers, dates of birth, and/or tax identification numbers.

"SPI" means, for purposes of this complaint, the following types of Personal Information: driver's license numbers, Social Security numbers, credit or debit card numbers, bank account or routing numbers, social insurance numbers, dates of birth, and/or tax identification numbers.

"Data Breach"). The information compromised in the Data Breach includes name, mailing address, email address, phone number, information about a vehicle purchased, leased, or inquired about, including the Vehicle Identification Number ("VIN"), make, model, year, color, and trim and, in some instances, buyers' or interested parties' driver's license numbers, Social Security numbers, account or loan numbers, and tax identification numbers.[4]

3. A memo to VGoA dealers identified Shift Digital as being involved in the Data Breach impacting more than 3.3 million customers and prospective buyers, primarily at Audi. Shift Digital is used by Audi, Volkswagen, and some authorized dealers in the United States and Canada. According to VGoA, Shift Digital left unsecured an electronic file containing PI and SPI, gathered for sales and marketing between 2014 and 2019.[5]

4. Plaintiffs Hajny, Villalobos, Service and Adams bring this class action lawsuit on behalf of a Nationwide Class and a California Sub-Class (together, the "Class") to address Defendants' inadequate safeguarding of class members' PI and SPI.

5. Armed with the SPI accessed in the Data Breach, data thieves can commit numerous crimes including opening new financial accounts in Class members' names, taking out loans in Class members' names, using Class members' names to obtain medical services, using Class members' information to obtain government benefits, filing fraudulent tax returns using Class members' information, obtaining driver's licenses in Class members' names but with another person's photograph, and giving false information to police during an arrest.

6. Indeed, news outlets are already reporting that the information stolen in the Data Breach is being sold on well-known hacking forums.[6] This shows the clear value of the stolen data to identity thieves and the imminent peril faced by Plaintiffs and the members of the Class.

---

[4] *See* https://oag.ca.gov/system/files/Audi%20Notification%20Letter%20Template.pdf (last visited Aug. 29, 2022).

[5] *See* Larry P. Vellequette, *Vendor linked to VW data breach named in memo to dealers*, AUTOMOTIVE NEWS (June 11, 2021), https://www.autonews.com/technology/vendor-linked-vw-data-breach-named-memo-dealers (last visited Aug. 29, 2022).

[6] *See, e.g.*, Lorenzo Fracheschi-Bicchierai, *Hackers Are Selling Data Stolen From Audi and Volkswagen*, MOTHERBOARD, TECH BY VICE (June 17, 2021), https://www.vice.com/en/article/xgxaq4/hackers-are-selling-data-stolen-from-audi-and-

7. As a result of the Data Breach, Plaintiffs and Class members have been exposed to a present and continuing risk of fraud and identity theft. Plaintiffs and Class members must now and in the future closely monitor their financial accounts to guard against identity theft.

8. Plaintiffs and Class members will also incur out-of-pocket costs for things such as paying for credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

9. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose PI and SPI were accessed during the Data Breach.

10. Plaintiffs and the Class request remedies including damages, reimbursement of out-of-pocket costs, and equitable and injunctive relief, including improvements to Defendants' data security systems, future annual audits, and ID protection services funded by Defendants.

PARTIES

11. Plaintiff John Hajny is resident of the state of California. He has leased at least six Audi vehicles since 2014 from various California Audi dealerships. Mr. Hajny received a Notice of Data Security Incident from Defendants on or about June 15, 2021.

12. Plaintiff Ricardo Villalobos is resident of the state of California. He has owned or leased three Audi vehicles since 2017. Mr. Villalobos received a Notice of Security Incident from Defendants on or about June 11, 2021.

13. Plaintiff Anthony Service is a resident of the State of Florida. He purchased an Audi vehicle from a dealership in Florida in 2015, has test-driven several Audi vehicles at Audi dealerships and rented vehicles from Silvercar by Audi on several occasions. Mr. Service received a Notice of Data Breach dated June 11, 2021.

volkswagen (last visited Aug. 29, 2022); Lawrence Abrams, *Audi, Volkswagen customer data being sold on hacking forum*, BLEEPING COMPUTER (June 17, 2021), https://www.bleepingcomputer.com/news/security/audi-volkswagen-customer-data-being-sold-on-a-hacking-forum/ (last visited Aug. 29, 2022).

14. Plaintiff Jeremy Adams is a resident of the State of Florida. He purchased an Audi vehicle in Florida in 2017. Mr. Adams received a Notice of Security Incident from Defendants by email on or about June 20, 2021.

15. Defendant Volkswagen Group of America, Inc. ("VGoA") is a corporation incorporated in New Jersey with its principal place of business in Herndon, Virginia. Defendant VGoA is the North American subsidiary of Volkswagen AG.

16. Defendant Audi of America, LLC ("Audi") is a registered trade name of VGoA and has its principal place of business in Herndon, Virginia.

17. Defendant Sanctus, LLC d/b/a Shift Digital ("Shift Digital") is a Michigan limited liability company headquartered in Birmingham, Michigan. Shift Digital claims to have invented "digital marketing program optimization" and its website touts its "data omniscience." It is "the leader in digital marketing program optimization."[7] At the time of the Data Breach, Shift Digital worked with Defendants VGoA and Audi on marketing.

JURISDICTION AND VENUE

18. This Court has jurisdiction over this action pursuant to Cal. Code Civ. Proc. § 410.10 and Cal. Bus. & Prof. Code §§ 17203-17204, 17604. This action is brought as a class action on behalf of Plaintiffs and the Class members pursuant to Cal. Code Civ. Proc. § 382.

19. This Court has personal jurisdiction over Defendants because Defendants conduct business in and throughout California, and the wrongful acts alleged in this Complaint were committed in California, among other venues.

20. Venue is proper in this Court pursuant to Cal. Code Civ. Proc. § 395 and § 395.5 because Defendants regularly conduct business in the State of California, and, with respect to putative class members, the unlawful acts or omissions giving rise to this action also occurred or arose in this county.

[7] https://www.shiftdigital.com/company/ (last visited Aug. 29, 2022).

FACTUAL ALLEGATIONS

21. Defendant VGoA is the North American subsidiary of Volkswagen AG, a German-based manufacturer of cars and other vehicles worldwide. Audi is a trademark of VGoA and a well-known brand of luxury cars. Shift Digital provides VGoA and Audi with marketing tools, data management, and other functions.

22. Defendants sell and market Volkswagen and Audi vehicles in the United States. Defendant Shift Digital helps deploy and manage marketing programs; its technology was initially developed to meet the needs of the automotive industry and has more recently evolved to serve clients in other industries such as power sports, home building, and healthcare. As a part of the automobile sales and marketing process, Defendants collect various types of PI and SPI from customers and potential customers, including name, mailing address, email address, phone number, and information about a vehicle purchased, leased, or inquired about including the VIN, make, model, year, color, and trim. In the event the buyer or potential buyer purchases the vehicle or applies to Defendants for financing, Defendants also collect the buyers' or interested parties' driver's license numbers, Social Security numbers, account or loan numbers, and tax identification numbers.

23. In addition to storing this information themselves, Defendants also provide it to third party vendors for sales and marketing purposes.

24. From 2014 through 2019, Defendants collected the PI and/or SPI of approximately 3.3 million U.S.-based customers. Roughly 90,000 of those customers provided SPI, including their driver's license numbers, Social Security numbers, account or loan numbers, or tax identification numbers.

25. While Defendants are more than happy to monetize that information, and despite the very sensitive nature of that information and the clear potential for misuse, Defendants left that data stored unsecured for *two years*.

26. In early March 2021, Defendants were informed that unauthorized third parties had gained access to this PI and SPI. Following an investigation, in May 2021, Defendants confirmed the PI and SPI were unsecured and that it had been stolen by cyber thieves.

27. On or about June 11, 2021, Defendants VGoA and Audi began notifying affected customers and state attorneys general about the breach and data theft.

28. Just a few days later, the information stolen in the Data Breach showed up for sale on well-known hacking forums.[8]

Plaintiff Hajny

29. To lease his Audi vehicles, Plaintiff Hajny was required by Defendants to provide his PI and SPI, including his full name, driver's license number, Social Security number, e-mail address, telephone numbers, date of birth, bank account numbers, and other sensitive information, including employer name, names and contact information of relatives and personal references, and insurance information. He provided this PI and SPI to Defendants with the understanding that his PI and SPI would be protected, maintained, and safeguarded from unauthorized use or disclosure, and that he would be timely notified of any unauthorized disclosure of his PI and SPI. He would not have agreed to provide his PI and SPI to Defendants, or would have taken precautions to protect it had he known that Defendants would not safeguard it.

30. Plaintiff Hajny received Defendants VGoA and Audi's Notice of Data Security Incident, dated June 15, 2021, on or about that date.

31. The Notice instructed Mr. Hajny to, among other things, "[l]ook out for spam emails" and "[b]e cautious when opening links or attachments from unsolicited third parties."

32. On or about May 24, 2021, Plaintiff Hajny was informed by the Internal Revenue Service ("IRS") that unauthorized third parties used his name and other personal information to electronically file a fraudulent 2019 tax return in his name. Because of this fraud, the IRS believes Mr. Hajny owes the government approximately $5,000. The IRS also informed Mr. Hajny that a different unauthorized third party electronically filed a 2020 tax return in his name, but because

---

[8] Fracheschi-Bicchierai & Abrams, *supra,* note 6.

that return was filed after Mr. Hajny filed his hard copy 2020 tax return, the fraud is pending investigation.

33. After receipt of the Notice letter, Plaintiff Hajny made reasonable efforts to mitigate further impact of the Data Breach. He spent time researching the Data Breach, reviewing and monitoring his credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. In response to the IRS fraud he suffered as a consequence of the Data Breach, Mr. Hajny has spent time online and on the telephone with various IRS departments, he filed a police report with the local police department, and he personally drove to the IRS office in Alameda County to dispute the fraudulent tax return filings in person. He estimates that he has spent 10-15 hours in response to the Data Breach so far. This is valuable time he otherwise would have spent on other activities.

34. Plaintiff Hajny suffered additional actual injury from having his PI compromised in the Data Breach including, but not limited to: (a) damage to and diminution in the value of his PI a form of property that Defendants obtained from Plaintiff; (b) violation of his privacy rights; and (c) continuing and impending injury arising from the increased risk of identity theft and fraud.

Plaintiff Villalobos

35. Plaintiff Ricardo Villalobos has leased three Audi vehicles since 2017 from Audi Pacific located in Torrance, California; Walter's Audi located in Riverside, California; and Audi Pasadena, located in Pasadena, California.

36. Plaintiff Villalobos provided his PI and SPI to Defendants to lease his Audi vehicles with the understanding that it would be protected, maintained, and safeguarded from unauthorized users or disclosure, and that he would be timely notified of any unauthorized disclosure of his PI and SPI. He would not have agreed to provide his PI and SPI to Defendants, or would have taken precautions to protect it had he known that Defendants would not safeguard it.

37. Plaintiff Villalobos received a letter from Audi of America, dated June 11, 2021, informing him that his information was affected by the Data Breach. A code contained in the letter indicates that he was one of the victims who had the full panoply of PI and SPI stolen, including

potentially his driver's license number, Social Security number, account numbers, and tax identification number.

38. The letter from Defendant Audi instructed Mr. Villalobos to, among other things, "look out for spam emails" and "[b]e cautious when opening links or attachments from unsolicited third parties." It also provided him an option to enroll in credit monitoring and identity theft recovery services.

39. Following the Data Breach, Plaintiff Villalobos noticed fraudulent inquiries on his credit report involving credit cards. He was also locked out of his Netflix account while watching a show. Further, Plaintiff Villalobos has received spam texts purporting to be an alert from Chase bank about an unapproved login which requires him to enter his personal information.

40. After receipt of the Notice letter, Plaintiff Villalobos made reasonable efforts to mitigate further impact of the Data Breach. He spent time researching the Data Breach and reviewing and monitoring his credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. This is valuable time he otherwise would have spent on other activities.

41. Plaintiff Villalobos suffered additional actual injury from having his PI and SPI compromised in the Data Breach including: (a) damage to and diminution in the value of his PI and SPI, a form of property that Defendants obtained from Plaintiff; (b) violation of his privacy rights; and (c) continuing and impending injury arising from the increased risk of identity theft and fraud.

Plaintiff Service

42. In order to purchase his Audi vehicle in 2015 from Audi Lighthouse Point (now known as Audi Fort Lauderdale), on the occasion of several test drives of Audi vehicles at Audi dealerships in Florida, and in order to rent Audi vehicles from Silvercar by Audi on multiple occasions since 2015, Plaintiff Service was required by Defendants to provide his PI and SPI, including his full name, driver's license number, Social Security number, e-mail address, telephone numbers, date of birth, bank account numbers, and other sensitive information, including

employer name, names and contact information of relatives and personal references, and insurance information. He provided this PI and SPI to Defendants with the understanding that his PI and SPI would be protected, maintained, and safeguarded from unauthorized use or disclosure, and that he would be timely notified of any unauthorized disclosure of his PI and SPI. He would not have agreed to provide his PI and SPI to Defendants, or would have taken precautions to protect it had he known that Defendants would not safeguard it.

43. Plaintiff Service received Defendants VGoA and Audi's Notice of Data Breach, dated June 11, 2021. A code contained in the letter indicates that he had at least his name, phone number and email address exposed in the Data Breach.

44. The Notice instructed Mr. Service to, among other things, "[l]ook out for spam emails" and "[b]e cautious when opening links or attachments from unsolicited third parties." It also provided him an option to enroll in credit monitoring and identity theft recovery services.

45. Following the Data Breach, Plaintiff Service noticed an intense uptick in Spam email and phone calls, and was notified by Experian, from which he purchases credit monitoring, that his PI is available to the public due the Data Breach. As a result of receiving the notice from Defendants VGoA and Audi, Plaintiff Service locked his credit, causing great stress and cost.

46. After receipt of the June 11 Notice letter, Plaintiff Service made reasonable efforts to mitigate further impact of the Data Breach. He spent time researching the Data Breach, reviewing and monitoring his credit reports and financial account statements for any indications of actual or attempted identity theft or fraud, and locking his credit, as described above. He estimates that he has spent 10-15 hours in response to the Data Breach so far. This is valuable time he otherwise would have spent on other activities.

47. Plaintiff Service suffered additional actual injury from having his PI compromised in the Data Breach including, but not limited to: (a) damage to and diminution in the value of his PI, a form of property that Defendants obtained from Plaintiff; (b) violation of his privacy rights; and (c) continuing and impending injury arising from the increased risk of identity theft and fraud.

/ / /

Plaintiff Adams

48. Plaintiff Adams purchased an Audi vehicle in Tampa, Florida in 2017 from Reeves Import Motorcars.

49. Plaintiff provided his PI and SPI to Defendants to purchase his Audi vehicle with the understanding that it would be protected, maintained, and safeguarded from unauthorized users or disclosure, and that he would be timely notified of any unauthorized disclosure of his PI and SPI. He would not have agreed to provide his PI and SPI to Defendants, or would have taken precautions to protect it, had he known that Defendants would not safeguard it.

50. Plaintiff Adams received an email from Audi of America, dated June 20, 2021, informing him that his PI was affected by the Data Breach.

51. The email from Defendant Audi instructed Mr. Adams to, among other things, "look out for spam emails" and "[b]e cautious when opening links or attachments from unsolicited third parties."

52. Following the Data Breach, in April 2021, Adams' information was fraudulently used to apply for a line of credit.

53. In July 2021, Adams received a letter from Chase Bank saying that they declined an application because they were concerned that someone may be using his information fraudulently

54. After receipt of the Notice letter, Plaintiff Adams made reasonable efforts to mitigate further impact of the Data Breach. He spent time researching the Data Breach and reviewing and monitoring his credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. This is valuable time he otherwise would have spent on other activities.

55. Plaintiff Adams suffered additional actual injury from having his PI compromised in the Data Breach, including: (a) damage to and diminution in the value of his PI, a form of property that Defendants obtained from Plaintiff; (b) violation of his privacy rights; and (c) continuing and impending injury arising from the increased risk of identity theft and fraud.

A. The SPI exposed by Defendants is very valuable to identity thieves

56. The information exposed by Defendants is very valuable to phishers, hackers, identity thieves and cyber criminals, especially at this time where unprecedented numbers of fraudsters are filing fraudulent unemployment benefit claims.

57. Cybercrime has been on the rise for the past decade and continues to climb exponentially; as of 2013 it was being reported that nearly one out of four data breach notification recipients become a victim of identity fraud.[9]

58. Stolen SPI is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. This is because malicious actors buy and sell that information for profit.[10] And, indeed, it appears this is already happening with the SPI stolen in the Data Breach here.

59. Law enforcement has difficulty policing the dark web due to this encryption, which allows users and criminals to conceal identities and online activity.

60. For example, when the U.S. Department of Justice announced its seizure of AlphaBay in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another person's identity. Other marketplaces, similar to the now-defunct AlphaBay, "are awash with [SPI] belonging to victims from countries all over the world. One of the key challenges of protecting SPI online is its pervasiveness. As data disclosures in the news continue to show, SPI about employees, customers and the public is housed in all kinds of organizations, and the increasing digital transformation of today's businesses only broadens the number of potential sources for hackers to target."[11]

---

[9] Al Pascual, *2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters*, JAVELIN (Feb. 20, 2013), https://javelinstrategy.com/research/2013-identity-fraud-report-data-breaches-becoming-treasure-trove-fraudsters (last visited Aug. 29, 2022).

[10] *Shining a Light on the Dark Web with Identity Monitoring*, IDENTITYFORCE (Feb. 2, 2020), https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last visited Aug. 29, 2022).

[11] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, ARMOR (April 3, 2018), https://res.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/ (last visited Aug. 29, 20221).

61. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[12] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[13] Criminals can also purchase access to entire company data breaches for $900 to $4,500.[14]

62. Some of the information compromised in the Data Breach here is significantly more valuable than the loss of, for example, credit card information because there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach—names, dates of birth, driver's license numbers and Social Security numbers, etc.—is difficult, if not impossible, to change.

63. Social Security numbers are among the worst kind of personal information to have stolen because they can be misused so many different ways and are very difficult to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[15]

---

[12] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs,* DIGITAL TRENDS (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Aug. 29, 2022).

[13] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Aug. 29, 2022).

[14] *In the Dark*, VPNOverview (2019), https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Aug. 29, 2022).

[15] Social Security Administration, *Identity Theft and Your Social Security Number*, https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Aug. 29, 2022).

64. It is no easy task to change or cancel a stolen Social Security number. Plaintiffs and the Class members cannot obtain new Social Security numbers without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

65. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[16]

66. Driver's license numbers are also incredibly valuable. "Hackers harvest license numbers because they're a very valuable piece of information. A driver's license can be a critical part of a fraudulent, synthetic identity – which go for about $1200 on the Dark Web. On its own, a forged license can sell for around $200."[17]

67. National credit reporting company, Experian, blogger Sue Poremba also emphasized the value of a 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.[18]

---

[16] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited Aug. 29, 2022).

[17] Lee Mathews, *Hackers Stole Customers' License Numbers from Geico in Months-Long Breach*, FORBES (April 20, 2021), https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3066c2218658 (last visited Aug. 29, 2022).

[18] Sue Poremba, *What Should I do If My Driver's License Number Is Stolen?*, EXPERIAN (Oct. 24, 2018), http://web.archive.org/web/20211015201626/https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/ (last visited Aug. 29, 2022).

68. 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."[19] Tim Sadler, CEO of email security firm Tessian, told CPO Magazine 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 . . . . [B]ad 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.[20]

69. Driver's license numbers have been taken from auto-insurance providers by hackers in other circumstances, indicating both that this particular form of SPI 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.[21]

---

[19] Scott Ikeda, *Geico Data Breach Leaks Driver's License Numbers, Advises Customers to Watch Out for Fraudulent Unemployment Claims*, CPOMAGAZINE (April 23, 2021), https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/ (last visited Aug. 29, 2022).

[20] *Id*.

[21] *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 (last visited Aug. 29, 2022) (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), https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html (last visited Aug. 29, 2022) (describing a scam involving drivers' license numbers and Progressive Insurance).

70. The data stolen in this case commands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x in price on the black market."[22]

71. Once SPI is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional PI and SPI being harvested from the victim, as well as PI and SPI from family, friends, and colleagues of the original victim.

72. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than $3.5 billion in losses to individuals and business victims.

73. Victims of driver's license number theft also often suffer unemployment benefit fraud, harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

B. Defendants failed to comply with Federal Trade Commission requirements for data security

74. Federal and State governments have established security standards and issued recommendations to minimize data disclosures and the resulting harm to individuals and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for businesses that highlight the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[23]

75. In 2016, the FTC updated its publication, *Protecting Personal Information: A*

---

[22] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, NETWORK WORLD (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Aug. 29, 2022).

[23] *See* Federal Trade Commission, *Start With Security: A Guide for Business* (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Aug. 29, 2022).

Guide for Business, which established guidelines for fundamental data security principles and practices for businesses.[24] Among other things, the guidelines note businesses should properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[25]

76. Additionally, the FTC recommends that companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[26]

77. Highlighting the importance of protecting against data disclosures, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect personally identifiable information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[27]

78. Through their negligence in securing Plaintiffs' and Class members' PI and SPI, Defendants failed to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and the Class members' PI and SPI. Defendants' data security policies and

---

[24] *See* Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Aug. 29, 2022).

[25] *Id.*

[26] Federal Trade Commission, *Start With Security*, *supra,* note 23.

[27] Federal Trade Commission, *Privacy and Security Enforcement Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited Aug. 29, 2022).

practices constitute unfair acts or practices prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45, in addition to violation of the Drivers' Privacy Protection Act, 18 U.S.C. § 2724 ("DPPA").

C. Plaintiffs and the Class members suffered damages as a result of Defendants' failure to protect their PI and SPI

79. Plaintiffs and Class members suffer a present and continuing risk of actual identity theft in addition to all other forms of fraud.

80. The PI and SPI belonging to Plaintiffs and Class members is private and sensitive in nature. Defendants failed to obtain Plaintiffs' and Class members' consent to disclose such PI and SPI to any other person as required by applicable law and industry standards.

81. Defendants' inattention to the possibility that anyone could obtain the PI and SPI of any customer or potential customer of Defendants left Plaintiffs and Class members with no ability to protect their sensitive and private information.

82. Defendants had the resources necessary to prevent the Data Breach, but neglected to adequately implement data security measures, despite their obligations to protect PI and SPI of Plaintiffs and Class members from unauthorized disclosure.

83. Had Defendants remedied the deficiencies in their data security systems and adopted security measures recommended by experts in the field, they would have prevented the intrusions into their systems and, ultimately, the theft of PI and SPI.

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

85. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more

than a year for some victims."[28]

86. As a result of Defendants' failures to prevent the Data Breach, Plaintiffs and Class members have suffered, will suffer, and are at increased risk of suffering:

a. The compromise, publication, theft, and/or unauthorized use of their PI and SPI;

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

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

d. The present and continuing risk to their PI and SPI, which remain in the possession of Defendants and is subject to further breaches so long as Defendants fail to undertake appropriate measures to protect the PI and SPI in their possession; and

e. Current and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, remediate, and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Class members.

f. Emotional distress, anguish, and worry about their PI and SPI being sold on the dark web, being in the possession of malicious actors, and being misused.

87. In addition to a remedy for the economic harm, Plaintiffs and the Class members maintain an undeniable interest in ensuring that their PI and SPI are secure, remains secure, and is not subject to further misappropriation and theft. Plaintiffs therefore requests the injunctive remedies outlined in the Prayer of this Complaint.

/ / /

/ / /

[28] U.S. Department of Justice, OFFICE OF JUSTICE PROGRAMS BUREAU OF JUSTICE STATISTICS, *Victims of Identity Theft, 2012*, December 2013, https://www.bjs.gov/content/pub/pdf/vit12.pdf (last visited Oct. 13, 2021).

CLASS ALLEGATIONS

88. Pursuant to Cal. Code Civ. Proc. § 382, Plaintiffs seek certification of the following national class ("Nationwide Class"):

> All persons residing in the United States whose PI and/or SPI, as defined herein, was compromised in the Data Breach that Defendants VGoA and Audi announced in June 2021.

89. Pursuant to Cal. Code Civ. Proc. § 382, Plaintiffs seek certification of the following California state subclass ("California Subclass"):

> All persons residing in the State of California whose PI and/or SPI, as defined herein, was compromised in the Data Breach that Defendants VGoA and Audi announced in June 2021.

90. The Nationwide Class and California Subclass are collectively referred to herein as the "Class" unless otherwise stated.

91. Excluded from the proposed Class are the Defendants, including their corporate affiliates and any entities in which they have a controlling interest or that are controlled by Defendants, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendants.

92. Plaintiffs reserve the right to amend or modify the Class definitions with greater specificity or division, or create and seek certification of additional classes, after having had an opportunity to conduct discovery.

93. **Numerosity.** Although the exact number of Class members is uncertain, Defendants have reported it to be around 3.3 million people. This number is clearly great enough that joinder is impracticable. The disposition of the claims of these Class members in a single action will provide substantial benefits to all parties and to the Court. The Class members may be identified by objective means, such as through information and records in Defendants' possession, custody, or control.

94. **Commonality and Predominance.** Common questions of law and fact exist as to the proposed Class members and predominate over questions affecting only individual Class members. These common questions include:

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

b. Whether Defendants' data security measures to protect Plaintiffs' and Class members' PI and SPI were reasonable in light of industry standards, the sensitivity of the information involved, the known threats to PI and SPI, the FTC data security recommendations, applicable cybersecurity standards, and best practices recommended by data security experts;

c. Whether Defendants violated the California and Florida state laws identified herein;

d. Whether Defendants' failure to implement adequate data security measures resulted in or was the proximate cause of the Data Breach;

e. Whether Defendants' conduct, including their failure to act, was a legal cause of the loss of PI and SPI of Plaintiffs and Class members;

f. Whether Defendants owed a legal duty to Plaintiffs and Class members to exercise due care in collecting, storing, and safeguarding their PI and SPI;

g. Whether Defendants negligently or recklessly breached legal duties owed to Plaintiffs and the other Class members to exercise due care in collecting, storing, and safeguarding their PI and SPI;

h. Whether Plaintiffs and the other Class members are entitled to actual, statutory, or other forms of damages, and other monetary relief; and

i. Whether Plaintiffs and the other Class members are entitled to equitable relief, including, but not limited to, injunctive relief and restitution.

95. **Typicality**. Plaintiffs' claims are typical of the claims of the Class members. All Class members were subject to the Data Breach and had their PI and SPI accessed by and/or disclosed to unauthorized third parties.

96. **Adequacy of Representation.** Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the other Class members they seek to represent, they have retained counsel competent and experienced in complex class action litigation, and Plaintiffs will prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and their counsel.

97. **Superiority.** 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 matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiffs and the other Class members are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendants, making it impracticable for Class members to individually seek redress for Defendants' wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments and increase 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 single adjudication, economies of scale, and comprehensive supervision by a single court.

FIRST CAUSE OF ACTION
Negligence
(On behalf of the Nationwide Class)
(Against all Defendants)

98. Plaintiffs incorporate by reference the allegations in paragraphs 1 through 97 as though fully set forth herein.

99. Plaintiffs bring this claim against Defendants on behalf of themselves and the Nationwide Class.

100. Defendants owed a duty to Plaintiffs and the Class to exercise reasonable care in securing, safeguarding, storing, and protecting Plaintiffs' and Class members' PI and SPI from being compromised, lost, stolen, and accessed by unauthorized persons. This duty includes, among

other things, designing, maintaining, and testing their data security systems to ensure that Plaintiffs' and Class members' PI and SPI in Defendants' possession was and is adequately secured and protected. Defendants also owed a duty to ensure that they have adequate intrusion detection systems so that they can timely detect intrusions into their systems and networks and can take appropriate corrective action.

101. Additionally, Defendants owed a duty to confirm that any affiliates, vendors, or third parties whom Defendants entrust to manage, store, and secure the PI and SPI provided to Defendants by their customers have adequate security for that PI and SPI, follow industry standards and laws relating to safeguarding PI and SPI, have properly segregated that PI and SPI, have securely encrypted that PI and SPI, and otherwise prioritize data security in a way that will ensure the PI and SPI is secure from cyber threats and malicious actors.

102. Defendants owed a duty of care to Plaintiffs and members of the Class because they were foreseeable and probable victims of any inadequate data security practices. Defendants knew or should have known of the inherent risks in collecting and storing the PI and SPI of Plaintiffs and Class members and the critical importance of adequately securing such information.

103. Plaintiffs and members of the Class entrusted Defendants with their PI and SPI with the understanding that Defendants would safeguard their information. Defendants were in a position to protect against the harm suffered by Plaintiffs and members of the Class as a result of the Data Breach whereas Plaintiffs and the Class members were dependent on Defendants for that protection.

104. Defendants' actions created a foreseeable risk of harm to Plaintiffs and Class members. Defendants' misconduct included failing to implement the systems, policies, and procedures necessary to prevent the Data Breach, failing to properly encrypt or redact the PI and SPI, failing to implement systems that could timely detect intrusions into their systems by threat actors, failing to train their personnel to recognize and respond to data security risks, or failing to ensure that parties entrusted by Defendants to store, manage, and secure the PI and SPI of Plaintiffs and the Class had those systems and procedures in place.

105. Defendants knew, or should have known, of the risks inherent in collecting and storing PI and SPI and the importance of adequate security. Defendants knew about – or should have been aware of - numerous, well-publicized data breaches affecting businesses that store PI and SPI in the United States.

106. Defendants also had independent duties under state and federal laws that required Defendants to reasonably safeguard Plaintiffs' and Class members' PI and SPI. These duties are non-delegable.

107. Defendants breached their duties to Plaintiffs and Class members by failing to provide reasonable or adequate computer systems and data security to safeguard the PI and SPI of Plaintiffs and Class members.

108. Furthermore, Defendants negligently entrusted Plaintiffs' and the Class members' PI and SPI to third party vendors and service providers without taking adequate steps to ensure they had the systems and protocols in place to protect that PI and SPI from theft or disclosure.

109. Through Defendants' acts and omissions, including Defendants' failure to provide adequate security and its failure to protect Plaintiffs' and Class members' PI and SPI from being foreseeably accessed, Defendants unlawfully breached their duty to use reasonable care to adequately protect and secure the PI and SPI of Plaintiffs and Class members.

110. In engaging in the negligent acts and omissions as alleged herein, which permitted an unknown third party to exfiltrate Plaintiffs' and Class members' PI and SPI and then misuse it, Defendants violated Section 5 of the FTC Act, which prohibits "unfair . . . practices in or affecting commerce." This prohibition includes failing to have adequate data security measures and failing to protect Plaintiffs' and Class members' PI and SPI. Defendants also violated the Drivers' Privacy Protection Act, 18 U.S.C. § 2724 ("DPPA"), in that they disclosed the driver's license numbers of Plaintiffs and the Class members to unauthorized third parties.

111. Plaintiffs and the Class members are among the class of persons Section 5 of the FTC Act and the DPPA were designed to protect, and the injuries suffered by Plaintiffs and the Class members is the type of injury those laws were intended to prevent.

112. Neither Plaintiffs nor any of the Class members contributed to the Data Breach as described in this Complaint.

113. As a direct and proximate cause of Defendants' negligent conduct, Plaintiffs and Class members have suffered and/or will suffer injury and damages, including: (i) actual instances of identity fraud or similar misuse of their PI and SPI; (ii) loss of their benefit of the bargain with Defendants; (iii) the publication, theft, or misuse of their PI and SPI, including instances of identity fraud or similar misconduct; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PI and SPI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (viii) the present and continuing risk to their PI and SPI, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect that PI and SPI in their continued possession; and, (ix) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PI and SPI for the rest of their lives.

SECOND CAUSE OF ACTION
Breach of Implied Contract
(On behalf of the Nationwide Class)
(Against Defendants VGoA and Audi)

114. Plaintiffs incorporate by reference the allegations from Paragraphs 1 through 97 as though fully set forth herein.

115. Plaintiffs bring this claim against Defendants VGoA and Audi on behalf of themselves and the Nationwide Class.

116. Defendants provided automobile products and services to Plaintiffs and Class members in exchange for compensation and other benefits. In so doing, Defendants either required

Plaintiffs and Class members to provide their PI and SPI or acquired their PI and SPI with the authorization of Plaintiffs and the Class members.

117. Implied in these exchanges was a promise by Defendants to ensure that the PI and SPI of Plaintiffs and Class members in their possession was only used to provide the agreed-upon services and other benefits from Defendants.

118. Defendants were therefore required to reasonably safeguard and protect the PI and SPI of Plaintiffs and Class members from unauthorized disclosure or use.

119. Plaintiffs and Class members accepted Defendants' offers for products and services and fully performed their obligations under the implied contract with Defendants by providing their PI and SPI, directly or indirectly, to Defendants.

120. Plaintiffs and Class members would not have provided and entrusted their PI and SPI to Defendants in the absence of their implied contracts with Defendants, and would have instead retained the opportunity to control their PI and SPI for uses other than products and services from Defendants.

121. Defendants breached their implied contracts with Plaintiffs and Class members by failing to reasonably safeguard and protect Plaintiffs' and Class members' PI and SPI.

122. As a proximate and direct result of Defendants' breaches of their implied contracts with Plaintiffs and Class members, Plaintiffs and the Class members suffered economic damages as described in detail above.

THIRD CAUSE OF ACTION
Violation of California's Consumer Privacy Act, Cal. Civ. Code § 1798.150
(On behalf of the California Subclass)
(Against all Defendants)

123. Plaintiffs incorporate by reference the allegations from paragraphs 1 through 97 as though fully set forth herein.

124. Plaintiff Villalobos brings this claim against Defendants on behalf of himself and the California Subclass.

125. Defendants are corporations organized for the profit or financial benefit of their owners and have annual gross revenues exceeding $25 million and collect SPI as defined in Cal. Civ. Code § 1798.140. In addition, Defendants annually buy, receive, sell, or share for commercial purposes the SPI of more than 50,000 consumers.

126. Defendants violated section 1798.150(a) of the California Consumer Privacy Act ("CCPA") by failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the SPI of Plaintiffs and the California Subclass. As a direct and legal result, Plaintiffs' and the California Subclass' nonencrypted and nonredacted SPI, including but not limited to driver's license numbers and Social Security numbers, was subject to unauthorized access and exfiltration, theft, or disclosure.

127. As a direct and proximate result of Defendants' acts, Plaintiffs and the California Subclass members were injured and lost money or property, including the loss of benefit of the bargain, the loss of their legally protected interest in the confidentiality and privacy of their SPI, nominal damages, and additional losses as described above.

128. Plaintiffs and California Subclass members seek injunctive or other equitable relief to ensure Defendants hereinafter adequately safeguard Plaintiffs' and the California Subclass members' SPI by implementing reasonable security procedures and practices. Such relief is particularly important because Defendants continue to hold Plaintiffs' and California Subclass members' SPI. These individuals have an interest in ensuring that their SPI is reasonably protected.

129. On or about June 28, 2021, Plaintiff Villalobos sent Defendants VGoA and Audi via certified mail the 30-day notice letter as required under Civil Code 1798.150(b). Because Defendants VGoA and Audi have not cured, and cannot cure, the results of their violations of the CCPA, Plaintiff Villalobos and the California Subclass members seek statutory damages against these Defendants under California Civil Code section 1798.150(b).

130. On or about August 6, 2021, Plaintiff Villalobos sent Defendant Shift Digital via certified mail the 30-day notice letter as required under California Civil Code 1798.150(b).

Because Defendant Shift Digital has not cured, and cannot cure, the results of its violations of the CCPA, Plaintiff and Villalobos and the California Subclass members seek statutory damages against this Defendant under Civil Code section 1798.150(b).

FOURTH CAUSE OF ACTION
Violation of California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq.*
(On behalf of the California Subclass)
(Against all Defendants)

131. Plaintiffs incorporate by reference the allegations from paragraphs 1 through 97 as though fully set forth herein.

132. Plaintiffs Hajny and Villalobos bring this claim against Defendants on behalf of themselves and the California Subclass.

133. Defendants have violated Cal. Bus. and Prof. Code § 17200, *et seq*., by engaging in unlawful and unfair acts and practices that constitute acts of "unfair competition" as defined in Cal. Bus. Prof. Code § 17200 with respect to the services provided to the Class.

Unlawful Business Practices

134. Defendants engaged in unlawful acts and practices with respect to the services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting the PI and SPI of Plaintiffs and California Subclass members with knowledge that the information would not be adequately protected; and by storing the PI and SPI of Plaintiffs Hajny and Villalobos and the California Subclass members in an unsecure environment in violation of the DPPA, 18 U.S.C. § 2724, and Section 5 of the FTC Act, 15 U.S.C. § 45, which require Defendants to employ reasonable methods of safeguarding the PI and SPI of Plaintiffs and the California Subclass.

135. As a direct and proximate result of Defendants' unlawful practices and acts, Plaintiffs Hajny and Villalobos and the California Subclass were injured and lost money or property, including but not limited to the price received by Defendants for the services, the loss of Plaintiffs Hajny's and Villalobos' and the California Subclass' legally protected interest in the

confidentiality and privacy of their PI and SPI, nominal damages, and additional losses as described above.

136. Defendants knew or should have known that their data security practices were inadequate to safeguard the PI and SPI of Plaintiffs Hajny and Villalobos and the California Subclass members and that the risk of a data breach or theft was highly likely, especially given their inability to adhere to basic encryption standards, data maintenance and disposal methodologies. Defendants' actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the California Subclass.

Unfair Business Practices

137. Defendants engaged in unfair acts and practices with respect to the services they provide by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting the PI and SPI Plaintiffs Hajny and Villalobos and the California Subclass members with knowledge that the information would not be adequately protected; and by storing the PI and SPI Plaintiffs Hajny and Villalobos and the California Subclass members in an unsecure electronic environment. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs Hajny and Villalobos and the California Class members. They were likely to deceive the public into believing their PI and SPI were securely stored, when it was not. The harm these practices caused to Plaintiffs Hajny and Villalobos and the California Subclass members outweighed their utility, if any.

138. Defendants engaged in unfair acts and practices with respect to the provision of services by failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect the PI and SPI of Plaintiffs and the California Subclass from further unauthorized disclosure, release, data breaches, and theft. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs Hajny and Villalobos and the California Subclass. They were likely to deceive the public into believing their PI and SPI were securely stored when they were not. The harm these practices

caused to Plaintiffs Hajny and Villalobos and the California Subclass members outweighed their utility, if any.

139. As a direct and proximate result of Defendants' acts of unfair practices, Plaintiffs Hajny and Villalobos and the California Subclass members were injured and lost money or property, including but not limited to the price received by Defendants for the services, the loss of Plaintiffs Hajny's and Villalobos' and the California Subclass member's legally protected interest in the confidentiality and privacy of their PI and SPI, nominal damages, and additional losses as described above.

140. Defendants knew or should have known that their data security practices were inadequate to safeguard the PI and SPI of Plaintiffs Hajny and Villalobos and the California Subclass and that the risk of a data breach or theft was highly likely. Defendants' actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiffs Hajny and Villalobos and the California Subclass.

141. Plaintiffs Hajny and Villalobos and the California Subclass seek relief under Cal. Bus. & Prof. Code § 17200, *et seq*., including, but not limited to, restitution to Plaintiffs Hajny and Villalobos and the California Subclass of money or property that the Defendants may have acquired by means of their unlawful and unfair business practices, restitutionary disgorgement of all profits accruing to Defendants because of their unlawful and unfair business practices, declaratory relief, attorneys' fees and costs, and injunctive or other equitable relief.

FIFTH CAUSE OF ACTION
Breach of Contracts to which Plaintiffs and the Class are Third Party Beneficiaries
(On behalf of the Nationwide Class)
(Against Defendant Shift Digital)

142. Plaintiffs incorporate by reference the allegations from paragraphs 1 through 97 as though fully set forth herein.

143. Plaintiffs bring this claim against Defendant Shift Digital on behalf of themselves and the Nationwide Class.

144. At all times relevant, Defendant Shift Digital had express or implied contracts or agreements with several automobile manufacturers and dealers, including Defendants VGoA and Audi, to provide secure data and records management, retention, retrieval, and storage for marketing purposes.

145. Plaintiffs and the members of the Class are intended third party beneficiaries of contracts entered into between Defendant Shift Digital and these manufacturers, dealers, and other business entities because their PI and SPI are a subject of the contracts and Defendant Shift Digital agreed to keep it secure as a part of providing data and records management, retention, retrieval, and storage to its customers

146. Defendant Shift Digital breached these contracts by failing to provide secure or adequate data storage services, resulting in the Data Breach and the theft and misuse of the PI and SPI of Plaintiffs and the Class by unauthorized third persons.

147. Plaintiffs and the members of the Class have a right to recovery for the breach because one or more of the parties to these contracts intended to give Plaintiffs and the Class members the benefit of the performance promised in the contracts.

148. As a direct and proximate result of Defendant Shift Digital's breaches of these contracts, Plaintiffs and the Class members suffered the injuries as described in detail above.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually, and on behalf of all others similarly situated, respectfully request that the Court enter an order:

a. Certifying the proposed Class as requested herein;

b. Appointing Plaintiffs as Class Representatives and undersigned counsel as Class Counsel;

c. Finding that Defendants engaged in the unlawful conduct as alleged herein;

d. Enjoining Defendants' conduct and requiring Defendants to implement proper data security policies and practices; specifically:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts

described herein;

ii. requiring Defendants to protect, including through encryption, all data collected through the course of their businesses in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Plaintiffs' and the Class members' PI and SPI;

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

v. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

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

vii. requiring Defendants to conduct regular database scanning and security checks;

viii. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

ix. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and

x. requiring Defendants to design, maintain, and test their computer systems

to ensure that PI and SPI in their possession is adequately secured and protected.

e. Awarding Plaintiffs and Class members damages, including statutory damages;

f. Awarding Plaintiffs and Class members pre-judgment and post-judgment interest on all amounts awarded;

g. Awarding Plaintiffs and the Class members reasonable attorneys' fees, costs, and expenses; and

h. Granting such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and the proposed Class, hereby demand a trial by jury as to all matters so triable.

DATED: August 30, 2022

WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP

By, Rachele R. Byrd
RACHELE R. BYRD

Rachele R. Byrd
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP
750 B Street, Suite 1820
San Diego, California
Telephone: (619) 239-4599
Facsimile: (619) 234-4599
byrd@whafh.com

Gayle M. Blatt
CASEY GERRY SCHENK FRANCAVILLA BLATT & PENFIELD, LLP
110 Laurel Street
San Diego, California 92101
Telephone: (619) 238-1811
Facsimile: (619) 544-9232
gmb@cglaw.com

M. Anderson Berry
Gregory Haroutunian
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829
aberry@justice4you.com
gharoutunian@justice4you.com

Karen Hanson Riebel
Kate M. Baxter-Kauf
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Avenue S, Suite 2200
Minneapolis, MN 55401
Telephone: (612) 339-6900
Facsimile: (612) 339-0981
khriebel@locklaw.com
kmbaxter-kauf@locklaw.com

Attorneys for Plaintiffs and the Class