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℠ 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.

0123456

Sincerely,

Dara Khosrowshahi
Chief Executive Officer

D2700-L01

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

D2700-L01