IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
COUNTY DEPARTMENT, CHANCERY DIVISION

CITY OF CHICAGO and PEOPLE OF THE STATE OF ILLINOIS, ex rel. Kimberly M. Foxx, State's Attorney of Cook County, Illinois, *Plaintiffs*, *v.* UBER TECHNOLOGIES, INC., a Delaware corporation, *Defendant.*	Case No.

COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiffs City of Chicago ("City") and People of the State of Illinois bring this Complaint and Demand for Jury Trial against Defendant Uber Technologies, Inc. ("Uber") to seek relief on behalf of the City, its residents, and People of the State of Illinois for harm and injuries arising from and as a result of its 2016 data breach and subsequent year-long failure to disclose that breach. Plaintiffs, for their Complaint, allege as follows:

INTRODUCTION

1. For the past several years, Uber has repeatedly failed to protect the privacy of its customers' and drivers' personal information. In 2014, Uber left personal information vulnerable to a data breach at the hands of a criminal hacker, exposing the confidential and personal data of more than 50,000 users. Following the 2014 breach, Uber entered into a settlement with the government in the form of a consent decree, and promised, among other things, to correct the vulnerabilities in its data management system to protect against any further occurrences of this sort.

2. Uber never made basic corrections to its data security platform that it was required to make. Not surprisingly, in October 2016, Uber once again experienced a data breach, but this time on a massive scale—exposing the data of over 57 million users, including full names, email addresses, and certain of its users' driver's license numbers. Using a relatively low-level attack, hackers were able to access Uber's massive trove of user data stored on a third-party cloud service, by exploiting virtually the same security flaw attackers used nearly a year prior to breach its systems.

3. As if the second breach wasn't bad enough—particularly because it shows that Uber altogether ignored its obligations and agreement with the government and once again knowingly put user data at risk—the company also engaged in a cover up to keep the breach out of the public eye. The cover up is particularly egregious because as soon as Uber became aware of the breach, it had a legal duty to inform Chicago and Illinois residents (as well as millions of other individuals throughout the country) and authorities of the breach. Rather than face further backlash and lose more customers and drivers, Uber opted to cover up the breach, both within and outside the company.

4. First, Uber paid the hackers $100,000 to supposedly delete the data and took substantial legal steps to keep them from speaking about the breach publically. Uber even went so far as to hide the payment on its own books by categorizing it as a "bug bounty" payment.

5. Of course, any agreement that Uber reached with the criminal hackers was meaningless since criminal hackers couldn't possibly be trusted to protect user data. Nor did Uber require any proof that the stolen data was, in fact, deleted. That is because, in an age where thousands of copies of digital information can be made in a second, it is *impossible* for Uber to know that all copies of the data were in fact destroyed.

6. This concealment kept riders, drivers, and government agencies in the dark for over a year about Uber's substandard security practices and the risks posed to millions of people by having their personal data stolen. Had riders and drivers been aware of these events, it is unlikely they would have continued to participate in Uber's services.

7. Uber could and should have prevented the data breach by implementing and maintaining reasonable safeguards, consistent with the representations Uber made to the public in its marketing materials and privacy policies (and to the government as part of the consent decree), and compliant with industry standards, best practices, and the requirements of Illinois State and Chicago municipal law. Unfortunately, Uber failed to do so, and as a result, has exposed the personal and sensitive data of potentially tens, if not hundreds, of thousands of Chicago and Illinois residents.

8. By failing to secure personal and sensitive data—despite its legal obligations to do so—and then covering the breach up for over a year—despite its legal obligations to disclose the breaches—Uber willfully and intentionally exposed many Chicago and Illinois residents to the risks of identity theft and financial fraud, tax return scams, and other potential harm.

9. Accordingly, Plaintiffs City of Chicago and People of the State of Illinois bring this suit on behalf of themselves and their residents to seek redress for Uber's unlawful conduct. Plaintiffs seek civil penalties, restitution, and all necessary, appropriate, and available equitable and injunctive relief to address, remedy, and prevent harm to Chicago and Illinois residents resulting from Uber's misconduct.

PARTIES

10. Plaintiff City of Chicago is a municipal corporation existing under the laws of the State of Illinois.

11. Plaintiff People of the State of Illinois, by and through Kimberly M. Foxx, State's Attorney of Cook County, Illinois, brings this action in the public interest for and on behalf of the People of the State of Illinois.

12. Defendant Uber Technologies, Inc. is a corporation existing under the laws of the State of Delaware, with its headquarters and principal place of business located at 1455 Market Street, San Francisco, California 94103. Uber conducts business in Cook County.

JURISDICTION AND VENUE

13. Pursuant to the Illinois Constitution art. VI, § 9, this Court has subject matter jurisdiction over Plaintiffs' claims.

14. This Court has jurisdiction over Defendant pursuant to 735 ILCS 5/2-209 because it conducts business transactions in Illinois, maintains an office in Illinois, has committed tortious acts in Illinois, has transacted substantial business in Illinois which has caused harm in Illinois, and is registered to conduct business in Illinois.

15. Venue is proper in Cook County because Defendant conducts business transactions in Cook County and the causes of action arose, in part, in Cook County.

FACTUAL BACKGROUND

I. An Overview of Defendant Uber.

16. Defendant Uber is a transportation technology company that connects individuals who need on-demand transportation with available drivers using its proprietary mobile application, *Uber*.

17. Less than a decade since its inception, Uber now operates in over 633 cities around the world and has over 40 million monthly active riders and millions of drivers, including in the City of Chicago, Cook County, and the State of Illinois.

18. To use its service, riders must download the *Uber* application on their smartphones and register for an account, including by providing their full names, email addresses, telephone numbers, and credit card information.

19. Drivers must apply to drive with Uber—not as employees, but as independent contractors—and provide it with their full names, email addresses, mailing addresses, Social Security numbers, and U.S. driver's license numbers, among other things.

20. Uber recognizes the sensitivity of this information and, in light of that, promises to protect and keep it secure.[1] For instance, in its marketing materials, Uber promises that it "take[s] the security of [its riders' and drivers'] data seriously" and "uses technical safeguards like encryption, authentication, fraud detection, and secure software development to protect [their] information."[2] Uber intended that the public, including Chicago and Illinois residents, rely on its representations regarding the security of their data.

21. Unfortunately, as described below, Uber first breached its promises and failed to protect its riders' and drivers' personal information in 2014, and after promising to fix its vulnerabilities, failed to do so.

II. The 2014 Data Breach.

22. In May 2014, an Uber employee placed highly sensitive Amazon Web Services ("AWS")[3] login credentials—used to access a user data database—onto a software development platform called GitHub, which was used by Uber software engineers to store their code. That post, however, was not protected or confidential, and was in fact accessible to the general public.

---

1 *See, e.g.*, Uber, *Responsible Disclosure Policy*, available at https://www.uber.com/legal/security.

2 Uber, *Uber Privacy*, available at https://privacy.uber.com/#faq.

3 AWS is a cloud or remote computing services platform that provides software companies, like Uber, with database storage, content delivery, and other functionality.

23. GitHub is a source code repository that lets developers work on programs together as a team, even when they are in different locations. Each repository on the site is a public folder designed to hold the software code that a developer is working on.

24. For years prior to the 2014 breach, the development and security industries have widely understood that storing credentials on GitHub repositories increases the risk of data being breached and an eventual compromise of the companies' technological assets. Unfortunately, companies with insufficient security and privacy policies do not implement necessary controls on their source code to make sure that no sensitive information is being published to GitHub code repositories.[4]

25. As this was against all known best practices, it did not take long for hackers to access the GitHub repository and find the credentials, and thereafter access an Uber database with 50,000 names and driver's license numbers in it.

26. On September 17, 2014, Uber discovered that its customers' and drivers' sensitive personal information had been accessed without authorization.

27. Uber investigated the unauthorized use of this access ID. Uber admitted that its investigation revealed that an unauthorized individual used the access ID on or around May 12, 2014 to access a stored copy of an Uber database located on Uber's third-party cloud storage provider.

28. After the details of Uber's May 12, 2014 data breach were revealed to the public, Uber was investigated by a number of state and federal regulators that were concerned about its inadequate data security practices. Uber ultimately promised to bolster its data security policies

---

[4] *See Best Practices for Managing AWS Access Keys*, available at https://web.archive.org/web/20140313092151/http://docs.aws.amazon.com/general/latest/gr/aws-access-keys-best-practices.html.

by, *inter alia*, adopting protective technologies for the storage, access, and transfer of private information, and credentials related to its access, *including the adoption of multi-factor authentication*, or similarly protective access control methodologies that may in the future be developed.

29. While Uber made direct promises to regulators, and increased public statements about protecting user privacy, including specifically as it applied to its use of GitHub, less than a year later the same failures led to a breach that was one thousand times worse.

III. The 2016 Data Breach.

30. In October 2016, Uber, then under the control of CEO Travis Kalanick, was contacted by two hackers who informed the company that they had breached an Uber database and were in possession of millions of sensitive personal records.

31. In striking resemblance to the 2014 breach, the hackers had accessed a private GitHub repository and found database login credentials.

32. While the repository was password protected, hackers were still able to breach it—indicating either a very weak password or the fact that the user credentials for the repository were found in a previous unrelated data breach. And even though Uber specifically promised regulators that it would use two-factor authentication on services like GitHub, it clearly failed to implement that promise.

33. Once inside the GitHub repository, the attackers *once again* found AWS login credentials, which the attackers then used to access and extract the personal information of over 50 million people, including Chicago and Illinois residents.

34. According to a blog post published by Uber's new CEO Dara Khosrowshahi, the attackers were able to download files containing "a significant amount of other information,"

which included:

- Full names and driver's license numbers of approximately 600,000 drivers in the United States; and
- Full names, email addresses, and mobile phone numbers of 57 million Uber users.[5]

35. However, Khosrowshahi's post is notably vague and does not state conclusively that the stolen information was in fact limited to the categories above. As such, the information stolen may actually include Uber users' and drivers' usernames, passwords, billing addresses, location history, credit card or bank account numbers, dates of birth, and for drivers, their Social Security numbers.

36. Based on the sheer volume of data stolen, as well as the extensive cover up described below, Uber's data breach is already being recognized as one of the most serious data breach incidents in U.S. history.[6]

IV. Uber Attempted to Cover Up the Data Breach and Did Not Notify the Public, Including Chicago and Illinois Residents, of the Breach Until Over A Year Later.

37. While not the largest breach in recent years, or even the most sensitive release of information, the "handling of the breach underscores the extent to which Uber executives were willing to go to protect the $70 billion ride-hailing giant's reputation and business, even at the potential cost of breaking users' trust and, perhaps more important, state and federal laws."[7]

38. Travis Kalanick, Uber's co-founder and then-CEO, learned of the hack in November 2016, a month after it took place. At the time, Uber had just settled a lawsuit with

---

5 *Uber*, 2016 Data Security Incident, available at https://www.uber.com/newsroom/2016-data-incident/.

6 *The New York Times*, Uber Discloses Data Breach, Kept Secret for a Year, Affecting 57 Million Accounts, available at https://www.nytimes.com/2017/11/21/technology/uber-hack.html?nytmobile=0.

7 *Id.*

state regulators over data security disclosures and was in the process of negotiating with U.S. regulators, including the Federal Trade Commission, who were investigating separate claims against the company for privacy-related violations. Even more, during this same time period, Uber was dealing with a number of public issues regarding its users' rights and privacy, as well as multiple local, state, federal, and even international investigations, including:

- Use of a tool called "Greyball" to identify and circumvent authorities and other officials who were trying to clamp down on the service (*i.e.*, in cities where Uber was not licensed, authorized to operate, or declared illegal);
- Use of a tool called "Hell", which was a program that allowed Uber to secretly track and monitor its rival's drivers;
- Refusal to seek permits from the California Department of Motor Vehicles to test autonomous vehicles and then testing self-driving vehicles in San Francisco, California, which regulators say is illegal;
- Multiple criminal probes from the Justice Department including probes into (i) whether Uber violated price- transparency and discrimination laws, (ii) Uber's role in the alleged theft of schematics and other documents outlining a competitor's autonomous-driving technology, which it is also working to develop, and (iii) bribery; and
- Illegal operation in a variety of cities, states, and countries.

39. Amidst this negative public attention and blows to its reputation, instead of reporting the 2016 breach to regulators and the affected individuals (which it was legally obligated to do), Uber chose to pay the attackers $100,000 to supposedly delete the data and conceal that the breach ever even occurred.

40. Uber went so far as to even track down the criminal hackers and enter into nondisclosure agreements with them as if they were common business partners—so Uber had legal recourse against them if they ever spoke publicly about their crime.

41. Uber's statement that it "obtained assurances that the downloaded data had been

destroyed"[8] is nonsensical. It has not demonstrated, in any way, how or why it knows the data was actually deleted. No matter what documents the hackers signed, or representations they made, Uber is saying little more than that they trust the word of criminals.[9]

42. In a further attempt to cover up the hack and hide the payment, Uber executives made the $100,000 payout to the attackers appear as if it was part of Uber's "bug bounty" program.[10] Since its inception, Uber has paid out over $1.3 million for 778 reported bugs through its bug bounty program. $1.3 million is an enormous amount of money to be paid through a single bug bounty program, even for a company of Uber's size. Uber's use of its bug bounty program to pay a ransom following a data breach makes all $1.3 million in payments suspect as other potential payoffs. If the $1.3 million does not include other ransom payments, it surely demonstrates that Uber is releasing heavily flawed software for public use.

43. The details of the attack remained hidden until November 21, 2017—over one year after Uber learned of the breach—after Uber's Board of Directors commissioned an investigation into the company's business practices and, in particular, the activities of Uber's former Chief Security Officer Joe Sullivan's team—which was known as Competitive Intelligence or COIN. That's because Sullivan's work was largely a mystery to Uber's board.

44. Through that investigation, the board learned that Sullivan had spearheaded the

---

[8] *Uber*, 2016 Data Security Incident, available at https://www.uber.com/newsroom/2016-data-incident/.

[9] Likewise, Uber has not stated (because it simply may not know) whether other hackers exploited the same vulnerability and removed data (without the courtesy of contacting Uber and demanding a ransom).

[10] "Bug bounty" programs are common in the technology industry and seek to incentive individuals to report bugs, exploits, and vulnerabilities to companies before the general public is aware of them. In typical bug bounty programs, the individuals identifying and reporting the bugs do not, and are not given authorization to, access—let alone download—any company data that is intended to be confidential.

response to the 2016 breach. Not surprisingly, shortly before the 2016 breach was announced to the public, Sullivan and one of his deputies were fired for their roles in keeping the breach under wraps.

45. As of the date of filing this Complaint, and despite its duty to do so, Uber still has not directly notified Chicago or Illinois residents of the breach. But, in yet another example of Uber's prioritization of profits over consumer rights, Uber *did* disclose the data breach to a *potential investor*—SoftBank Group Corp.—before going public with details of the incident."[11]

V. Uber Harmed Chicago and Illinois Residents By Concealing the Data Breach and its Deficient Data Security Practices, and Otherwise Engaging in the Deceptive Practices Described Above.

46. Chicago and Illinois residents have already suffered significant and lasting harm as a result of Uber's misconduct described above.

47. First, consumers place value in data privacy and security, and they consider that when making purchasing decisions. In fact, it is widely accepted that consumers are willing to pay higher prices to do business with merchants that better protect their privacy and information. Consumer technology markets have likewise demonstrated that consumers value their privacy and security and incorporate data security practices into their purchases. For example, companies have begun providing consumers with "cloaking services" that allow them to browse the Internet anonymously for a fee. Likewise, companies now offer services that, in exchange for a monthly fee, will offer online services designed to protect data privacy.

48. Because of the value consumers place on data privacy and security, services with better security practices command higher prices than those without. Indeed, if consumers did not

---

[11] *CNBC*, Uber told SoftBank about data breach before telling public, available at https://www.cnbc.com/2017/11/24/uber-told-softbank-about-data-breach-before-telling-public.html. (Emphasis added.)

value their data security and privacy, profit-seeking corporations (like Uber) would have no reason to tout their privacy and security credentials to current and prospective customers.

49. These value propositions reflect the fact that consumers view technology companies that promise to adequately secure customer data as being far more useful—and valuable—than those with substandard protections.

50. As a result, a technology-related service with substandard data security and privacy protections is less useful and valuable than a product or service using adequate security protocols, and is, in reality, a different service entirely.

51. Stated simply, had consumers known the truth about Uber's data security practices—*e.g.*, that it did not adequately protect and store their data—they would not have purchased or chosen to use Uber's services.

52. Second, Chicago and Illinois residents clearly have already suffered significant and lasting harm as a result of the data breach, and such harm is likely to continue and worsen over time.

53. Armed with an individual's sensitive and personal information—like a name and driver's license number—hackers and criminals can commit identity theft, financial fraud, and other identity-related crimes.

54. Identity theft results in real financial losses, lost time, and aggravation to Chicago and Illinois residents. In fact, in its 2014 Victims of Identity Theft report, the United States Department of Justice stated that 65% of the over 17 million identity theft victims that year suffered a financial loss, and 13% of all identity theft victims never had those losses

reimbursed.[12] The average out-of-pocket loss for those victims was $2,895.

55. Identity theft victims also "paid higher interest rates on credit cards, they were turned down for loans or other credit, their utilities were turned off, or they were the subject of criminal proceedings."[13] The report also noted that more than one-third of identity theft victims suffered moderate or severe emotional distress due to the crime.[14]

56. Ultimately Uber's misconduct has substantially increased the risk that the affected Chicago and Illinois residents will be, or already have become, victims of identity theft or financial fraud. Worse still, because Uber has known about this data breach for over a year and has still not directly notified any Chicago or Illinois residents affected by the breach, Chicago and Illinois residents with compromised personal information (who still do not know if they have been affected) have been unable to adequately protect themselves from potential identity theft, including by purchasing credit monitoring services or identity theft protection, or even switching ride-sharing companies.

57. In addition to these harms, Uber's conduct undermines the City's regulation of Uber drivers. Uber (as with others) is classified by the City as a Transportation Network Provider ("TNP") and is comprehensively regulated by Chapter 9-115 of the Chicago Municipal Code. Importantly, those regulations require that Uber's drivers be qualified and screened. Among other things, a driver must: possess a valid driver's license; possess a chauffeur's license; not be convicted of various driving offenses or non-driving crimes; complete a training course; and pass a background check. It is therefore critical to the integrity of the City's vetting and safety

---

12 *See* U.S. Dept. of Justice, Bureau of Justice Statistics, Victims of Identity Theft 2014, at 6 & Table 6, available at http://www.bjs.gov/index.cfm?ty=pbdetail&iid=5408.

13 *Id.* at 8.

14 *See id.* at 9, Table 9.

regulations that Uber's data relating to drivers' identities be protected and accurate. Uber's failure to properly safeguard its drivers' personal data undermines confidence in the City's regulatory system and requires the City to expend further resources to ensure that only qualified individuals drive for Uber.

FIRST CAUSE OF ACTION
Failure to Safeguard Personal Information
Violation of Municipal Code of Chicago § 2-25-090
(On Behalf of Plaintiff City of Chicago Against Defendant)

58. Plaintiff City of Chicago incorporates the foregoing allegations as if fully set forth herein.

59. Chicago Municipal Code Section 2-25-090 (the "Ordinance") provides that any "unlawful practice" under the Illinois Consumer Fraud and Deceptive Business Practices Act ("ICFA") constitutes a violation of the Ordinance.

60. The Ordinance states, in relevant part that:

> (a) No person shall engage in any act of consumer fraud, unfair method of competition, or deceptive practice while conducting any trade or business in the city. *Any conduct constituting an unlawful practice under the Illinois Consumer Fraud and Deceptive Business Practices Act,* as now or hereafter amended, or constituting a violation of Section 7-4-040, Section 7-4-060 or any section of this Code relating to business operations or consumer protection, *shall be a violation of this section.* In construing this section, consideration shall be given to court interpretations relating to the Illinois Consumer Fraud and Deceptive Business Practices Act, as amended. In construing this section, consideration shall also be given to the interpretations of the Federal Trade Commission and the federal courts relating to Section 5(a) of the Federal Trade Commission Act, 15 U.S.C.A., Section 45.
>
> MCC § 2-25-090(a) (*emphasis added*).

61. For its part, Section 2 of the ICFA, 815 ILCS 505/2, provides:

> Unfair methods of competition and unfair or deceptive acts or practices, including but not limited to the use or employment of any deception fraud, false pretense, false promise, misrepresentation or the concealment,

> suppression or omission of any material fact, with intent that others rely upon the concealment, suppression or omission of such material fact, or the use or employment of any practice described in section 2 of the 'Uniform Deceptive Trade Practices Act', approved August 5, 1965, in the conduct of any trade or commerce are hereby declared unlawful whether any person has in fact been misled, deceived or damaged thereby. In construing this section consideration should be given to the interpretations of the Federal Trade Commission and the federal courts relating to Section 5 (a) of the Federal Trade Commission Act.

62. While engaging in trade or commerce, Uber has engaged in conduct that constitutes a deceptive act or practice declared unlawful under Section 2 of the ICFA, inasmuch as it made deceptive public representations about the nature of its data security safeguards to the public, including Chicago residents, assuring them that it would take appropriate measures to ensure that their personal information was secure.

63. Uber intended that the public, including Chicago residents, rely on its deceptive representations and communications regarding the security of their personal information.

64. Rather than following industry best practices to keep personal information protected, secure, and not susceptible to access by unauthorized third parties, Uber mishandled that personal information in such a manner that allowed it to be easily susceptible to attack.

65. Uber's conduct constitutes an unlawful practice under the ICFA and, accordingly, violates the Ordinance.

66. The penalty for violating the Ordinance is a fine of not less than $2,000 nor more than $10,000 for each offense. MCC § 2-25-090(f). Moreover, "[e]ach day that a violation continues shall constitute a separate and distinct offense to which a separate fine shall apply." *Id.*

67. A violation of the Ordinance also entitles the City to equitable relief, including, but not limited to, restitution. MCC § 2-25-090(e)(4).

SECOND CAUSE OF ACTION
Failure to Give Prompt Notice of Data Breach
Violation of Municipal Code of Chicago § 2-25-090
(On Behalf of Plaintiff City of Chicago Against Defendant)

68. Plaintiff City of Chicago incorporates the foregoing allegations as if fully set forth herein.

69. The Ordinance provides that any "unlawful practice" under the ICFA constitutes a violation of the Ordinance.

70. A violation of Illinois's Personal Information Protection Act, 815 ILCS 530/1, *et seq*. ("PIPA") "constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act." *See* 815 ILCS 530/20.

71. Thus, a violation of PIPA is also a violation of the Ordinance.

72. Section 10(a) of PIPA states that:

> (a) Any data collector that owns or licenses personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach. *The disclosure notification shall be made in the most expedient time possible and without unreasonable delay*, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.
>
> 815 ILCS 530/10 (*emphasis added*).

73. Section 10(a) of PIPA also specifies the required content of the disclosure notification:

> The disclosure notification to an Illinois resident shall include, but need not be limited to, information as follows:
>
> (1) With respect to personal information as defined in Section 5 in paragraph (1) of the definition of "personal information":
>
> (A) the toll-free numbers and addresses for consumer reporting agencies;

(B) the toll-free number, address, and website address for the Federal Trade Commission; and

(C) a statement that the individual can obtain information from these sources about fraud alerts and security freezes.

(2) With respect to personal information defined in Section 5 in paragraph (2) of the definition of "personal information", notice may be provided in electronic form or other form directing the Illinois resident whose personal information has been breached to promptly change his or her user name or password and security question or answer, as applicable, or to take other steps appropriate to protect all online accounts for which the resident uses the same user name or email address and password or security question and answer.

74. Upon information and belief, Uber is a data collector that owns or licenses personal information concerning Illinois, including Chicago, residents.

75. Additionally, Section 10(b) of PIPA states:

(b) Any data collector that maintains or stores, but does not own or license, computerized data that includes personal information that the data collector does not own or license shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. In addition to providing such notification to the owner or licensee, the data collector shall cooperate with the owner or licensee in matters relating to the breach. That cooperation shall include, but need not be limited to, (i) informing the owner or licensee of the breach, including giving notice of the date or approximate date of the breach and the nature of the breach, and (ii) informing the owner or licensee of any steps the data collector has taken or plans to take relating to the breach. The data collector's cooperation shall not, however, be deemed to require either the disclosure of confidential business information or trade secrets or the notification of an Illinois resident who may have been affected by the breach.

815 ILCS 530/10(b).

76. In the alternative, pursuant to Section 10(b) of PIPA, Uber is a data collector that maintains or stores computerized data that includes personal information of Chicago and Illinois

residents.

77. Uber failed to notify Chicago residents that a data breach of the security of its system data had occurred in the most expedient time possible and without unreasonable delay. In fact, as of the date of filing this Complaint, Uber has failed to provide the disclosure notifications to Chicago residents required by Section 10 of PIPA and the Ordinance, even though Uber has known about this data breach for over a year.

78. Because of this delay, Chicago residents with compromised personal information have been unable to adequately protect themselves from potential identity theft.

79. As a result, Uber has violated PIPA.

80. Uber's violations of PIPA constitute unlawful practices under the ICFA and, therefore, violations of the Ordinance. The penalty for violating the Ordinance is a fine of not less than $2,000 nor more than $10,000 for each offense. MCC § 2-25-090(f). Moreover, "[e]ach day that a violation continues shall constitute a separate and distinct offense to which a separate fine shall apply." *Id.*

81. A violation of the Ordinance also entitles the City to equitable relief, including, but not limited to, restitution. MCC § 2-25-090(e)(4).

THIRD CAUSE OF ACTION
Concealment of Data Breach
Violation of Municipal Code of Chicago § 2-25-090
(On Behalf of Plaintiff City of Chicago Against Defendant)

82. Plaintiff City of Chicago incorporates the foregoing allegations as if fully set forth herein.

83. The Ordinance provides that any "unlawful practice" under the ICFA constitutes a violation of the Ordinance.

84. While engaging in trade or commerce, Uber has engaged in conduct that

constitutes a deceptive act or practice declared unlawful under Section 2 of the ICFA, in that it made deceptive public representations and communications about the nature of its data security safeguards to the public, including Chicago residents, assuring them that it would take appropriate measures to ensure that their personal information was secure.

85. Uber became aware of the data breach in October 2016. Instead of reporting the breach as it is required to do under law, Uber concealed the breach—deciding instead to pay the hackers $100,000 to delete the data and not report the breach to authorities and affected consumers. Uber has known about this data breach for over a year and has still not directly notified any Chicago resident affected by the data breach.

86. Rather than following industry best practices to keep personal information protected, secure, and not susceptible to access by unauthorized third parties, Uber mishandled that personal information in such a manner that allowed it to be easily susceptible to attack.

87. Uber's conduct constitutes an unfair practice deemed unlawful under the ICFA and, accordingly, violates the Ordinance.

88. The penalty for violating the Ordinance is a fine of not less than $2,000 nor more than $10,000 for each offense. MCC § 2-25-090(f). Moreover, "[e]ach day that a violation continues shall constitute a separate and distinct offense to which a separate fine shall apply." *Id.*

89. A violation of the Ordinance also entitles the City to equitable relief, including, but not limited to, restitution. MCC § 2-25-090(e)(4).

FOURTH CAUSE OF ACTION
Failure to Safeguard Personal Information
Violation of Municipal Code of Chicago § 2-25-090
(On Behalf of Plaintiff City of Chicago Against Defendant)

90. Plaintiff City of Chicago incorporates the foregoing allegations as if fully set forth herein.

91. The Ordinance provides that any "unlawful practice" under the ICFA constitutes a violation of the Ordinance.

92. While conducting trade or commerce, Uber has engaged in conduct that constitutes an unfair act or practice declared unlawful under Section 2 of the ICFA, in that it purposefully concealed the data breach, allowing it to maintain its advantage over its competition.

93. Uber knows that its customers and drivers value the security of their data, and if the data breach was made public, Uber would potentially lose customer and driver business.

94. Uber's conduct constitutes an unfair practice deemed unlawful under the ICFA and, accordingly, violates the Ordinance.

95. The penalty for violating the Ordinance is a fine of not less than $2,000 nor more than $10,000 for each offense. MCC § 2-25-090(f). Moreover, "[e]ach day that a violation continues shall constitute a separate and distinct offense to which a separate fine shall apply." *Id.*

96. A violation of the Ordinance also entitles the City to equitable relief, including, but not limited to, restitution. MCC § 2-25-090(e)(4).

FIFTH CAUSE OF ACTION
Declaratory and Injunctive Relief
(On Behalf of Plaintiff City of Chicago Against Defendant)

97. Plaintiff City of Chicago incorporates the foregoing allegations as if fully set forth herein.

98. Pursuant to 735 ILCS 5/2-701, this Court "may make binding declarations of rights, having the force of final judgments . . . including the determination . . . of the construction of any statute, municipal ordinance, or other governmental regulation . . . and a declaration of the rights of the parties interested."

99. Such a declaration of rights "may be obtained . . . as incident to or part of a complaint . . . seeking other relief as well." 735 ILCS 5/2-701(b).

100. Chicago seeks a judgment declaring that Uber has violated the Ordinance.

101. Chicago further contends that Uber's data security measures were inadequate to protect the public's sensitive personal information.

102. Upon information and belief, these data security measures remain inadequate. Chicago residents will continue to suffer or be vulnerable to injury, unless this is rectified through injunctive relief.

SIXTH CAUSE OF ACTION
Deceptive Public Representations of Data Protection Safeguards
Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act
(On Behalf of Plaintiff People of the State of Illinois Against Defendant)

103. Plaintiff People of the State of Illinois incorporate the foregoing allegations as if fully set forth herein.

104. Section 2 of the ICFA, 815 ILCS 505/2, provides:

> Unfair methods of competition and unfair or deceptive acts or practices, including but not limited to the use or employment of any deception fraud, false pretense, false promise, misrepresentation or the concealment, suppression or omission of any material fact, with intent that others rely upon the concealment, suppression or omission of such material fact, or the use or employment of any practice described in section 2 of the 'Uniform Deceptive Trade Practices Act', approved August 5, 1965, in the conduct of any trade or commerce are hereby declared unlawful whether any person has in fact been misled, deceived or damaged thereby. In construing this section consideration should be given to the interpretations of the Federal Trade Commission and the federal courts relating to Section 5 (a) of the Federal Trade Commission Act.

105. While engaging in trade or commerce, Uber has engaged in conduct that constitutes a deceptive act or practice declared unlawful under Section 2 of the ICFA, inasmuch as it made deceptive public representations about the nature of its data security safeguards to the

public, including Illinois residents, assuring them that it would take appropriate measures to ensure that their personal information was secure.

106. Uber intended that the public, including Illinois residents, rely on its deceptive representations and communications regarding the security of their personal information.

107. Rather than following industry best practices to keep personal information protected, secure, and not susceptible to access by unauthorized third parties, Uber mishandled that personal information in such a manner that allowed it to be easily susceptible to attack.

108. Uber's conduct constitutes an unlawful practice under the ICFA.

109. Pursuant to 815 ILCS 505/7(b), the penalty for violating the ICFA is a sum not to exceed $50,000 or, if the Court finds that Uber's above-described practices were intended to defraud Illinois residents, $50,000 per violation.

110. In addition to any other civil penalty provided, if a person is found by the Court to have engaged in any method, act, or practice declared unlawful under the ICFA, and the violation was committed against a person 65 years of age or older, the Court may impose an additional civil penalty in a sum not to exceed $10,000 per violation. 815 ILCS 505/7(c).

SEVENTH CAUSE OF ACTION
Failure to Give Prompt Notice of Data Breach
Violation of Illinois's Personal Information Protection Act
(On Behalf of Plaintiff People of the State of Illinois Against Defendant)

111. Plaintiff People of the State of Illinois incorporates the foregoing allegations as if fully set forth herein.

112. A violation of PIPA, 815 ILCS 530/1, *et seq.*, "constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act." *See* 815 ILCS 530/20.

113. Section 10 of PIPA states that:

(a) Any data collector that owns or licenses personal information

concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach. *The disclosure notification shall be made in the most expedient time possible and without unreasonable delay*, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system . . . .

(b) Any data collector that maintains or stores, but does not own or license, computerized data that includes personal information that the data collector does not own or license shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. In addition to providing such notification to the owner or licensee, the data collector shall cooperate with the owner or licensee in matters relating to the breach. That cooperation shall include, but need not be limited to, (i) informing the owner or licensee of the breach, including giving notice of the date or approximate date of the breach and the nature of the breach, and (ii) informing the owner or licensee of any steps the data collector has taken or plans to take relating to the breach. The data collector's cooperation shall not, however, be deemed to require either the disclosure of confidential business information or trade secrets or the notification of an Illinois resident who may have been affected by the breach.

815 ILCS 530/10 (*emphasis added*).

114. Section 10 of PIPA also specifies the required content of the disclosure notification:

The disclosure notification to an Illinois resident shall include, but need not be limited to, information as follows:

(1) With respect to personal information as defined in Section 5 in paragraph (1) of the definition of "personal information":

(A) the toll-free numbers and addresses for consumer reporting agencies;

(B) the toll-free number, address, and website address for the Federal Trade Commission; and

(C) a statement that the individual can obtain information from these sources about fraud alerts and security freezes.

> (2) With respect to personal information defined in Section 5 in paragraph (2) of the definition of "personal information", notice may be provided in electronic form or other form directing the Illinois resident whose personal information has been breached to promptly change his or her user name or password and security question or answer, as applicable, or to take other steps appropriate to protect all online accounts for which the resident uses the same user name or email address and password or security question and answer.

115. Uber is a data collector that owns or licenses personal information concerning Illinois, including Cook County, residents.

116. Uber failed to notify Illinois residents that a data breach had occurred in the most expedient time possible and without unreasonable delay. In fact, as of the date of filing this Complaint, Uber has failed to provide the disclosure notifications to Illinois residents required by Section 10 of PIPA, even though Uber has known about this data breach for over a year.

117. Because of this delay, Illinois residents with compromised personal information have been unable to adequately protect themselves from potential identity theft.

118. As a result, Uber has violated PIPA.

119. Uber's violations of PIPA constitute unlawful practices under the ICFA. Pursuant to 815 ILCS 505/7(b), the penalty for violating the ICFA is a sum not to exceed $50,000 or, if the Court finds that Uber's above-described practices were intended to defraud Illinois residents, $50,000 per violation.

120. In addition to any other civil penalty provided, if a person is found by the Court to have engaged in any method, act, or practice declared unlawful under the ICFA, and the violation was committed against a person 65 years of age or older, the Court may impose an additional civil penalty in a sum not to exceed $10,000 per violation. 815 ILCS 505/7(c).

EIGHTH CAUSE OF ACTION
Concealment of Data Breach
Violation of Illinois Consumer Fraud and Deceptive Business Practices Act
(On Behalf of Plaintiff People of the State of Illinois Against Defendant)

121. Plaintiff People of the State of Illinois incorporates the foregoing allegations as if fully set forth herein.

122. While engaging in trade or commerce, Uber has engaged in conduct that constitutes a deceptive act or practice declared unlawful under Section 2 of the ICFA, in that it made deceptive public representations and communications about the nature of its data security safeguards to the public, including Illinois residents, assuring them that it would take appropriate measures to ensure that their personal information was secure.

123. Uber became aware of the data breach in October 2016. Instead of reporting the breach as it is required to do under law, Uber concealed the breach—deciding instead to pay the hackers $100,000 to delete the data and not report the breach to authorities and affected consumers. Uber has known about this data breach for over a year and has still not directly notified any Illinois residents affected by the data breach.

124. Rather than following industry best practices to keep personal information protected, secure, and not susceptible to access by unauthorized third parties, Uber mishandled that personal information in such a manner that allowed it to be easily susceptible to attack.

125. Uber's conduct constitutes an unfair practice deemed unlawful under the ICFA.

126. Pursuant to 815 ILCS 505/7(b), the penalty for violating the ICFA is a sum not to exceed $50,000 or, if the Court finds that Uber's above-described practices were intended to defraud Illinois residents, $50,000 per violation.

127. In addition to any other civil penalty provided, if a person is found by the Court to have engaged in any method, act, or practice declared unlawful under the ICFA, and the

violation was committed against a person 65 years of age or older, the Court may impose an additional civil penalty in a sum not to exceed $10,000 per violation. 815 ILCS 505/7(c).

NINTH CAUSE OF ACTION
Concealment of Data Breach
Violation of Illinois Consumer Fraud and Deceptive Business Practices Act
(On Behalf of Plaintiff People of the State of Illinois Against Defendant)

128. Plaintiff People of the State of Illinois incorporates the foregoing allegations as if fully set forth herein.

129. While conducting trade or commerce, Uber has engaged in conduct that constitutes an unfair act or practice declared unlawful under Section 2 of the ICFA, in that it purposefully concealed the data breach, allowing it to maintain its advantage over its competition.

130. Uber knows that its customers and drivers value the security of their data, and if the data breach was made public, Uber would potentially lose customer and driver business.

131. Uber's conduct constitutes an unfair practice deemed unlawful under the ICFA.

132. Pursuant to 815 ILCS 505/7(b), the penalty for violating the ICFA is a sum not to exceed $50,000 or, if the Court finds that Uber's above-described practices were intended to defraud Illinois residents, $50,000 per violation.

133. In addition to any other civil penalty provided, if a person is found by the Court to have engaged in any method, act, or practice declared unlawful under the ICFA, and the violation was committed against a person 65 years of age or older, the Court may impose an additional civil penalty in a sum not to exceed $10,000 per violation. 815 ILCS 505/7(c).

TENTH CAUSE OF ACTION
Declaratory and Injunctive Relief
(On Behalf of Plaintiff People of the State of Illinois Against Defendant)

134. Plaintiff People of the State of Illinois incorporates the foregoing allegations as if

fully set forth herein.

135. Pursuant to 735 ILCS 5/2-701, this Court "may make binding declarations of rights, having the force of final judgments . . . including the determination . . . of the construction of any statute, municipal ordinance, or other governmental regulation . . . and a declaration of the rights of the parties interested."

136. Such a declaration of rights "may be obtained . . . as incident to or part of a complaint . . . seeking other relief as well." 735 ILCS 5/2-701(b).

137. Plaintiff People of the State of Illinois seeks a judgment declaring that Uber has violated the ICFA and PIPA.

138. Plaintiff People of the State of Illinois further contends that Uber's data security measures were inadequate to protect the public's sensitive personal information.

139. Upon information and belief, these data security measures remain inadequate. Illinois residents will continue to suffer or be vulnerable to injury, unless this is rectified through injunctive relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs City of Chicago and People of the State of Illinois respectfully request that the Court enter an Order granting the following relief:

A. Declaring that Defendant Uber's actions constitute violations of the Ordinance, PIPA, and ICFA, including by (i) failing to notify Chicago and Illinois residents of the data breach within the most expedient time possible and without unreasonable delay, and (ii) engaging in conduct that constitutes a deceptive act or practice declared unlawful under Section 2 of the Illinois ICFA;

B. Fining Uber for each violation of the Ordinance involving a Chicago resident, in

the amount of $10,000 for each day such violation has existed and continues to exist;

C. Fining Uber $50,000 for violating the ICFA or, if the Court finds that Uber engaged in the above-described conduct with the intent to defraud, $50,000 for each such violation;

D. Fining Uber an additional $10,000 for each violation described above involving an Illinois resident 65 years of age or older for each day such violation has existed and continues to exist;

E. Awarding appropriate restitution to Plaintiffs in an amount to be determined at trial;

F. Awarding Plaintiffs their reasonable attorneys' fees and costs;

G. Awarding Plaintiffs pre- and post-judgment interest, to the extent allowable;

H. Awarding such and other injunctive and declaratory relief as is necessary; and

I. Awarding such other and further relief as the Court deems reasonable and just.

JURY DEMAND

Plaintiffs request a trial by jury of all claims that can so be tried.

Dated: November 27, 2017

Respectfully submitted,

EDWARD SISKEL
Corporation Counsel, City of Chicago

By: /s/ Edward N. Siskel

Edward N. Siskel
Corporation Counsel
edward.siskel@cityofchicago.org
CITY OF CHICAGO, DEPARTMENT OF LAW
30 North LaSalle Street, Suite 1230
Chicago, Illinois 60602
Tel: 312.744.6929
Fax: 312.742.3832

KIMBERLY M. FOXX
State's Attorney of Cook County

By: /s/ Chaka M. Patterson

Chaka M. Patterson
Assistant State's Attorney
chaka.patterson@cookcountyil.gov
COOK COUNTY STATE'S ATTORNEY'S OFFICE
69 West Washington Street, Suite 3130
Chicago, Illinois 60602
Tel: 312.603.8600
Fax: 312.603.9830

Special Assistant Corporation Counsel

By: /s/ Jay Edelson

Jay Edelson
jedelson@edelson.com
Rafey S. Balabanian
rbalabanian@edelson.com
Benjamin H. Richman
brichman@edelson.com
Ari J. Scharg
ascharg@edelson.com
EDELSON PC
350 North LaSalle Street, 13th Floor
Chicago, Illinois 60654
Tel: 312.589.6370
Fax: 312.589.6378
Firm ID: 62075

Special Assistant State's Attorney

By: /s/ Jay Edelson

Jay Edelson
jedelson@edelson.com
Rafey S. Balabanian
rbalabanian@edelson.com
Benjamin H. Richman
brichman@edelson.com
Ari J. Scharg
ascharg@edelson.com
EDELSON PC
350 North LaSalle Street, 13th Floor
Chicago, Illinois 60654
Tel: 312.589.6370
Fax: 312.589.6378
Firm ID: 62075