PERKINSCOIE

1201 Third Avenue
Suite 4900
Seattle, WA 98101-3099

+1.206.359.8000
+1.206.359.9000
PerkinsCoie.com

March 31, 2023

VIA EMAIL

State of New Hampshire
Department of Justice
Office of the Attorney General John M. Formella
33 Capitol Street
Concord, NH 03301
attorneygeneral@doj.nh.gov

Re: Notification of Security Incident

Dear Attorney General Formella:

I write on behalf of Uber Technologies, Inc. regarding a recent data incident involving personal information of residents of your state. On March 1, 2023, Genova Burns LLC, legal counsel to Uber, confirmed that data involving certain information related to the firm's representation of Uber was impacted during a cybersecurity event impacting Genova Burns. On March 2, 2023, Genova Burns notified Uber about the incident. Genova Burns became aware of suspicious activity on its information systems on January 31, 2023, and launched an investigation. It determined that an unauthorized third party gained access to its systems and certain limited files were accessed or exfiltrated between January 23, 2023 and January 31, 2023. The impacted file contained information certain drivers had provided to Uber, for approximately 13 residents of your state. At this time, Genova Burns is not aware of any actual or attempted misuse of any information obtained in this incident.

Genova Burns has indicated to Uber that it is taking additional steps to improve its security and better protect against similar incidents in the future. It has investigated to determine the nature and scope of the incident and secured the environment by changing all system passwords. It has notified and is cooperating with law enforcement.

Enclosed is a copy of the notification being mailed to affected individuals beginning March 31, 2023.

Sincerely,

Rebecca S. Engrav

Attachment: Template Individual Notice

ATTACHMENT

GENOVA BURNS

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

NOTICE OF DATA BREACH

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Genova Burns LLC ("Genova Burns") is writing to notify you of a recent data security incident that may have impacted your personal information, which is in our possession due to our legal representation of Uber Technologies, Inc. In connection with this legal representation, we received data regarding certain drivers on the Uber platform, which included information about you. We want to provide you with information about the incident, our response, and steps you may take to better help protect against possible misuse of your personal information.

What Happened? On January 31, 2023, Genova Burns became aware of suspicious activity relating to our internal information systems. In response, we engaged outside forensic and data security specialists to investigate the nature and scope of the activity. We determined that an unauthorized third party gained access to our systems and certain limited files were accessed or exfiltrated between January 23, 2023 and January 31, 2023. In response, we undertook a comprehensive review to determine what was impacted. On March 1, 2023, we determined that information related to you was contained in an impacted file, after which we notified Uber. At this time, we are unaware of any actual or attempted misuse of your information as a result of this incident.

What Information Was Involved? The investigation determined that information you provided to Uber, including was among the impacted data.

What We Are Doing. The confidentiality, privacy, and security of personal information within our care is important to us. Upon learning of the event, we investigated to determine the nature and scope of the incident and secured the environment by changing all system passwords. We also notified law enforcement and are cooperating with its investigation. We will be taking additional steps to improve security and better help protect against similar incidents in the future. As an added precaution, Genova Burns is offering you access to 12 months of complimentary identity monitoring services through Kroll. Details of this offer and instructions on how to activate the services may be found in the attached *Steps You Can Take to Help Protect Personal Information*.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements. Additional information may be found in the attached *Steps You Can Take to Help Protect Personal Information*.

For More Information. We understand you may have questions that are not answered in this letter. If you have questions or concern regarding this incident, we ask that you please contact our dedicated assistance line at 1-???-???-???? between the hours of 9:00 am and 6:30 pm Eastern Time, Monday through Friday, excluding major U.S. holidays. You may also write to Genova Burns at 494 Broad Street Newark, NJ 07102.

Sincerely,

James Burns
Managing Partner
Genova Burns

Steps You Can Take to Help Protect Personal Information

Activate Identity Monitoring

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.

Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are [#] Rhode Island residents impacted by this incident.