

*Each of the Participating States filed a lawsuit similar to the example below.*

*While states' laws vary, this example illustrates the states' general allegations.*

STATE	)	IN THE STATE COURT
	)	
Plaintiff,	)	
	)	
vs.	)	
	)	
UBER TECHNOLOGIES, INC.	)	
	)	
Defendant.	)	___ JUDICIAL DISTRICT

**PLAINTIFF'S ORIGINAL PETITION**

Plaintiff, the STATE OF \_\_\_\_\_ (“Plaintiff” or “State”) acting by and through its Attorney General, brings this action against Defendant, Uber Technologies, Inc. (“Uber” or “Defendant”) alleging violations of the State’s Consumer Protection Act and Personal Information Protection Act and submits the following:

**PUBLIC INTEREST**

1. Plaintiff has reason to believe Defendant has caused adverse effects to legitimate business enterprises which lawfully conduct trade and commerce in the state and therefore, believes this action is in the public interest.

**JURISDICTION AND VENUE**

2. This action is brought by the Attorney General in the public interest pursuant to the authority granted by state consumer protection laws upon the grounds that Defendant engaged in false, deceptive, and misleading acts and practices in the course of trade and commerce.
3. This action is further brought pursuant to the state’s personal information protection laws which authorize the Attorney General to enforce violations.

4. Venue for this action properly lies in this county and court pursuant to state laws.

### **THE PARTIES**

5. Plaintiff is the state represented by its Attorney General.
6. Defendant is a Delaware corporation with its principal place of business at 1455 Market Street, San Francisco, California 94103.
7. As used herein, any reference to “Uber” or “Defendant” shall mean Uber Technologies, Inc., including all its officers, directors, affiliates, subsidiaries, and divisions, predecessors, successors, and assigns doing business in the United States.

### **TRADE AND COMMERCE**

8. At all times described below, Defendant and its agents have engaged in conduct constituting “trade” and “commerce” as defined in state law. “Trade” and “commerce” mean the advertising, offering for sale, sale, lease, or distribution of any good or service; of any property, tangible or intangible, real, personal, or mixed; and any other article, commodity, or thing of value wherever situated; and shall include any trade or commerce directly or indirectly affecting the people of this state. Uber engaged in trade and commerce in this state in that Uber is a technology company that provides a ride hailing mobile application that connects drivers with riders. Riders hail and pay drivers using the Uber platform.

### **BACKGROUND**

9. Uber’s Privacy Policy recognizes that users trust and rely on it to safeguard their personal information: “When you use Uber, you trust us with your information. We are committed to keeping that trust.” In this regard, the frequently asked questions on Uber’s Privacy Policy webpage state: “We take the security of your data seriously. Uber uses technical safeguards like encryption, authentication, fraud detection, and secure software development to protect

your information. We also have an extensive team of data security and privacy experts working around the clock to prevent theft, fraud, or abuse of your information.”

10. In November 2016, hackers contacted Uber to inform them that they had accessed and acquired Uber data and to demand payment in exchange for deleting the data.
11. Uber was able to determine the security vulnerability that the hackers had exploited and eliminate the vulnerability.
12. In December 2016, the hackers deleted the data.
13. Among the data the hackers acquired was personal information as defined in relevant state laws: name and driver’s license information pertaining to some Uber drivers.
14. Uber did not disclose the data breach to affected Uber drivers in 2016 when the breach was discovered.
15. In August 2017, Uber named a new CEO, Dara Khosrowshahi.
16. In September 2017, Khosrowshahi was informed that Uber had suffered a data breach and ordered an investigation into the data breach, hiring a third-party cyber security provider to conduct the investigation.
17. The cyber security provider verified the 2016 data breach, and, on November 21, 2017, Uber notified regulators and consumers of the 2016 breach.
18. Uber offered affected drivers free credit monitoring and identity theft protection.

**CAUSE OF ACTION I – STATE CONSUMER PROTECTION ACT**

19. The State re-alleges and incorporates by reference each and every preceding paragraph of this petition.
20. The State further alleges that Defendant has, in the conduct of trade or commerce, engaged in false, misleading, or deceptive acts or practices in violation of the State’s Consumer Protection Act by:

- a. failing to implement and maintain reasonable security practices to protect the sensitive personal information it maintains for its users;
- b. failing to disclose a data breach to affected users; and
- c. representing to users that Uber protects the sensitive personal information of its users, when in fact the hackers were able to gain access to some Uber users' personal information.

*REMEDIES UNDER STATE'S CONSUMER PROTECTION ACT*

21. The State's law authorizes the following in cases brought by the State:
  - a. The State may seek injunctive relief when it has reason to believe that any person is engaging in, has engaged in, or is about to engage in any act or practice declared to be unlawful by this subchapter, and that proceedings would be in the public interest; and
  - b. The State may seek and recover a penalty for violations of the law.

**CAUSE OF ACTION II – PERSONAL INFORMATION PROTECTION ACT (PIPA)**

22. The State re-alleges and incorporates by reference as if fully set out here the preceding paragraphs 1 through 21.
23. PIPA defines sensitive personal information as follows:
  - A. an individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted:
    - i. social security number;
    - ii. driver's license number or government-issued identification number; or
    - iii. account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; or
  - B. information that identifies an individual and relates to:

- i. the physical or mental health or condition of the individual;
  - ii. the provision of health care to the individual; or
  - iii. payment for the provision of health care to the individual.
24. PIPA provides that a business shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business.
25. PIPA further provides in relevant part that:
  - a. “Breach of system security” means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data;
  - b. A person who conducts business in this state and owns or licenses computerized data that includes sensitive personal information shall disclose any breach of system security, after discovering or receiving notification of the breach, to any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made as quickly as possible, except as provided by Subsection (d) or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system.
26. Uber conducts business in the State and owns or licenses computerized data that includes sensitive personal information as defined by PIPA.
27. The Uber information the hackers acquired included sensitive personal information as defined in the State’s law.

28. Uber violated PIPA, in that Uber suffered a breach of the security of its system data and failed to timely notify affected residents of the State of the fact that their sensitive personal information had been breached.

29. Uber further violated PIPA, in that Uber failed to implement and maintain reasonable security measures to protect sensitive personal information from unlawful use or disclosure.

*REMEDIES UNDER PERSONAL INFORMATION PROTECTION ACT*

30. PIPA authorizes the Attorney General to recover civil penalties and to obtain injunctive and equitable relief to prevent further harm to affected consumers. State law further provides that the Attorney General is entitled to recover reasonable expenses, including reasonable attorneys' fees, court costs, and investigatory costs, incurred in obtaining injunctive relief or civil penalties, or both, under this section.

**PRAYER**

**WHEREFORE**, the Plaintiff prays that this Honorable Court enter an Order:

- a. Finding that Uber has violated the State's Consumer Protection Act law by engaging in the unlawful acts and practices alleged herein;
- b. Finding that Uber has violated PIPA by engaging in the unlawful acts and practices alleged herein;
- c. Enjoining Uber from engaging in the deceptive acts and practices alleged herein;
- d. Requiring Uber to pay a civil monetary penalty as provided under state law;
- e. Granting Plaintiff any other equitable relief that the court considers appropriate to prevent any additional harm to victims of identity theft or to prevent any further violations of the State's Consumer Protection Act or PIPA;
- f. Requiring Uber to pay all costs and fees for the prosecution and investigation of this action pursuant to state law; and

- g. Providing such other and further relief as the Court deems just, proper, and equitable under the circumstances.

\_\_\_\_\_/s/\_\_\_\_\_  
**STATE ATTORNEY GENERAL**