PAUL
HASTINGS

1(202) 551-1216
rsilvers@paulhastings.com

August 20, 2020

VIA E-MAIL (SECURITYBREACH@ATG.WA.GOV)

Washington State Office of the Attorney General
1125 Washington St SE
PO Box 40100
Olympia, WA 98504

RE: Data Security Incident Notice

Dear Office of the Attorney General:

My law firm represents Dave, Inc. ("Dave"). Pursuant to RCW 19.255.010, I am writing to notify you of a data security incident at Dave involving approximately 40,998 residents of Washington.

NATURE OF THE DATA SECURITY INCIDENT

As a result of a breach at a former third-party service provider, an unauthorized party illegally accessed and stole certain customer data at Dave between June 23 and July 1, 2020. As soon as Dave became aware of this incident on July 1, 2020, Dave's security team quickly took steps to secure the company's systems, including its customers' accounts. Dave immediately began an investigation, retained a leading cybersecurity firm, and notified law enforcement, including the Federal Bureau of Investigation ("FBI").

After the compromise at Dave's service provider, the unauthorized party was able to gain temporary access to Dave's systems and obtained certain Dave customer data. It appears this data is now posted online as available for sale on, or download from, illicit online marketplaces, which the FBI is aware of and is investigating. The types of data that may have been exposed as a result of this incident included the following. However, not every customer had every data element exposed:

- First and last name
- Email
- Phone
- Date of birth
- Physical address
- Gender
- Profile image
- Customer application preferences (e.g., notification frequency, default tip percentage, etc.)
- Hashed password
- Encrypted Social Security number

Importantly, the breach did not affect bank account numbers, credit card numbers, or records of financial transactions. Dave has no evidence of fraudulent customer account usage or that any customer has experienced any financial loss as a result of this incident. Dave also has no evidence to indicate the unauthorized party accessed the encryption keys used to encrypt Social Security numbers. Social Security numbers were encrypted using AES-256 encryption and customer passwords were stored in illegible form using bcrypt, an industry-recognized hashing algorithm. Dave subsequently confirmed the likelihood that a party was able to "crack" or determine the plain text characters of at least some of the stolen hashed passwords.

REMEDIAL STEPS

Dave is no longer working with the third-party service provider whose security breach enabled the unauthorized party to ultimately obtain Dave's customer data. Moreover, upon Dave's discovery of the incident, Dave's security team quickly took steps to secure the company's systems, including its customers' accounts. Dave retained a leading cybersecurity company to investigate and to provide remediation recommendations. Dave has forced a reset of all customer login credentials and is requiring all customers to change their passwords. When logging in, customers will receive instructions on how to change their password, which they should do immediately. Dave is also advising customers to change passwords on any other sites where they used the password they had previously used with Dave. Dave's security team has also put in place additional technical measures to enhance account security, in consultation with independent cybersecurity experts, which will provide additional layers of security and protection.

NOTIFICATION TO AFFECTED WASHINGTON RESIDENTS

Notices to the approximately 40,998 Washington residents whose personal information was compromised will be sent beginning tomorrow based on available contact information, by email as authorized, or via U.S. mail. A representative sample of the notice is attached. In addition, the company is posting information about the incident on its website and major social media platforms, as well as to major statewide print and broadcast media. Dave has made arrangements for potentially affected customers to receive complimentary identity protection services through December 31, 2021. Additional information on the identity theft protection services is included in the attached sample notification made to the affected parties.

CONTACT INFORMATION

Should you have any additional questions, please contact me at rsilvers@paulhastings.com or (202) 551-1216.

Sincerely,

/s/ Robert Silvers

Robert Silvers
of PAUL HASTINGS LLP

Enclosure: 1

1265 South Cochran Avenue
Los Angeles, CA 90066

August 21, 2020

[Customer Name]
[Customer Address]
[City, State, ZIP]

RE: Notice of Data Breach

Dear [Customer Name],

We are writing on behalf of Dave, Inc. ("Dave") to inform you about a cybersecurity incident affecting certain personal information. We value our relationship with you and take data protection and privacy issues seriously. This notification provides you with information about the incident and outlines additional steps you may take to help protect yourself.

What Happened?

As a result of a breach at a former third-party service provider, an unauthorized party illegally accessed and stole certain customer data at Dave between June 23 and July 1, 2020. As soon as we became aware of this incident on July 1, 2020, our security team quickly took steps to secure our systems including our customers' accounts. We immediately began an investigation, retained a leading cybersecurity firm, and notified law enforcement, including the Federal Bureau of Investigation ("FBI").

After the compromise at Dave's service provider, the unauthorized party was able to gain temporary access to Dave's systems and obtained certain Dave customer data. It appears this data is now posted online as available for sale on, or download from, illicit online marketplaces, which the FBI is aware of and is investigating. You are receiving this notice because we determined that your records are among those that may have been impacted.

What Information Was Involved?

The types of data that may have been exposed as a result of this incident included the following. However, not every customer had every data element exposed:

- First and last name
- Email
- Phone
- Date of birth
- Physical address
- Gender
- Profile image
- Hashed password
- Encrypted Social Security number
- Customer application preferences (e.g., notification frequency, default tip percentage, etc.)

Importantly, the breach did not affect bank account numbers, credit card numbers, or records of financial transactions. Dave has no evidence of fraudulent customer account usage or that any customer has experienced any financial loss as a result of this incident. We also have no evidence to indicate the unauthorized party accessed the encryption keys used to encrypt your Social Security number. Social Security numbers were encrypted using AES-256 encryption and customer passwords were stored in illegible form using bcrypt, an industry-recognized hashing algorithm. We subsequently confirmed, however, the likelihood that a party was able to "crack" or determine the plain text characters of at least some of the stolen hashed passwords.

What We Are Doing

Please be assured that we take this matter seriously and continue to implement measures to secure your personal information. We are no longer working with the third-party service provider whose security breach enabled the unauthorized party to obtain your data. Moreover, upon our discovery of the incident, our security team quickly took steps to secure our systems including our customers' accounts. We have forced a reset of all customer login credentials and are requiring all customers to change their passwords. When logging in, you will receive instructions on how to change your password, which you should do immediately. Dave's security team has also put in place additional technical measures to enhance account security in consultation with our independent cybersecurity experts that will provide additional layers of security and protection.

Recognizing that identity protection is of paramount concern, we have partnered with Mastercard ID Theft Protection to provide you with complimentary identity theft resolution services through December 31, 2021. If you are not already enrolled in this or a similar service, please refer to the instructions in the attachment and enroll at https://mastercardus.idprotectiononline.com/.

What You Can Do

First, in order to further protect your account and related information, we require that you create a new, strong password as soon as possible that you have never used elsewhere before. We also recommend that if you use your old password on other accounts, you should change those passwords too.

Here are some helpful tips when creating a password:

DO:

- Use LONG passwords.
- Use UNIQUE passwords. Each website and application you access should have a different password, not just a modification of the same password (ex.: changing the number at the end).
- Use PASS PHRASES whenever possible. Pass phrases are when you combine multiple words into a phrase and use it as your password (ex.: DogJumpHouseRoad).

DON'T:

- Use the same password for different accounts.
- Write down passwords.
- Recycle the same password by changing the number at the end (ex.: Password1, Password2, etc.).

After logging into your account, please review your account information and activity. If you notice anything unusual or suspicious, please contact us at support@dave.com or by phone at 1-888-865-8193.

Going forward, you should continue to monitor your account statements and credit reports for evidence of fraud or identity theft. For more information on steps you can take to protect your information, please review the attached instructions entitled "*Steps You Can Take to Protect Your Information.*"

More Information

If you have any additional questions, please contact us at support@dave.com or by phone at 1-888-865-8193. You may also write to us at 1265 S Cochran Avenue, Los Angeles, CA 90019. On behalf of Dave's entire team, we regret this incident and apologize for any concern or inconvenience it may cause.

Sincerely,
The Dave team

1265 South Cochran Avenue
Los Angeles, CA 90066

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Enroll in Mastercard ID Theft Protection™

Dave has partnered with Mastercard ID Theft Protection to provide you with complimentary identity theft resolution services through December 31, 2021. To enroll in this service, please visit https://mastercardus.idprotectiononline.com/ and enter the following 16-digit code: [●].

This service is offered through Iris on watch®, Generali Global Assistance's proprietary Internet surveillance technology, which proactively detects the illegal trading and selling of personally identifiable information online. At any point in time, Iris on watch® is tracking thousands of websites and millions of data points, and alerting customers whose personal information they find has been compromised online. This information is being gathered in real-time so that you have the opportunity to react quickly and take the necessary steps to protect yourself.

The Mastercard services also include the following features:

- Providing a uniform Identity Theft Affidavit and assisting with completion of the Affidavit. (Note that it is your responsibility to submit the Affidavit to the proper authorities, credit bureaus, and creditors.)
- Assisting in notifying all three major credit reporting agencies to obtain a free credit report and assisting with placing an alert on your record with the agencies.
- Providing information about how identity theft can occur and protective measures to avoid further occurrences.
- Providing an Identity Theft Resource Kit.
- Providing sample letters for use in canceling checks, ATM cards, and other accounts.

These services are provided are on a 24-hour basis, 365 days a year. If you have questions about the services, or believe that you have been a victim of Identity Theft, simply contact 1-800-Mastercard.

In addition to enrolling in Mastercard ID Theft Protection, we recommend taking the following steps:

- Remain vigilant about reviewing your financial accounts and monitoring free credit reports to detect any suspicious activity. See below for more information.
- Consider placing a fraud alert or security freeze on your account with the credit agencies. See below for more information.
- Contact the Federal Trade Commission ("FTC") Consumer Response Center for further information on fraud alerts and security freezes at 600 Pennsylvania Avenue, NW, Washington, DC 20580, by calling 1-877-IDTHEFT (877-438-4338), or through their website at www.consumer.gov/idtheft.
- Report any suspected identity theft to law enforcement, including the FTC.

If you are a resident of the following states:

- If you are a resident of **Maryland**, you may contact the Maryland Office of the Attorney General for further information on consumer protection at 200 St. Paul Place, Baltimore, MD 21202, by calling 1-888-743-0023, or through their website at http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx.
- If you are a resident of **Washington, D.C.**, you may contact the Office of the Attorney General for the District of Columbia for further information on consumer protection at 441 4th Street, NW, Washington D.C. 20001, by calling (202) 442-9828, or through their website at https://oag.dc.gov/consumer-protection/consumer-alert-identity-theft#:~:text=You%20should%20file%20a%20complaint,at%20202%2D727%2D4159.
- If you are a resident of **New York**, you may contact New York State Office of the Attorney General for further information on consumer protection at The Capitol, Albany, NY 12224-0341, by calling 1-800-771-7755, or through their website at https://ag.ny.gov/consumer-frauds/identity-theft#:~:text=Depending%20on%20your%20specific%20situation,(800)%20771%2D7755.
- If you are a resident of **North Carolina**, you may contact the North Carolina Department of Justice for further information about preventing identity theft at 9001 Mail Service Center, Raleigh, NC 27699-9001, by calling 1-877-566-7226, or through their website at https://ncdoj.gov/protecting-consumers/identity-theft/.
- If you are a resident of **Oregon**, report any suspected identity theft to the Oregon Department of Justice or contact the Oregon Department of Justice for further information on consumer protection at 1162 Court St. NE, Salem, OR 97301-4096, by calling 1-877-877-9392, or through their website at https://www.doj.state.or.us/consumer-protection/id-theft-data-breaches/identity-theft/.
- If you are a resident of **Rhode Island**, you may contact the Office of the Attorney General for Rhode Island for further information on consumer protection at 150 South Main Street, Providence, RI 02903, by calling (401) 274-4400, or through their website at http://www.riag.ri.gov/ConsumerProtection/About.php. You may also file or obtain a police report by contacting your local police department. The report may be filed in the location in which the offense occurred, or the city or county in which you reside. The personal information of approximately 5,971 Rhode Island residents was affected by the breach.
- If you are a resident of **Iowa**, you should report suspected incidents of identity theft to local law enforcement or the Office of the Attorney General of Iowa at Hoover State Office Building, 1305 E. Walnut Street, Des Moines, Iowa 50319-0106, by calling 888-777-4590, or through their website at: https://www.iowaattorneygeneral.gov/for-consumers/general-consumer-information/identity-theft
- If you are a resident of **Massachusetts**, you may also file or obtain a police report by contacting your local police department. The report may be filed in the location in which the offense occurred, or the city or county in which you reside.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, (877) 322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report, as follows:

- **Experian**: P.O. Box 9532, Allen, TX 75013, (888) 397-3742 or www.experian.com
- **TransUnion**: P.O. Box 1000, Chester, PA 19022, (800) 888-4213 or www.transunion.com
- **Equifax**: P.O. Box 740241, Atlanta, Georgia 30374-0241, (800) 685-1111 or www.equifax.com

Security Freezes

You have the 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. The security 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 security 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 security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies, as follows:

- **Experian**: P.O. Box 9554, Allen, TX 75013, (888) 397-3742 or www.experian.com/freeze/center.html
- **TransUnion**: P.O. Box 160, Woodlyn, PA 19094, (800) 909-8872 or www.transunion.com/credit-freeze
- **Equifax**: P.O. Box 105788, Atlanta, Georgia 30348-5788, (888) 298-0045 or www.equifax.com/personal/credit-report-services/credit-freeze/

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, 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 either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

Fraud Alerts

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your 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 agencies listed below:

- **Experian**: P.O. Box 2002, Allen, TX 75013, (888) 397-3742 or www.experian.com/fraud/center.html
- **TransUnion**: P.O. Box 2000, Chester, PA 19016, (800) 680-7289 or www.transunion.com/fraud-victim-resource/place-fraud-alert
- **Equifax**: P.O. Box 105069, Atlanta, Georgia 30348, (888) 766-0008 or www.equifax.com/personal/credit-report-services