Jennifer C. Archie
Direct Dial: (202) 637-2205
jennifer.archie@lw.com

LATHAM & WATKINS LLP

STATE OF NH
DEPT OF JUSTICE
2016 MAR 11 AM 10:48

555 Eleventh Street, N.W., Suite 1000
Washington, D.C. 20004-1304
Tel: +1.202.637.2200 Fax: +1.202.637.2201
www.lw.com

FIRM / AFFILIATE OFFICES

Abu Dhabi	Milan
Barcelona	Moscow
Beijing	Munich
Boston	New Jersey
Brussels	New York
Century City	Orange County
Chicago	Paris
Dubai	Riyadh
Düsseldorf	Rome
Frankfurt	San Diego
Hamburg	San Francisco
Hong Kong	Shanghai
Houston	Silicon Valley
London	Singapore
Los Angeles	Tokyo
Madrid	Washington, D.C.

March 10, 2016

Attorney General Joseph A. Foster
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Dear Attorney General Foster:

I am writing on behalf of my client, Care.com, Inc. (Care.com), to notify you that on March 3, 2016, my client became aware that certain 2015 payroll data was acquired by an unauthorized party on or about March 3, as a result of a phishing attack targeted at Care.com.

The 2015 payroll data contained the IRS Form W-2s, including name, address, Social Security number, and 2015 salary and tax information, for 39 New Hampshire residents. This payroll data was acquired (not merely accessed) by the unauthorized party.

Care.com is preparing to notify the 39 residents of New Hampshire affected by the unauthorized access with a letter to be dated March 10, 2016. In addition to information about the breach, the notice will provide contact information should the individual have questions about the incident, free identity theft monitoring as offered by AllClear ID, and resources and guidance for dealing with identity theft and tax fraud. A copy of the planned notice is attached.

Please contact me at (202) 637-2205 or jennifer.archie@lw.com in the event that you have any questions regarding this matter.

Sincerely yours,

Jennifer C. Archie /AGS

Jennifer C. Archie
LATHAM & WATKINS LLP

Enclosure

77 Fourth Avenue, 5th Floor, Waltham, MA 02451

00076
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789
United States

00002
ACD1234

March 10, 2016

Dear John:

On March 3, 2016, we became aware of a disclosure of certain 2015 Care.com payroll data to an unauthorized party, as a result of a cyberattack on March 3, 2016. The compromised information also included certain 2015 payroll information of Care.com's US based subsidiaries (Breedlove & Associates, Care Concierge and Citrus Lane). Unfortunately, a review of the data in question has determined that some of your personally identifiable information was acquired by this unauthorized party, including the following types of data: first name; last name; address; Social Security number; and 2015 salary and tax related information.

We are alerting affected individuals so that you can take steps to protect yourself. We consider the security of our current and former employees' personal information a serious matter. We will continue to address this incident and will inform you promptly if we become aware of any new information regarding this matter.

As a precaution, Care.com has made arrangements for free credit watch monitoring and identity repair services over a 24 month period as an extra and valuable measure. **We urge you to carefully review this letter and its attachments, and to enroll in the offered benefits.** This service, provided by AllClear ID, will start on the date of this notice and you can use it at any time during the next 24 months.

AllClear SECURE: The team at AllClear ID is ready and standing by if you need identity repair assistance. This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-877-579-2261 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

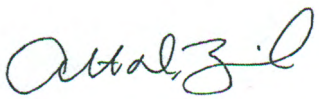
AllClear PRO: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. To use the PRO service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-877-579-2261 using the following redemption code: Redemption Code. Please note that additional steps may be required by you in order to activate your phone alerts and monitoring options.

01-04-2-00

You will also find attached to this letter some steps that you can take to protect your identity. We encourage you to review these steps and take appropriate action to help prevent any misuse of your information.

We are incredibly sorry that this happened and for the inconvenience it may cause. We wish to assure you that we are actively managing this incident, as well as our security practices for safeguarding our payroll data. If you have questions about this incident, we ask that you direct them to me at (781) 693-1781 or azink@care.com or to Marsha Necco, Director of Human Resources Operations at (781) 795-7199 or mnecco@care.com.

Very truly yours,



Al Zink
SVP Human Resources
Care.com

Information about Identity Theft Prevention

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax: P.O. Box 740241, Atlanta, GA 30374-0241, 1-800-685-1111, www.equifax.com
Experian: P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com
TransUnion: P.O. Box 1000, Chester, PA 19022, 1-800-888-4213, www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

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

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General, Consumer Protection Division
200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us

For residents of Massachusetts: You also have the right to obtain a police report.

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division
9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

Fraud Alerts: There are also two types of fraud alerts that 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 at least 90 days. 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 calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax: 1-888-766-0008, www.equifax.com
Experian: 1-888-397-3742, www.experian.com
TransUnion: 1-800-680-7289, fraud.transunion.com

Credit Freezes (for Non-Massachusetts Residents): You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit 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 credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. If you believe a credit freeze is appropriate under your circumstances, with appropriate documentation and for a period of 24 months from the date of this notice, Care.com will reimburse affected individuals up to an aggregate of $10 of the cost of placing, temporarily lifting and/or removing a credit freeze. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax: P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian: P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion LLC: P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

Credit Freezes (for Massachusetts Residents): Massachusetts law gives you the right to place a security freeze on your consumer reports. A security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. Using a security freeze, however, may delay your ability to obtain credit. You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below:

Equifax: P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian: P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion LLC: P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent). 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. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail. If you believe a credit freeze is appropriate under your circumstances, with appropriate documentation and for a period of 24 months from the date of this notice, Care.com will reimburse affected individuals up to an aggregate of $10 of the cost of placing, temporarily lifting and/or removing a credit freeze.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) 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, you must call or send a written request to the credit reporting agencies by mail 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 as well as the identities 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 three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail 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 three (3) business days after receiving your request to remove the security freeze.

Contact the IRS: You may also want to contact the IRS Identity Theft toll free line at 1-800-908-4490 or file IRS Form 14039 ("Identity Theft Affidavit") to inform the IRS that your information was disclosed. You can find additional information and recommendations at https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft.

AllClear Secure Terms of Use

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- Twenty-four (24) months of coverage with no enrollment required;
- No cost to you – ever. AllClear Secure is paid for by the participating Company.

Services Provided
If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services ("Services") to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Secure is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

Coverage Period
Service is automatically available to you with no enrollment required for twenty-four (24) months from the date of the breach incident notification you received from Company (the "Coverage Period"). Fraud Events that occurred prior to your Coverage Period are not covered by AllClear Secure services.

Eligibility Requirements
To be eligible for Services under AllClear Secure coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident eighteen (18) years of age or older, and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

How to File a Claim
If you become a victim of fraud covered by the AllClear Secure services, you must:

- Notify AllClear ID by calling 1.855.434.8077 to report the fraud prior to expiration of your Coverage Period.
- Provide proof of eligibility for AllClear Secure by providing the redemption code on the notification letter you received from the sponsor Company.
- Fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require;
- Fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft;

Coverage under AllClear Secure Does Not Apply to the Following:
Any expense, damage or loss:

- Due to
  - Any transactions on your financial accounts made by authorized users, even if acting without your knowledge
  - Any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your "Misrepresentation")
- Incurred by you from an Event that did not occur during your coverage period;
- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Secure coverage period.

Other Exclusions:

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity;
- AllClear ID is not an insurance company, and AllClear Secure is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur; and
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud;
- AllClear ID reserves the right to reasonably investigate any asserted claim to determine its validity. All recipients of Secure coverage are expected to protect their personal information in a reasonable way at all times. Accordingly, recipients will not deliberately or recklessly disclose or publish their Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information.

Opt-out Policy

If for any reason you wish to have your information removed from the eligibility database for AllClear Secure, please contact AllClear ID:

E-mail	**Mail**	**Phone**
support@allclearid.com	AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701	1.855.434.8077