

RECEIVED

SEP 27 2019

D/-

CONSUMER PROTECTION DIVISION
SEATTLE

BakerHostetler

Baker&Hostetler LLP

11601 Wilshire Boulevard
Suite 1400
Los Angeles, CA 90025-0509

T 310.820.8800
F 310.820.8859
www.bakerlaw.com

M. Scott Koller
direct dial: 310.979.8427
mskoller@bakerlaw.com

September 26, 2019

**VIA EMAIL (SECURITYBREACH@ATG.WA.GOV)
AND OVERNIGHT MAIL**

Office of the Washington Attorney General
Consumer Protection Division
800 5th Ave., Suite 2000
Seattle, WA 98104-3188

Re: *Incident Notification*

Dear Sir or Madam:

We are writing on behalf of our client, DoorDash Inc. ("DoorDash"), to notify you of a data security incident.

On September 5, 2019, DoorDash became aware of unusual activity involving a third-party service provider. Upon learning of this, DoorDash immediately launched an investigation and outside security experts were engaged to assess what occurred. DoorDash was subsequently able to determine that an unauthorized third-party accessed some DoorDash user data on May 4, 2019. DoorDash took immediate steps to block further access by the unauthorized third-party and to enhance security across its platform.

DoorDash's investigation determined that account information for some users, merchants and Dashers¹ who joined its platform on or before April 5, 2018 was accessed, including names email address, phone number, hashed/salted password², and in some cases, the last four digits of the payment card or bank account number associated with their DoorDash Account. For some Dashers, their name and driver's license number were also accessed.

¹ Dashers are individuals who sign up with DoorDash to deliver food and other items from merchants to DoorDash customers.

² "Hashing and Salting" is a form of rendering the actual password indecipherable to third parties. Access or acquisition of the hashed password does not allow access to the individual's online account.

Atlanta Chicago Cincinnati Cleveland Columbus Costa Mesa Denver
Houston Los Angeles New York Orlando Philadelphia Seattle Washington, DC


Beginning on September 26, 2019, DoorDash is providing notification via email with a copy sent via United States Postal Service First-Class mail to those Dashers whose names and driver's license numbers were involved, including to 2,243 Washington residents, in accordance with Wash. Rev. Code § 19.255.010. A copy of the notification letter is enclosed. Even though access to the hashed and salted passwords would not allow access to the individual's account, DoorDash is also notifying all users, Dashers, and merchants whose account information was accessed.

In addition to issuing a press release and posting notice on its website, DoorDash is also providing a telephone number for individuals to call with any questions they may have. DoorDash is offering Dashers whose driver's license numbers were involved complimentary one-year memberships to ID Experts® MyIDCare™, which include credit monitoring and fraud protection services.

To help prevent something like this from happening in the future, DoorDash has taken a number of additional steps to further secure its users data, which include adding additional protective security layers around the data, improving security protocols that govern access to its systems, and bringing in outside expertise to increase its ability to identify and repel threats.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,



M. Scott Koller
Partner

Enclosure



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Name 1>>

<<Name 2>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<Address 4>>

<<Address 5>>

<<City>><<State>><<Zip>>

<<Country>>

<<Date>>

Important Security Notice About Your DoorDash Account

Dear [NAME],

What Happened:

We take the security of our community very seriously. Earlier this month, we became aware of unusual activity involving a third-party service provider. We immediately launched an investigation and outside security experts was engaged to assess what occurred. We were subsequently able to determine that an unauthorized third party accessed some DoorDash user data on May 4, 2019. We took immediate steps to block further access by the unauthorized third party and to enhance security across our platform.

What Information Was Involved:

Based on our investigation, we believe that some of your DoorDash user account information has been accessed, including your name and driver's license number. Other types of data that have been accessed could include:

Profile information including email address, phone number, date of birth, information from your Dasher sign up process, hashed, salted passwords—a form of rendering the actual password indecipherable to third parties, and the last four digits of your bank account number. Please note that full bank account information

was not accessed. The information accessed is not sufficient to make fraudulent charges on your payment card or fraudulent withdrawals from your bank account.

What We Are Doing:

While we have no reason to believe your information has been misused, because of the nature of driver's license information, as a precaution, we are offering MyIDCare™ identity theft protection services through ID Experts®. MyIDCare services include: Credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised. To sign up for these services, please visit <https://ide.myidcare.com/doordash>. You'll be prompted to enter an authorization code. Your unique authorization code is [UNIQUE CODE]. To help prevent something like this from happening in the future, we have also taken a number of additional steps to further secure your data, which include adding additional protective security layers around the data, improving security protocols that govern access to our systems, and bringing in outside expertise to increase our ability to identify and repel threats.

What You Can Do:

We encourage you to take advantage of the identity theft protection services being offered. We do not believe that user passwords have been compromised, but out of an abundance of caution, we are encouraging all users whose information was involved to reset their passwords to one that is unique to DoorDash. As a best practice, if you use the same password for multiple accounts, we recommend that you reset your passwords for all those accounts. You can change your DoorDash password by visiting <https://www.doordash.com/accounts/password/reset/> and using the email address associated with your DoorDash account.

For More Information:

We deeply regret the frustration and inconvenience that this may cause you. Every member of the DoorDash community is important to us, and we want to assure you that we value your information security and privacy. For further information, please see our blog and FAQ page by visiting blog.doordash.com. We've also set up a dedicated call center available 24/7 for support at 855-646-4683.

We know that you trust us to connect you with the best of your community, and we will never take that trust for granted.

Team DoorDash

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

If you are a resident of Maryland or North Carolina, you may contact and obtain information from your state attorney general at:

- *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us
- *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6400 / 1-877-566-7226, www.ncdoj.gov

If you are a resident of West Virginia, you have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described below. You also have a right to place a security freeze on your credit report, as described below.

Fraud Alerts: There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one (1) year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Credit Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and

other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

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 years, provide 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, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one hour after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have one hour after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty

agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Here is a summary of your major rights under FCRA. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies 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 reports to be provided to employers.
- You may limit “prescreened” offers of credit and insurance you get based on information in your credit report.
- You have a right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.