

3. As used herein, any reference to “UBER” or “Defendant” shall mean UBER TECHNOLOGIES, INC., including all of its officers, directors, affiliates, subsidiaries and divisions, predecessors, successors and assigns doing business in the United States.

COMMERCE

4. UBER was at all times relevant hereto, engaged in trade and commerce in the State of North Carolina as defined in North Carolina’s Unfair and Deceptive Trade Practices Act, N.C.G.S. §§ 75-1.1, *et seq.*, in that UBER is a technology company that provides a ride hailing mobile application that connects drivers with riders, including in North Carolina. Riders hail and pay drivers using the UBER platform.

BACKGROUND

5. 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 states, “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.”

6. 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.

7. UBER was able to determine the security vulnerability that the hackers had exploited and eliminate the vulnerability.

8. In December 2016, the hackers deleted the data.

9. Among the data the hackers acquired was personal information pursuant to the North Carolina Identity Theft Protection Act, N.C.G.S. §§ 75-60, *et seq.*: name and driver's license information pertaining to some UBER drivers.

10. The hackers violated the North Carolina Identity Theft Protection Act, N.C.G.S. §§ 75-60, *et seq.* with respect to that personal information.

11. UBER did not disclose the data breach to affected UBER drivers in 2016 when the breach was discovered.

12. In August 2017, UBER named a new CEO, Dara Khosrowshahi.

13. 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.

14. The cyber security provider verified the 2016 data breach, and, on November 21, 2017, UBER notified regulators and consumers of the 2016 breach.

15. UBER offered affected drivers free credit monitoring and identity theft protection.

COUNT I – UNFAIR AND DECEPTIVE TRADE PRACTICES ACT

16. The preceding paragraphs are incorporated herein by reference as if the same were fully set forth.

17. UBER failed to implement and maintain reasonable security practices to protect the sensitive personal information it maintains for its users.

18. UBER failed to disclose a data breach to affected users.

19. UBER represented 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 user personal information.

20. UBER's failures to maintain reasonable security practices and protect personal information, and its representation that personal information was protected was likely to mislead consumers.

21. Defendant has therefore engaged in unfair or deceptive acts and practices in violation of North Carolina's Unfair and Deceptive Trade Practices Act, N.C.G.S. §§ 75-1.1, *et seq.*

COUNT II – IDENTITY THEFT PROTECTION ACT

22. The preceding paragraphs are incorporated herein by reference as if the same were fully set forth.

23. UBER is an owner or licensor of personal information pursuant to the North Carolina Identity Theft Protection Act, N.C.G.S. §§ 75-760, *et seq.*

24. The UBER information the hackers acquired included personal information pursuant to the North Carolina Identity Theft Protection Act, N.C.G.S. §§ 75-760, *et seq.*

25. UBER violated N.C.G.S. § 75-65 in that UBER suffered a breach of the security of its system data and failed to notify affected North Carolina residents without unreasonable delay.

PRAYER FOR RELIEF

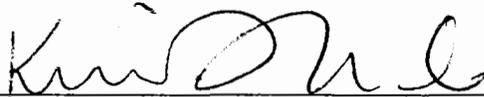
WHEREFORE, Plaintiff, State of North Carolina, respectfully requests that:

A. Pursuant to N.C.G.S. § 75-1.1, the Court permanently enjoin and restrain UBER, their agents, employees, and all other persons and entities, corporate or otherwise, in active concert or participation with any of them, from engaging in false, misleading, or deceptive practices in the handling of personal information as it pertains to UBER's ride hailing mobile application.

- B. The Court fashion equitable relief to cure UBER's deceptive practices;
- C. Pursuant to N.C.G.S. § 75-16.1, the Defendant be ordered to pay costs and reasonable attorneys' fees incurred by the State in connection with the investigation and litigation of this matter; and
- D. The Court grant such further relief as the Court deems necessary or appropriate to remedy the effects of UBER's unlawful trade practices.

Respectfully submitted this the 26th day of September, 2018.

JOSHUA H. STEIN
Attorney General



Kimberley A. D'Arruda
Special Deputy Attorney General
N.C. Department of Justice
P.O. Box 629
Raleigh, NC 27602-0629
Telephone: (919) 716-6013
Facsimile: (919) 716-6050
Email: kdarruda@ncdoj.gov
NC State Bar No.: 25271