

November 21, 2017

Rebecca S. Engrav
REnggrav@perkinscoie.com
D. +1.206.359.6168
F. +1.206.359.7168

Office of the Attorney General of Iowa
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, IA 50319-0106

RECEIVED
17 NOV 27 PM 12:20
CONSUMER PROTECTION DIV.

Re: Notification of Security Breach

To Whom It May Concern:

On behalf of our client Uber Technologies, Inc. ("Uber"), we are writing to notify you of a data security incident.

In November 2016, Uber was contacted by an individual who claimed he had accessed Uber user information. Uber investigated and determined that the individual and another person working with him had obtained access to certain stored copies of Uber databases and files located on Uber's private cloud data storage environment on Amazon Web Services. Uber determined the means of access, shut down a compromised credential, and took other steps intended to confirm that the actors had destroyed and would not use or further disseminate the information. Uber also implemented additional measures to improve its security posture. To the best of Uber's knowledge, the unauthorized actor's access to this data began on October 13, 2016, and there was no further access by the actor to Uber's data after November 15, 2016.

As determined by Uber and outside forensic experts, the accessed files contained user information that Uber used to operate the Uber service. Most of this information does not trigger data breach notifications under state law. However, the files did include, for a subset of users in the files, the names and driver's license numbers of about 600,000 Uber drivers in the United States.¹ Beginning on November 22, 2017, Uber is providing notice to the individuals whose driver's license information was downloaded in this incident. Uber will offer 12 months of credit monitoring and identity theft protection services to these individuals free of charge, and the notice will provide information on how to use such services. A copy of the notice is enclosed.

As it has publicly announced today, Uber now thinks it was wrong not to provide notice to affected users at the time. Accordingly, Uber is now providing notice. In order to treat its driver

¹ The files also included other types of data and salted and hashed user passwords, but they do not trigger notification.

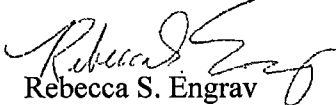
November 21, 2017
Page 2

partners consistently throughout the United States, Uber is providing notice to affected drivers in all states without regard to whether the facts and circumstances of this incident (or the number of affected individuals) trigger notification in each particular state.

Uber is taking personnel actions with respect to some of those involved in the handling of the incident. In addition, Uber has implemented and will implement further technical security measures, including improvements related to both access controls and encryption.

Uber sincerely regrets that this incident occurred. It is committed to working with your office to address this matter. Please do not hesitate to contact me with any questions or for more information. My contact information is above.

Very truly yours,


Rebecca S. Engrav

Attachment

Return Mail Processing
P.O. Box 589
Claysburg, PA 16625-0589



1455 Market Street
San Francisco, CA 94103
UBER.com

##D2700-L01-0123456 0001 00000001 *****9-OELZZ 123

SAMPLE A SAMPLE



APT ABC

123 ANY ST

ANYTOWN, US 12345-6789



November 22, 2017

NOTICE OF DATA BREACH

Dear Sample A Sample:

I am writing to let you know about a data security incident at Uber that affected your information. Uber deeply regrets that this happened and we recommend that you closely review the information in this letter.

What Happened	In November 2016, Uber learned that unauthorized actors obtained access to a private cloud storage environment used by Uber. They accessed stored copies of Uber databases and files. To the best of our knowledge, the unauthorized access began on October 13, 2016 and ended no later than November 15, 2016.
What Information Was Involved	The accessed files contained user information that Uber used to operate the Uber service, including your name and driver's license number. The files included this information for about 600,000 Uber drivers in the United States.
What We Are Doing	We have made changes to our data storage environment and security procedures to decrease the chance of a similar occurrence in the future. To assist you, we are also providing identity theft protection and mitigation services from Experian, including credit monitoring, for twelve (12) months at no cost to you. See details below.
What You Can Do	We recommend enrolling in Experian IdentityWorks SM and reviewing the additional information below.
For More Information	If you have any questions regarding this incident or if you desire further information or assistance, please contact (844) 439-7669.

Again, and on behalf of everyone at Uber, I am sorry that this happened. Drivers like you are at the heart of our service. Simply put, Uber wouldn't exist without you and we thank you for your partnership.

Sincerely,

Dara Khosrowshahi
Chief Executive Officer

0123456



Activate Experian IdentityWorksSM

We encourage you to activate the fraud detection tools available through Experian IdentityWorksSM as a complimentary one-year membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: February 28, 2018**. (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcreditone
- Provide your **activation code: ABCDEFGHI**

Additionally, complimentary Identity Restoration assistance is immediately available to you. If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this offer is available to you for one year from the date of this letter and does not require any action on your part at this time.

The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

If you have questions about these products, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (844) 439-7669 by **February 28, 2018**. Be prepared to provide engagement number [REDACTED] as proof of eligibility for the identity restoration services by Experian.

Additional Steps You Can Take

Learn More and Report Suspected Identity Theft

You are encouraged to contact the Federal Trade Commission (FTC), law enforcement, or your state attorney general's office to report incidents of suspected identity theft or to learn about steps you can take to protect yourself from identity theft. You can contact the FTC at:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
www.identitytheft.gov

If you find that your information has been misused, the FTC encourages you to file a complaint with the FTC and to take these additional steps: (1) close the accounts that you have confirmed or believe have been tampered with or opened fraudulently; and (2) file and keep a copy of a local police report as evidence of the identity theft crime.

You can contact the nationwide consumer reporting agencies at:

Equifax
P.O. Box 105788
Atlanta, GA 30348
(800) 525-6285
www.equifax.com

Experian
P.O. Box 9554
Allen, TX 75013
(888) 397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19016
(800) 680-7289
www.transunion.com

You should remain vigilant for incidents of fraud, identity theft, and errors by regularly reviewing your account statements and monitoring free credit reports. If you discover any suspicious or unusual activity on your accounts, be sure to report it immediately to your financial institutions, as major credit card companies have rules that restrict them from requiring you to pay for fraudulent charges that are timely reported.

Obtain Your Credit Reports

You should also monitor your credit reports. You may periodically obtain free credit reports from each nationwide consumer reporting agency. If you discover inaccurate information or a fraudulent transaction on your credit report, you have the right to request that the consumer reporting agency delete that information from your credit report file.

You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

Place a Fraud Alert or Security Freeze on Your Credit Report File

A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. You should know that it also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide consumer reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file. An initial fraud alert will last 90 days. An extended alert stays on your file for seven years. To place either of these alerts, a consumer reporting agency will require you to provide appropriate proof of your identity, which may include your Social Security number. If you ask for an extended alert, you will have to provide an identity theft report.

A security freeze, sometimes called a credit freeze, is designed to prevent credit, loans, and services from being approved in your name without your consent. You should know that it also may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. Unlike a fraud alert, you must separately place a security freeze on your credit file by sending a request to each of the three major credit reporting agencies listed above. When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

0123456



With certain exceptions, a consumer reporting agency may charge you a fee to place a freeze on your credit report, to temporarily lift a freeze on your credit report, or to remove a freeze from your credit report.

IF YOU ARE A MARYLAND RESIDENT:

You may obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's Office. This office can be reached at:

Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(410) 576-6491
www.oag.state.md.us

IF YOU ARE A NORTH CAROLINA RESIDENT:

You may obtain information about preventing identity theft from the North Carolina Attorney General's Office. This office can be reached at:

North Carolina Department of Justice
Office of the Attorney General
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
<http://www.ncdoj.gov>

IF YOU ARE A RHODE ISLAND RESIDENT:

You have the right to obtain a police report in regard to this incident, and if you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. Additionally, you may obtain information about preventing identity theft from the Rhode Island Attorney General's Office. This office can be reached at:

Rhode Island Office of the Attorney General
150 South Main Street
Providence, RI 02903
(401) 274-4400
<http://www.riag.ri.gov/>

IF YOU ARE A RESIDENT OF OTHER STATES:

Your state attorney general's office and website may also provide relevant information.

PERKINScoie

1201 Third Avenue
Suite 4900
Seattle, WA 98101-3099

SEATTLE
WA 980
21 NOV '17
PM 5 L

neopost
11/21/2017
FIRST-CLASS MAIL
US POSTAGE \$000.46⁰



ZIP 98101
0411417051348

Office of the Attorney General of Iowa
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, IA 50319-0106

50319-010999

