NON-PROSECUTION AGREEMENT

The United States Attorney's Office for the Northern District of California ("USAO") hereby enters into the following Non-Prosecution Agreement (the "Agreement" or "Non-Prosecution Agreement") with Uber Technologies, Inc. ("Uber," or the "Company"), a Delaware corporation, pursuant to authority granted by the Company's Board of Directors as reflected in Exhibits C and D, to resolve the federal criminal investigation related to the conduct described in the Statement of Facts attached as Exhibit A to this Agreement. This Agreement is binding only on Uber and the USAO; it specifically does not bind any other component of the Department of Justice; other federal agencies, or any state, local or foreign law enforcement or regulatory agencies; or any other authorities.

I. Introduction and Relevant Considerations

a. The USAO enters into this Agreement with Uber based on the individual facts and circumstances presented by this case, including the following factors:

i. Uber's acceptance of responsibility for its conduct in the wake of a data breach that Uber suffered in October and November of 2016 (the "2016 Data Breach"), as described in the Statement of Facts;

ii. Uber's voluntary disclosure in November 2017, under new executive leadership, of the 2016 Data Breach to the public, law enforcement, and foreign and domestic regulators, including state attorneys general and the Federal Trade Commission ("FTC").

iii. The presence of new executive leadership, who established a strong tone from the top of the organization regarding ethics and compliance and who otherwise strengthened the Company's culture of compliance and transparency, including by acting promptly upon learning of the 2016 Data Breach to investigate and ultimately disclose it to government authorities, drivers, and the public. More specifically, the Company:

1. Invested substantial resources to significantly restructure and enhance the Company's compliance, legal, and security functions;

2. In 2017 and thereafter, hired a Chief Legal Officer, Chief Ethics and Compliance Officer, and Chief Trust and Security Officer, all of whom had significant experience, and hired an experienced

attorney as its first Chief Privacy Officer responsible for managing the Company's global data privacy compliance program; and

3. Terminated the employment of two of the individuals who led Uber's response to the 2016 Data Breach;

iv. Uber's October 2018 settlement with the FTC, in which Uber agreed to, among other things:

1. Maintain a detailed and comprehensive privacy program, including biennial assessments of Uber's privacy controls by qualified, objective, independent third-party professionals, for a period of twenty years; and

2. Submit a report to the FTC regarding any incident in which any United States federal, state, or local law or regulation requires Uber to notify any United States federal, state, or local government entity that information collected or received by Uber from or about an individual consumer was, or was reasonably believed to have been, accessed or acquired without authorization;

v. Uber's settlement of civil litigation with the attorneys general for all 50 States and the District of Columbia related to the 2016 Data Breach, which resulted in Uber paying $148,000,000 and agreeing to the implementation of (a) a corporate integrity program, (b) specific and robust data security safeguards, (c) a comprehensive information security program, (d) a comprehensive incident response and data breach notification plan, and (e) biennial assessments of Uber's information security program by a qualified, independent third party, for a period of ten years;

vi. The USAO's determination, based on Uber's existing compliance program, in addition to the commitments listed in sections (iv) and (v) above, that an independent compliance monitor is unnecessary;

vii. Uber's full cooperation with the USAO's investigation, which has assisted the government's efforts and has included:

1. The Company's early and continued full engagement with the USAO regarding facts relevant to the USAO's investigation;

2. Producing extensive documentation to the USAO relating to the 2016 Data Breach in an efficient, responsive manner; and

3. Voluntarily making available several current and former Company employees, including Company executives, for interviews or meetings with the USAO.

viii. Uber's agreement (in accordance with Section IV of this Agreement) to continue to cooperate with the USAO and the Federal Bureau of Investigation ("FBI") during the pendency of the criminal prosecution the USAO has instituted in this matter against Uber's former Chief Security Officer ("Sullivan Prosecution").

II. The Term of the Agreement

a. This Agreement shall be deemed effective as of the last date of execution by a party to this Agreement and shall continue in effect until twelve months after the entry of final judgment by the District Court in the Sullivan Prosecution, at which point the Agreement shall no longer be in effect, regardless of whether any appeals are filed in the Sullivan Prosecution.

III. Uber's Acceptance of Responsibility

a. Uber admits, accepts, and acknowledges that it is responsible for the acts of its officers, directors, employees, and agents within the scope of their employment, as set forth in the Statement of Facts. The Company agrees that the factual statements contained within the Statement of Facts are true and accurate to the best of its knowledge.

IV. Cooperation

a. Uber shall cooperate fully with the Sullivan Prosecution and any other criminal investigation or prosecution relating to the 2016 Data Breach that the USAO may initiate. The USAO shall have sole discretion to determine what matters are "relating to the 2016 Data Breach." All such cooperation described in this Paragraph shall include, but not be limited to:

i. Timely providing upon oral or written request, consistent with applicable law and regulations, including data protection and privacy laws, all non-

privileged information, documents, records, and other tangible evidence that can be obtained through reasonable efforts, including from Uber;

ii. Identifying, upon oral or written request, witnesses who, to the knowledge of the Company, may have material information regarding the matters under indictment; and

iii. Upon oral or written request, using its best efforts to facilitate the availability for interview or testimony, in a timely fashion, of any current or former officer, executive, director, employee, agent, or consultant of the Company, including by facilitating such persons' availability in the Northern District of California, at Uber's expense, regardless of their location or residence.

b. Uber shall provide complete, truthful, and accurate information to the USAO and the FBI in connection with the Sullivan Prosecution and any other criminal investigation or prosecution relating to the 2016 Data Breach that the USAO may initiate. Uber's obligation to cooperate pursuant to Section IV will no longer apply if a prosecution by the USAO is commenced against Uber as a result of a breach of this Agreement.

c. Nothing in this Agreement is intended to request or require the Company to waive its attorney-client privilege or work product protections, and no such waiver shall be deemed effected by any provision herein.

V. Non-Prosecution

a. The USAO and the Company intend for this Agreement to resolve the USAO's criminal investigation of Uber or any of its parents, subsidiaries, or direct and indirect affiliates (collectively, the "Uber Entities") relating to the conduct described in the Statement of Facts, and the USAO agrees that if the Company fully complies with all of its obligations under this Agreement, the USAO will not criminally prosecute the Uber Entities, during the term of this Agreement or thereafter, for any crime related to the conduct described in the Statement of Facts. Moreover, the USAO agrees that if the Company fully complies with all of its obligations under this Agreement, the USAO will not criminally prosecute the Uber Entities for any conduct regarding the Uber Entities that is not described in the Statement of Facts and that attorneys representing the Company have discussed with or otherwise disclosed to the USAO as of the date of this Agreement.

b. Except as expressly provided in Section V(a) above, this Agreement does not preclude or limit the USAO, any other United States Attorney's Office, or the United States Department of Justice from investigating or prosecuting Uber, or for prosecuting any other individual or entity, including any current or former officer, employee, or agent of the Company.

VI. Breach of Agreement

a. If, during the term of the Agreement, (a) Uber knowingly and willfully provides in connection with this Agreement materially false, incomplete, or misleading information, including in connection with its disclosure of information about individual culpability; (b) the USAO determines that Uber, prior to execution of the Agreement, knowingly and willfully provided materially false, incomplete, or misleading information, including in connection with its disclosure of information about individual culpability; or (c) Uber otherwise knowingly, willfully, and materially fails to perform or fulfill any of its obligations under the Agreement – and has failed to remedy such breach after receiving notice from the USAO as set forth in Section VI(b) – the USAO will deem the Company in breach of the Agreement, and the Company shall thereafter be subject to prosecution for any federal criminal violation of which the USAO has knowledge as of the date of this Agreement, including, but not limited to, charges arising from the conduct described in the Statement of Facts. After meeting and conferring with Uber regarding any potential breach, the USAO, in its sole discretion, may determine by a preponderance of the evidence whether Uber has breached the Agreement.

b. In the event that the USAO determines that the Company has breached this Agreement by a preponderance of the evidence, the USAO shall provide the Company with written notice of such determination prior to instituting any prosecution resulting from such breach. Within 30 days of receipt of such notice, the Company shall have the opportunity to address such breach by providing a response to the USAO to demonstrate that no breach has occurred, to demonstrate that the breach was not a knowing and willful breach, to demonstrate that any breach was not material or did not involve material information, and/or to explain the actions taken to address and remediate the breach. The USAO shall thereafter provide written notice to the Company of its final determination regarding whether to declare the Agreement breached. The Company shall thereafter have 30 days from receipt of the USAO's final determination to submit an appeal in writing to a higher authority within the Department of Justice in order to seek to reverse the USAO's determination that the Company has breached the

agreement. The USAO will not institute a prosecution based on the alleged breach until the appeal to a higher authority is no longer under consideration and the Company has been notified in writing of the outcome of the appeal.

c. In the event that the USAO decides to institute a criminal prosecution against the Company after a breach of this Agreement, then:

i. All statements made by or on behalf of the Company to the USAO, including the attached Statement of Facts, shall be admissible in evidence in any and all criminal proceedings brought by the USAO against Uber, and Uber shall stipulate to the admissibility into evidence of the Statement of Facts as an admission by the Company, and shall be precluded from offering any evidence or argument that contradicts the Statement of Facts or that suggests those facts are untrue or misleading;

ii. Uber shall not assert any claim under the United States Constitution, Rule 11(f) of the Federal Rules of Criminal Procedure, Rule 410 of the Federal Rules of Evidence, or any other federal rule that such statements made by or on behalf of Uber prior or subsequent to this Agreement should be suppressed or are otherwise inadmissible;

iii. The USAO shall immediately be free to use the waiver of indictment provided by the Company in Exhibit B attached hereto and to prosecute the Company by way of information for any federal offense arising out of the Statement of Facts. The Company remains bound by all other waivers expressly made as part of this Agreement; and

iv. Uber will not assert that the bringing of charges based upon the conduct outlined in the attached Statement of Facts is barred by the statute of limitations or any analogous equitable doctrine, statutory provision, or Constitutional right. By this Agreement, the Company expressly intends to and hereby does waive its right to make a claim premised upon the statute of limitations, as well as any constitutional, statutory, or other claim concerning pre-indictment delay. These waivers are knowing, voluntary, and in express reliance upon the advice of the Company's counsel.

VII. Sale, Merger, or Other Change in Corporate Form of the Company

a. This Agreement shall be binding upon Uber and its successors and assigns. Except as may otherwise be agreed by the parties in connection with a particular transaction, Uber agrees that in the event that, during the term of the Agreement, Uber sells, assigns, or otherwise directly transfers all or substantially all of its business to another person/entity, whether such sale is structured as an asset sale by the Company, merger of the Company into another person/entity, transfer by the Company, or change in corporate form of the Company, such business shall continue to be subject to the terms and conditions of this Agreement.

VIII. Notice

a. Any notice to the USAO under this Agreement shall be provided (1) via email to andrew.dawson@usdoj.gov; and (2) via personal delivery, overnight delivery by a recognized delivery service, or registered or certified mail, addressed to:

AUSA Andrew F. Dawson
U.S. Attorney's Office
Northern District of California
450 Golden Gate Ave., 11th Fl.
San Francisco, CA 94103

Any notice to Uber under this Agreement shall be provided (1) via email to twest@uber.com and (2) via personal delivery, overnight delivery by a recognized delivery service, or registered or certified mail, addressed to:

Tony West, Chief Legal Officer
Uber Technologies, Inc.
1515 3rd Street
San Francisco, CA 94158

-and-

Steven E. Fagell
Covington & Burling LLP
800 Tenth Street, NW
Washington, DC 20001

b. Notice shall be effective upon actual receipt by the USAO or Uber.

IX. Jurisdiction and No Other Agreements

a. This Agreement is covered by the laws of the United States. The USAO and Uber agree that exclusive jurisdiction and venue for any dispute arising under this Agreement is in the United States District Court for the Northern District of California.

b. This Agreement, with its attached Exhibits A through D, sets forth all the terms of the agreement between the Company and the USAO. No modifications or additions to this Agreement, or to its attached Exhibits A through D, shall be valid unless they are in writing and signed by the USAO, Uber's attorneys, and a duly authorized agent of the Company.

Exhibit A – Statement of Facts
Exhibit B – Waiver of Indictment
Exhibit C – Company Officer's Certificate
Exhibit D – Certificate of Counsel

AGREED:

Stephanie M. Hinds
United States Attorney

Andrew Dawson — July 21, 2022

Andrew F. Dawson — DATE
Assistant United States Attorney

DocuSigned by: Tony West — July 20, 2022
202A918A3690C4A...

Uber Technologies, Inc. — DATE
by: Tony West, Chief Legal Officer

SA Fagell — July 20, 2022

Steven E. Fagell — DATE
W. Douglas Sprague
Covington & Burling LLP
Counsel for Uber Technologies, Inc.

EXHIBIT A

STATEMENT OF FACTS

Uber Technologies, Inc. ("Uber") admits, accepts, and acknowledges as true the following facts:

Relevant Parties

1. The United States Federal Trade Commission ("FTC") is an independent agency of the United States. During the relevant period, the FTC's Division of Privacy and Identity Protection oversaw and investigated, among other things, issues related to consumer privacy, identity theft, and information security.

2. Uber was, at all times relevant to the conduct described herein, a privately held corporation incorporated in the State of Delaware. Uber was founded in 2009, and it operated a technology platform connecting consumers with independent service providers ("drivers") for ridesharing and delivery services.

The 2014 Data Breach

3. In September 2014, Uber learned it had been the victim of a data breach. Uber discovered that a security key allowing access to its Amazon Web Service Simple Storage Service account ("AWS" or "S3") had been inadvertently published to a public repository on GitHub, a cloud-based third-party development platform that contained Uber's computer programming source code. Uber determined that a third party used the security key to access an unencrypted copy of its data. Uber also determined that the file accessed by the outsider in the 2014 Data Breach contained enough information to allow a user to match names and drivers' license numbers of approximately 50,000 drivers. When it completed its investigation, Uber notified the affected drivers, the FTC, and state attorneys general.

4. In the wake of the 2014 Data Breach, Uber expanded its security workforce and created a Security group with the goal, in part, of strengthening the protections that safeguarded the personally identifiable information ("PII") in its possession. In April 2015, Uber hired Joseph Sullivan as its first Chief Security Officer ("CSO") to lead its newly formed security team. Sullivan had previously served in legal and security roles for major corporations, including in roles in which he was responsible for regulatory, privacy, and data security matters, as well as information security, product security, investigations, and law enforcement relations. Before those private sector roles, Sullivan had served for many years as a prosecutor in the U.S. Attorney's Office for the Northern District of California.

FTC Investigation

5. On May 21, 2015, the FTC issued a Civil Investigative Demand ("CID") to Uber. Included in the CID were four interrogatories, each with various subparts. The fourth interrogatory required Uber to provide information "[w]ith respect to any Breach or suspected breach," including:

- "When and how the Company learned of the Breach";
- "The location, type(s), and amount(s) of Personal Information that unauthorized person(s) could have accessed or viewed";
- "The location, type(s), and amount(s) of Personal Information that the unauthorized person(s) did copy, download, or remove"; and
- "[W]hen and . . . how the Company notified Consumers, law enforcement, and other third parties about the Breach."

6. The CID defined "Breach" as "unauthorized access into the Company's systems or to Personal Information in the Company's file(s), including but not limited to the unauthorized

access to the Company's database(s) that took place on or around May 12, 2014 [the 2014 Data Breach]." "Personal Information" was defined broadly as "individually identifiable information from or about an individual Consumer," specifically including "a driver's license . . . or other personal identification number." The applicable time period was defined as "from January 1, 2014, until the date of full and complete compliance with this CID."

7. On June 10, 2016, the FTC issued a second CID, which required Uber to designate an officer to provide sworn testimony on a variety of topics. Among these topics, the FTC compelled testimony on a variety of issues related to S3, Uber's use of encryption, and Uber's storage of "personal information." Uber designated Sullivan as its witness, and he prepared for the hearing with both in-house and outside counsel.

8. The investigative hearing took place on November 4, 2016. The FTC's investigation topics included Uber's use of S3 and its implications for data privacy. Sullivan testified that he understood that the 2014 Data Breach, which predated his employment at Uber, involved an Amazon Web Services access ID that had been inadvertently posted publicly on GitHub.

9. Sullivan also testified about Uber's storage of database backups in AWS. He was asked about Uber's statement in an interrogatory response that all new database backup files had been encrypted as of August 2014, and he testified about the difficulties using Amazon's native encryption functions and the fact that encryption became more important as companies began moving to cloud-based infrastructure.

The 2016 Data Breach and Payment to the Hackers

10. Approximately ten days after Sullivan's testimony, he learned that Uber's AWS S3 datastore had been breached again. On November 14, 2016, Sullivan received an email from

johndoughs@protonmail.com claiming to have found a "major vulnerability in uber," and that "I was able to dump uber database and many other things."

11. At Sullivan's direction, Uber's security team began an investigation. Within approximately one day, the security team learned that an unauthorized person or persons had, like the 2014 hacker, accessed AWS. The hackers were able to access Uber's source code on GitHub, locate an AWS credential, and use that credential to download Uber's data. Unlike in the 2014 Data Breach, however, where an Uber employee inadvertently posted an AWS credential publicly, the hackers responsible for the 2016 Data Breach used stolen credentials in order to access private GitHub repositories, where they found the code containing an AWS credential.

12. Also within approximately one day, the security team learned that the unauthorized person or persons had obtained, among other things, a copy of a database containing approximately 600,000 drivers' license numbers for Uber drivers.

13. Within hours of contact from the hackers, the security team sealed off the hackers' access point to Uber's data. The security team initiated a password reset, established two-factor authentication for GitHub accounts, and rotated AWS service keys.

14. Records reflect that Sullivan instructed his team to keep knowledge of the 2016 Data Breach tightly controlled. The hackers responsible for the 2016 Data Breach engaged in email communications with Uber representatives in the weeks following the hackers' revelation of the breach. In those communications, the hackers demanded a payment in the six figures. The hackers ultimately received their requested payment under the auspices of Uber's bug bounty program.

15. Generally speaking, a bug bounty program is an invitation for outside experts to search for vulnerabilities in a company's systems and report them to the company that is the sponsor of the particular bug bounty program. These outside experts can augment a company's in-house engineering team, and their efforts can assist a company in identifying and remedying unintentional imperfections in the company's software code. As of November 2016, Uber's bug bounty policy stated that the Company was "interested in any vulnerability that could negatively affect the security of our users." The policy explained that "[i]f you get access to an Uber server please report it [to] us and we will reward you with an appropriate bounty taking into full consideration the severity of what could be done." The policy also indicated that using an "AWS access key to dump user info" was "[n]ot cool."

16. In connection with the payment to the hackers, Sullivan arranged for the hackers to sign non-disclosure agreements ("NDAs") that forbade the hackers from ever disclosing that Uber had been hacked another time. By contrast, the terms of Uber's bug bounty program at the time provided that program participants would be permitted to publicize their activities once Uber had fixed the identified "bug." Specifically, the policy in effect at the time stated, "We're more than happy to publicly disclose your bug once it has been remediated by our developers."

17. The NDAs also contained a provision stating that the hackers "did not take or store any data during or through [their] research." In fact, the hackers did take and store large quantities of data, including data pertaining to approximately 57 million user records, which included the 600,000 drivers' license numbers referenced above. Sullivan and various other Uber employees were aware that the hackers had acquired PII.

18. The two hackers responsible for the 2016 Data Breach signed the NDAs, first under pseudonyms. Uber employees were able to identify and locate the two hackers in January 2017, and the hackers thereafter agreed to execute the same agreements in their real names.

19. The hackers withdrew their $100,000 payment in December 2016, before the hackers had been identified and before members of the security team received assurances that the data had been deleted.

The 2016 Data Breach Was Not Disclosed to the FTC Until November 2017

20. The FTC investigation into Uber's data security practices was pending during Uber's response to the 2016 Data Breach, and Uber continued to respond to FTC interrogatories and document requests. In connection with its responses to the FTC, Uber consulted with Sullivan, who was aware that the FTC's investigation included a focus on data security, data breaches, and protection of PII. Sullivan did not inform the FTC or the attorneys working on the FTC investigation on behalf of Uber of the 2016 Data Breach. For example, on December 20, 2016, Sullivan received by email a copy of a draft set of supplemental interrogatory responses, sent by the in-house attorney responsible for managing the FTC investigation. Those responses stated that "all new database backup files" had been encrypted since August 2014. In fact, the database backup stolen by the hackers in 2016 was created after August 2014 and was not encrypted. The in-house attorney stated in her email, "We anticipate that this will be the last submission, slated for tomorrow night (other than responding to the new set of FTC questions about access controls which we'll respond to in January)." Sullivan responded to the in-house attorney's email, stating that he had been working with another in-house attorney "on getting lots of additional information added to the chart on locking down data access. I think for FTC we could present a pretty compelling narrative given how much we have done." Unaware of the

2016 Data Breach, attorneys working on the FTC investigation on behalf of Uber ultimately submitted interrogatory responses to the FTC containing the statement that "all new database backup files" had been encrypted since August 2014.

21. Additionally, on April 7, 2017, Sullivan received a draft letter that Uber planned to send to the FTC requesting that the FTC close its investigation into Uber. Sullivan responded "Letter looks ok to me. Thanks." Unaware of the 2016 Data Breach, attorneys working on the FTC investigation on behalf of Uber sent the letter to the FTC on April 19, 2017. The letter stated that Uber had implemented a variety of additional security protections since the 2014 Data Breach and that Uber had "described these improved and updated practices extensively in the course of this investigation." The letter also stated that Uber should not be judged for "what a company did *then* (back when the company was much smaller and the technology at issue was evolving) according to the standards that the agency thinks are appropriate *now* (given the current sophistication of the company and current industry best practices)" (emphasis in original). As of the end of April 2017, Uber had not disclosed the 2016 data breach to any law enforcement or regulatory entity, including the FTC.

22. The FTC declined Uber's request to close the investigation. Instead, Uber and the FTC began negotiating a resolution to the investigation, to include a civil complaint and a consent order imposing on Uber certain data security and third-party assessment requirements. Within Uber, Sullivan supported settling with the FTC.

23. In August 2017, the FTC announced a proposed settlement of its investigation. In connection with the proposed settlement, the FTC released for public comment a Complaint and proposed consent order. The Complaint alleged, among other things, that Uber had not provided reasonable security for consumers' personal information stored in AWS. More specifically, and

among other things, the Complaint alleged that "[u]ntil approximately March 2015, [Uber] stored sensitive personal information in the Amazon S3 Datastore in clear, readable text, including in database back-ups and database prune files, rather than encrypting the information." In fact, as the 2016 Data Breach had revealed, Uber's Amazon S3 Datastore contained at least one unencrypted database backup until approximately November 2016. The Complaint also alleged that Uber's failures resulted in an intruder in 2014 being able "to access consumers' personal information in plain text in Respondent's Amazon S3 Datastore . . . ." The Complaint made no reference to the 2016 Data Breach, which occurred during the FTC's investigation, as Uber had not disclosed that breach to the FTC, the public, or law enforcement as of the date of the Complaint. This settlement was never fully finalized because, as discussed below, the FTC withdrew its agreement after Uber voluntarily disclosed the 2016 Data Breach to the FTC (and other regulatory and governmental authorities and the public) in November 2017.

Uber's New Management Discloses the 2016 Data Breach Publicly

24. In June 2017, Uber's CEO ("CEO One")—who had also been CEO at the time of the 2016 Data Breach—stepped down. In August 2017, Uber appointed a new CEO ("CEO Two").

25. In September 2017, Sullivan was asked to brief CEO Two on the 2016 Data Breach. Sullivan asked his team to prepare a summary, which they did. After receiving that summary, Sullivan provided a summary via email to CEO Two that omitted certain key details about the breach. For example, the summary Sullivan received from his team disclosed that an unauthorized party had gained access to "AWS buckets that contained potentially all rider and driver data in plaintext," and that the unauthorized party "still had possession of our data" when he reached out to Uber in 2016. However, the summary that Sullivan subsequently provided to

CEO Two via email disclosed only that the unauthorized party had gained access to "some rider and driver data," and the email did not inform CEO Two that the hackers had taken possession of the data by the time they contacted Sullivan in 2016.

26. In addition, the summary provided to CEO Two stated that the bug bounty payment had been made only after the unauthorized party had been identified. The summary stated that Sullivan's team told the unauthorized party that "we would only pay the bounty if he signed the documents in his real identity," and the summary further stated that he "fully cooperated" with this condition. In fact, the hackers did not sign the documents using their real names, and Sullivan authorized transmission of the payment before the hackers had been identified.

27. Following further investigation by Uber, on November 21, 2017, Uber terminated the employment of Sullivan and another individual who led Uber's response to the 2016 Data Breach. That same day, CEO Two published a blog post regarding the 2016 Data Breach. The blog post disclosed the 2016 Data Breach to the public for the first time. CEO Two explained that he "recently learned that in late 2016 we became aware that two individuals outside the company had inappropriately accessed user data stored on a third-party cloud-based service that we use." That data included the "names and driver's license numbers of around 600,000 drivers in the United States," in addition to "[s]ome personal information of 57 million Uber users around the world," including "names, email addresses and mobile phone numbers." CEO Two also announced that Uber would be notifying the drivers whose drivers' license numbers were downloaded, notifying regulatory authorities, and providing affected drivers with free credit monitoring and identity theft protection.

28. Uber disclosed the 2016 Data Breach to affected drivers, and state and federal agencies, including the Department of Justice and the FTC. Following Uber's disclosure of the 2016 Data Breach, the FTC declined to finalize the previously negotiated Consent Order. Instead, the FTC strengthened the previously negotiated Consent Order in various ways, such as by adding a provision obligating Uber to notify the FTC directly of future data breaches that triggered federal, state, or local reporting requirements, including the nature of the breach, the information that triggered notification, and the acts taken to remediate the incident.

EXHIBIT B

WAIVER OF INDICTMENT

In the event that the United States Attorney's Office for the Northern District of California institutes a criminal prosecution against Uber Technologies, Inc. ("Uber") following a determination of a breach of the Non-Prosecution Agreement, in accordance with Section VI of that Agreement, Uber, having been advised by counsel of its rights and the nature of potential charges arising out of the Statement of Facts, waives its right to indictment and agrees that criminal proceedings may be by information rather than indictment for any federal offense arising out of the Statement of Facts attached as Exhibit A to the Non-Prosecution Agreement.

DocuSigned by:
Tony West
202A018A3690C4A...

July 20, 2022

Uber Technologies, Inc. DATE
by: Tony West, Chief Legal Officer

Steven E. Fagell

July 20, 2022

Steven E. Fagell DATE
W. Douglas Sprague
Covington & Burling LLP
Counsel for Uber Technologies, Inc.

EXHIBIT C

COMPANY OFFICER'S CERTIFICATE

I have carefully reviewed every part of this Non-Prosecution Agreement, including Exhibits A through D, with outside counsel for Uber Technologies, Inc. ("Uber"). I understand the terms of this Agreement and voluntarily agree, on behalf of Uber, to each of its terms. Before signing this Non-Prosecution Agreement, I consulted with outside counsel for Uber. Counsel fully advised me of Uber's rights, of possible defenses, of the Sentencing Guidelines' provisions, and of the consequences of entering into this Non-Prosecution Agreement.

No promises or inducements have been made other than those contained in this Non-Prosecution Agreement. Furthermore, no one has threatened or forced me, or to my knowledge any person authorizing this Non-Prosecution Agreement on behalf of Uber, in any way to enter into this Non-Prosecution Agreement. I am also satisfied with outside counsel's representation in this matter. I certify that I am duly authorized by Uber's Board of Directors to execute this Non-Prosecution Agreement on behalf of Uber.

DocuSigned by:
Tony West
282A918A3690444...

July 20, 2022

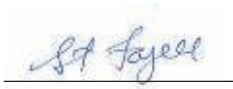
Uber Technologies, Inc.
by: Tony West, Chief Legal Officer

DATE

EXHIBIT D

CERTIFICATE OF COUNSEL

The undersigned is counsel for Uber Technologies, Inc. ("Uber") in the matter covered by this Non-Prosecution Agreement. In connection with such representation, I have examined relevant company documents and have discussed the terms of this Non-Prosecution Agreement with Management for Uber. Based on my reviews of the foregoing materials and discussions, I am of the opinion that Tony West is duly authorized to enter into this Non-Prosecution Agreement on behalf of Uber, and that this Non-Prosecution Agreement has been duly and validly authorized, executed, and delivered on behalf of Uber, and is a valid and binding obligation of Uber. Further, I have carefully reviewed the terms of this Non-Prosecution Agreement with Mr. West. I have fully advised him of Uber's rights, of possible defenses, of the Sentencing Guidelines' provisions, and of the consequences of entering into this Non-Prosecution Agreement. To my knowledge, Uber's decision to enter into this Non-Prosecution Agreement, based on the authorization of Mr. West, is informed and voluntary.



July 20, 2022

Steven E. Fagell
W. Douglas Sprague
Covington & Burling LLP
Counsel for Uber Technologies, Inc.

DATE