TINA WOLFSON (SBN 174806)
*twolfson@ahdootwolfson.com*
ROBERT AHDOOT (SBN 172098)
*rahdoot@ahdootwolfson.com*
THEODORE MAYA (SBN 223242)
*tmaya@ahdootwolfson.com*
**AHDOOT & WOLFSON, PC**
2600 W. Olive Avenue, Suite 500
Burbank, CA 91505-4521
Telephone: 310.474.9111
Facsimile: 310.474.8585

ANDREW W. FERICH (*pro hac vice* to be filed)
*aferich@ahdootwolfson.com*
**AHDOOT & WOLFSON, PC**
201 King of Prussia Road, Suite 650
Radnor, PA 19087
Telephone: 310.474.9111
Facsimile: 310.474.8585

*Attorneys for Plaintiff and the Proposed Class*

**UNITED STATES DISTRICT COURT**
**FOR THE CENTRAL DISTRICT OF CALIFORNIA**

| | |
|---|---|
| BARBARA TREVINO, individually and on behalf of all others similarly situated,<br><br>Plaintiff,<br><br>v.<br><br>AUTOMATIC FUNDS TRANSFER SERVICES, INC.,<br><br>Defendant. | Case No.<br><br>**CLASS ACTION COMPLAINT**<br><br>**JURY TRIAL DEMANDED** |

Plaintiff Barbara Trevino ("Plaintiff"), individually and on behalf of all others similarly situated, upon personal knowledge of facts pertaining to herself and on information and belief as to all other matters, by and through undersigned counsel, brings this Class Action Complaint against Defendant Automatic Funds Transfer Services, Inc. ("AFTS" or "Defendant").

## NATURE OF THE ACTION

1. Plaintiff brings this class action on behalf of herself and millions other individuals in California ("Class Members") whose private and confidential information, including names, addresses, license plate numbers, and vehicle identification numbers ("VIN") (collectively, "Personal Information") were knowingly stored by AFTS on its unsecured systems and accessed by and disclosed to unauthorized third parties during a ransomware attack (the "Data Breach").

2. Reports indicate that Personal Information for as many as 38 million Class Members, which the California Department of Motor Vehicles ("California DMV") provided to AFTS, including the last 20 months of California vehicle registration records, may have been compromised in the Data Breach.

3. The harm caused to California citizens by the Data Breach is not speculative—already, reports are indicating that a criminal "ransomware gang" operating under the name "Cuba" is selling off data stolen during the Data Breach on the dark web.[1]

4. As a result of the Data Breach, Plaintiff and Class Members' privacy has been invaded, their Personal Information is now in the hands of criminals (who are already selling the data), they face a substantially increased risk of identity theft and fraud, and they must take immediate and time-consuming action to protect themselves from such identity theft and fraud.

[1] https://gizmodo.com/ransomware-gang-says-its-selling-data-from-cyberattack-1846307574 (last visited Feb. 19, 2021).

5. The acts of AFTS, as described more particularly below, were in violation of the Driver's Privacy Protection Act, 18 U.S.C. § 2721, *et seq.* ("DPPA") and the California Consumer Privacy Act, Cal. Civ. Code § 1798.100, *et seq.* ("CCPA").

## PARTIES

6. Plaintiff Barbara Trevino is a citizen of California and resides in Los Angeles County. On November 12, 2020, Plaintiff registered her vehicle with the California DMV.

7. Defendant Automatic Funds Transfer Services, Inc., has a principal place of business located in Seattle, Washington.

## JURISDICTION AND VENUE

8. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331, because this civil action arises under statutes of the United States, specifically the Driver's Privacy Protection Act, 18 U.S.C. § 2721, *et seq.* This Court also has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332 of the Class Action Fairness Act of 2005 because: (i) there are 100 or more class members, (ii) there is an aggregate amount in controversy exceeding $5,000,000, exclusive of interest and costs, and (iii) there is minimal diversity because at least one plaintiff and one defendant are citizens of different states. This Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

9. The Court has personal jurisdiction over AFTS because AFTS does business in California and on information and belief is authorized to do business in California, and AFTS has sufficient minimum contacts with and otherwise intentionally avails itself of the markets in California through its promotion, marketing, and sale of payment and invoice processing and address verification services.

10. Venue properly lies in this district pursuant to 28 U.S.C. § 1391, because a substantial part of the events giving rise to the claims occurred in this judicial district and Plaintiff resides in this judicial district.

## FACTUAL ALLEGATIONS

11. AFTS is a Seattle-based company that provides address verification services, including to the California DMV for addresses associated with motor vehicle registrations. AFTS is used across the United States to process payments, invoices, and verify addresses. It has provided services to the California DMV since 2019.

12. On Wednesday, February 17, 2021, the California DMV announced that a massive ransomware attack in February 2021 impacted AFTS, warning drivers in the state of California about the Data Breach and the potential impact it could have on their sensitive information.

13. In a statement, the California DMV said that the attack may have compromised "the last 20 months of California vehicle registration records that contain names, addresses, license plate numbers and vehicle identification numbers."

14. The Data Breach is massive in its impact on drivers owning or leasing motor vehicles registered in the state of California. Anita Gore, a spokeswoman for the California DMV, identified that "[a]pproximately 38 million records have potentially been compromised."

15. The California DMV confirmed it has since stopped all data transfers to AFTS and has since initiated an emergency contract to prevent any downtime.

16. At this time, the California DMV does not know the actual extent and scope of the impact on DMV customers, but is emphasizing that drivers take precaution while the FBI conducts an investigation into the Data Breach.

17. The harm caused to California citizens by the Data Breach is already apparent. Just two days after the California DMV announced the breach, reports have surfaced that a criminal "ransomware gang" operating under the name "Cuba" is selling off data stolen during the Data Breach on the dark web.[2]

[2] https://gizmodo.com/ransomware-gang-says-its-selling-data-from-cyberattack-1846307574 (last visited Feb. 19, 2021).

18. While it is currently unknown what kind of ransomware was used during the AFTS breach, the impact of the Data Breach may extend to other customers to which AFTS provided services across the country. Several municipalities have already confirmed that they are affected by the Data Breach, suggesting it may not be limited to California's DMV.

19. To date, AFTS has not provided individuals who may have been impacted by the Data Breach with any guidance. As of present, AFTS's website appears to offline, and displays only the following short message: "The website for AFTS and all related payment processing website [sic] are unavailable due to technical issues. We are working on restoring them as quickly as possible."[3]

20. Ransomware attacks are nothing new. These types of attacks should be anticipated by companies that store sensitive and personally identifying information, and companies storing this type of data must ensure that data privacy and security is adequate to protect against and prevent ransomware and other types of known attacks.

21. Ransomware typically encrypts a company's files and will unlock those files in exchange for payment of a ransom. But since many companies have backup systems and files, some ransomware groups threaten to publish the stolen files online unless the ransom is paid.

22. It is well known amongst companies that store sensitive personally identifying information that sensitive information, like the Personal Information stolen in the Data Breach, is valuable and frequently targeted by criminals. In a recent article, *Business Insider* noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers . . . . Many of them were caused by flaws in . . . systems either online or in stores."[4]

---

[3] http://www.afts.com (last visited February 19, 2021).

[4] Dennis Green and Mary Hanbury, *If you bought anything from these 11 companies in the last year, your data may have been stolen*, BUSINESS INSIDER (Nov. 19, 2019), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.

23. Despite the known risk of data breaches and the widespread publicity and industry alerts regarding other notable (similar) data breaches, AFTS failed to take reasonable steps to adequately protect its systems from being breached.

24. AFTS is, and at all relevant times has been, aware that the sensitive Personal Information it maintains regarding driver registrations is highly sensitive. As a company that provides address verification and other services involving highly sensitive and identifying information, AFTS is aware of the importance of safeguarding that information and protecting its systems from vulnerabilities, such as a ransomware attack.

25. AFTS was aware, or should have been aware, of regulatory and industry guidance regarding data security, and it was alerted to the risk associated with failing to ensure that its computer and other systems were adequately secured.

26. Despite the well-known risks of a ransomware and other similar intrusion, AFTS failed to maintain its data security systems in a meaningful way in order prevent breaches, including the Data Breach.

27. AFTS's security flaws run afoul of industry best practices and standards. Had AFTS maintained its information technology systems, adequately protected them, and had adequate security safeguards in place, it could have prevented the Data Breach.

28. Despite the fact that AFTS was on notice of the very real possibility of data theft associated with its security practices and that AFTS knew or should have known about the elementary infirmities associated with its security systems, it still failed to make necessary changes to its security practices and protocols, and permitted a massive intrusion to occur that allegedly exposed Personal Information for upwards of 38 million drivers in California.

29. AFTS permitted Class Members' Personal Information to be compromised by failing to take reasonable steps against an obvious threat.

30. Industry experts are clear that a data breach is indicative of data security failures. Indeed, industry-leading research and advisory firm Aite Group has identified

that: "If your data was stolen through a data breach that means you were somewhere out of compliance" with payment industry data security standards.[5]

31. Because data breaches are so common, and given the high level of data security measures available to companies that take in sensitive and identifying information, there is no reason why AFTS could not have adequately protected its systems and servers from the Data Breach.

32. As a result of the events detailed herein, Plaintiff and class members suffered harm and loss of privacy, and will continue to suffer future harm, resulting from the Data Breach, including but not limited to: invasion of privacy; loss of privacy; loss of control over personal information and identities; fraud and identity theft; unreimbursed losses relating to fraud and identity theft; loss of value and loss of possession and privacy of Personal Information; harm resulting from damaged credit scores and information; loss of time and money preparing for and resolving fraud and identity theft; loss of time and money obtaining protections against future identity theft; and other harm resulting from the unauthorized use or threat of unauthorized exposure of Personal Information.

33. Congress has acknowledged the need to protect the privacy of personal information contained in an individual's motor vehicle record (such as the Personal Information at issue here), including the driver's name, address, phone number, Social Security number, driver identification number, photograph, height, weight, gender, age, certain medical or disability information, and in some states, fingerprints.

34. In 1994, Congress enacted the Driver's Privacy Protection Act ("DPPA") 18 U.S.C. §§ 2721-2725, to protect the privacy of personal information[6] gathered by state

---

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

[6] "'[P]ersonal information' means information that identifies an individual, including an individual's photograph, social security number, driver identification number, name, address, (but not the 5-digit zip code), telephone number, and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver's status." 18 U.S.C. § 2725(3).

departments or bureaus of motor vehicles. The DPPA was passed in reaction to the series of abuses of drivers' personal information held by government. *See, e.g.*, 140 Cong. Rec. H2,518, H2, 522-24 (daily ed. Apr. 20, 1994) (statement of Rep. Moran) (In Iowa, a gang of thieves copied down the license plate numbers of expensive cars they saw, found out the names and addresses of the owners and robbed their homes at night. In Virginia, a woman regularly wrote to the DMV, provided the license plate numbers of drivers and asked for the names and addresses of the owners who she claimed were stealing the fillings from her teeth at night."); 139 Cong. Rec. S15,745, S15,766 (daily ed. Nov. 16, 1993) (statement of Sen. Harkin) (recounting the store of a woman who visited an obstetrics clinic and received a "venomous letter" from anti-abortion activists who "got her name and address from department of transportation records, after they spotted her car parked near [the] clinic"); *Protecting Driver Privacy: Hearing on H.R. 3365 Before the Subcomm. On Civil & Constitutional Rights*, 1994 WL 212698 (Feb. 3, 1994) statement of Rep. Moran) ("While the release of this information to direct marketers does not pose any inherent safety risks to people, it does present, to some people, an invasion of privacy.").

35. The purpose of the DPPA is to regulate the disclosure and resale of personal information contained in the records of state DMVs. As relevant here, the DPPA underscores the value of that personal information and, critically, the significant threats to individuals' privacy rights when that personal information is released—even sold for significant revenues—to third parties.

36. Furthermore, the California Consumer Privacy Act was enacted in order to enhance privacy rights and consumers protection for individuals residing in the state of California. AFTS's data security failures run afoul of both the letter and spirit of these statutes, exposing the sensitive Personal Information of millions upon millions of people in California to unauthorized persons and criminals with nefarious intent.

37. As a result of AFTS's data privacy failures, Plaintiff and Class Members' privacy has been invaded, their Personal Information is now in the hands of criminals,

they face a substantially increased risk of identity theft and fraud, and they must take immediate and time-consuming action to protect themselves from such identity theft and fraud.

## CLASS ALLEGATIONS

38. Pursuant to Fed. R. Civ. P. 23, Plaintiff brings this action individually and on behalf of the following class of individuals (the "Class"):

> All persons whose California motor vehicle registration information was disclosed to unauthorized persons as a result of a ransomware attack on AFTS's unsecured servers and systems that was announced February 17, 2021.

39. Excluded from the Class are AFTS and its affiliates, officers, directors, assigns, successors, and the Judge(s) assigned to this case.

40. **Numerosity**: Because the Class is estimated to include more than 38 million individuals, joinder of all Class members is impracticable and the numerosity requirement is satisfied.

41. **Typicality**: Plaintiff's claims are typical of Class Members' claims. Plaintiff and all Class members were injured through AFTS's uniform misconduct—the storage of their Personal Information in an unsecured manner and exposure of that information to unauthorized individuals—and assert identical claims against AFTS. Accordingly, Plaintiff's claims are typical of Class members' claims.

42. **Adequacy**: Plaintiff's interests are aligned with the Class she seeks to represent and has retained counsel with significant experience prosecuting complex class action cases, including cases involving alleged privacy and data security violations. Plaintiff and counsel intend to prosecute this action vigorously. The Class's interests are well-represented by Plaintiff and undersigned counsel.

43. **Superiority**: A class action is the superior—and only realistic—mechanism to fairly and efficiently adjudicate Plaintiff's and other Class Member's claims. The injury suffered by each individual Class member is relatively small in comparison to the

burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for class members individually to effectively redress AFTS's wrongdoing. Even if Class Members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

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

- whether AFTS engaged in the wrongful conduct alleged herein;
- whether AFTS knowingly disclosed Plaintiff's and other Class Members' Personal Information for a purpose not permitted under the DPPA;
- whether AFTS violated the California Consumer Privacy Act by disclosing Plaintiff's and Class Members' Personal Information;
- whether AFTS violated privacy rights under the California Constitution; and
- whether Plaintiff and Class Members are entitled to damages, equitable relief, or other relief and, if so, in what amount.

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

## CAUSES OF ACTION

### COUNT I
### Violations of the Driver's Privacy Protection Act
### 18 U.S.C. §§ 2721, *et seq.* ("DPPA")
### (On Behalf of Plaintiff and the Class)

46. Plaintiff realleges and incorporates all previous allegations as though fully

set forth herein.

47. The DPPA, 18 U.S.C. § 2722(a), prohibits any person, organization, or entity from knowingly obtaining or disclosing "personal information, from a motor vehicle record, for a purpose not permitted under [§ 2721(b) of the DPPA]."

48. The DPPA defines "motor vehicle record" to mean "any record that pertains to a motor vehicle operator's permit, motor vehicle title, motor vehicle registration, or identification card issued by a department of motor vehicles." 18 U.S.C. § 2725(1).

49. The DPPA defines "personal information" to mean "information that identifies an individual, including an individual's photograph, social security number, driver identification number, name, address (but not the 5-digit zip code), telephone number, and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver's status." 18 U.S.C. § 2725(3).

50. AFTS knew Plaintiff's and other Class Members' Personal Information was obtained from the California DMV.

51. In violation of the DPPA, AFTS knowingly disclosed the Personal Information of Plaintiff and approximately 38 million other Class Members by storing that information on its systems without adequate protection.

52. Consistent with the manner in which they were programmed and configured by AFTS, AFTS's unsecured systems disclosed Plaintiff's and Class Members' Personal Information to unauthorized individuals.

53. Pursuant to 18 U.S.C. § 2724(b), as a result of AFTS's violation of the DPPA, Plaintiff's and Class Members are entitled to actual damages, but not less than liquidated damages in the amount of $2,500.

**COUNT II**
**Violations of California's Consumer Privacy Act**
**Cal. Civ. Code § 1798.100, *et seq.* ("CCPA")**
**(On Behalf of Plaintiff and the Class)**

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

55. California's Consumer Privacy Act recently was enacted to protect consumers' Personal Information from collection and use by businesses without appropriate notice and consent.

56. Through the above-detailed conduct, AFTS violated the CCPA by subjecting Class Members' Personal Information to unauthorized access and exfiltration, theft, or disclosure as a result of AFTS's violation of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature and protection of that information. Cal. Civ. Code § 1798.150(a).

57. In accordance with Cal. Civ. Code §1798.150(b), prior to the filing of this Complaint, Plaintiff's counsel served AFTS with notice of these CCPA violations by certified mail, return receipt requested.

58. On behalf of Class Members, Plaintiff seeks injunctive relief in the form of an order enjoining AFTS from continuing to violate the CCPA. If AFTS fails to respond to Plaintiff's notice letter or agree to rectify the violations detailed above, Plaintiff also will seek actual, punitive, and statutory damages, restitution, attorneys' fees and costs, and any other relief the Court deems proper as a result of AFTS's CCPA violations.

**COUNT III**
**Breach of Contracts to Which Plaintiff and Class Members Were Intended Third-Party Beneficiaries**
**(On Behalf of Plaintiff and the Class)**

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

60. Upon information and belief, Plaintiff and Class Members are intended third-party beneficiaries of contracts entered into between AFTS and its customers, including the California DMV.

61. Upon further information and belief, these contracts and require, *inter alia*, that AFTS take appropriate steps to safeguard the sensitive Personal Information entrusted to it by its customers, like the California DMV, that obtain that information from Plaintiff and Class Members.

62. Plaintiff and the Class Members are intended third party beneficiaries of these contracts. Under the circumstances, recognition of a right to performance by Plaintiff and the Class Members is appropriate to effectuate the intentions of the parties to these contracts. One or more of the parties to these contracts intended to give Plaintiff and the Class Members the benefit of the performance promised in the contracts.

63. AFTS breached these agreements, which directly and/or proximately caused Plaintiff and the Class Members to suffer substantial damages.

64. Upon further information and belief, AFTS saved (or avoided spending) a substantial sum of money by knowingly failing to comply with its contractual obligations, and continues to do so.

65. Accordingly, AFTS has been unjustly enriched and Plaintiff and Class Members who have been injured are entitled to damages, restitution, disgorgement of profits and other relief in an amount to be proven at trial.

**COUNT IV**
**Invasion of Privacy and Violation of the California Constitution, art. 1, § 1 (On Behalf of Plaintiff and the Class)**

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

67. Plaintiff and Class Members had a reasonable expectation of privacy in the Personal Information that AFTS disclosed without authorization.

68. By failing to keep Plaintiff's and Class Members' Personal Information safe, and by disclosing said information to unauthorized parties for unauthorized use, AFTS invaded Plaintiff's and Class Members' privacy by, *inter alia*:

(a) intruding into Plaintiff's and Class Members' private affairs in a manner that would be highly offensive to a reasonable person; and

(b) violating Plaintiff's and Class Members' right to privacy under California Constitution, Article 1, Section 1, through the improper use of Plaintiff's and Class Members' private information properly

obtained for a specific purpose for another purpose, or the disclosure of it to some third party.

69. AFTS knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiff's and Class Members' position would consider its actions highly offensive.

70. Defendant invaded Plaintiff's and Class Members' right to privacy and intruded into Plaintiff's and Class Members' private affairs by disclosing their Personal Information to unauthorized persons without their informed, voluntary, affirmative, and clear consent.

71. As a proximate result of such unauthorized disclosures, Plaintiff's and Class Members' reasonable expectations of privacy in their Personal Information was unduly frustrated and thwarted. Defendant's conduct amounted to a serious invasion of Plaintiff's and Class Members' protected privacy interests.

72. In failing to protect Plaintiff's and Class Members' Personal Information, and in disclosing Plaintiff's and Class Members' Personal Information, AFTS acted with malice and oppression and in conscious disregard of Plaintiff's and Class Members' rights to have such information kept confidential and private.

73. Plaintiff seeks injunctive relief on behalf of the Class, restitution, and all other damages available under this Count.

## PRAYER FOR RELIEF

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

A. Certify this case as a class action pursuant to Fed. R. Civ. P. 23(a) and (b)(3), and, pursuant to Fed. R. Civ. P. 23(g), appoint Plaintiff as class representative and undersigned counsel as class counsel;

B. Award Plaintiff and Class Members actual and statutory damages to the maximum extent allowable;

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

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

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

**JURY TRIAL DEMAND**

Plaintiff, individually and on behalf of all others similarly situated, hereby requests a jury trial, pursuant to Federal Rule of Civil Procedure 38, on all claims so triable.

Dated: February 19, 2021

Respectfully submitted,

*/s/ Tina Wolfson*

TINA WOLFSON (SBN 174806)
*twolfson@ahdootwolfson.com*
ROBERT AHDOOT (SBN 172098)
*rahdoot@ahdootwolfson.com*
THEODORE MAYA (SBN 223242)
*tmaya@ahdootwolfson.com*
**AHDOOT & WOLFSON, PC**
2600 W. Olive Avenue, Suite 500
Burbank, CA 91505-4521
Telephone: 310.474.9111
Facsimile: 310.474.8585

ANDREW W. FERICH (*pro hac vice* to be filed)
*aferich@ahdootwolfson.com*
**AHDOOT & WOLFSON, PC**
201 King of Prussia Road, Suite 650
Radnor, PA 19087
Telephone: 310.474.9111
Facsimile: 310.474.8585

*Attorneys for Plaintiff and the Proposed Class*