NELSON MULLINS

NELSON MULLINS RILEY & SCARBOROUGH LLP
ATTORNEYS AND COUNSELORS AT LAW

Lynda R. Jensen
T 617.217.4639
lynda.jensen@nelsonmullins.com

One Post Office Square, 30th Floor
Boston, MA 02109
T 617.217.4700 F 617.217.4710
nelsonmullins.com

May 8, 2019

Via U.S. Mail Certified Return Receipt and E-mail

Gordon J. MacDonald, Attorney General
Office of the Attorney General
33 Capitol Street
Concord, NH 03301
E-mail: attorney.general@doj.nh.gov

Re: Data Security Incident Notification

Dear Attorney General:

I am writing to inform you of a data security incident that may affect two (2) New Hampshire residents, as detailed below. Our client, Care.com, Inc. ("Care.com"), 77 Fourth Ave., 5th Floor, Waltham MA 02451, which serves as an online marketplace for persons seeking services with care providers, will be sending the residents the attached written notices with an offer to enroll in a 12-month Equifax credit monitoring product at no cost.

On January 28, 2019, Care.com became aware that it was the victim of a single e-mail account compromise by unauthorized user(s). Specifically, its team was informed of an unauthorized e-mail campaign involving an employee's e-mail account, which was quickly isolated and locked down by its IT team.

As a result of this incident, Care.com engaged an industry-leading forensic investigation cybersecurity firm to investigate the nature and circumstances of the compromise. The investigation revealed that unauthorized user(s) gained access to the subject e-mail account between January 26 and 28, 2019. Based upon the type of Internet connection protocol utilized by the unauthorized user(s), it is possible the unauthorized user(s) were capable of accessing and acquiring the entire contents of the e-mail account, although Care.com has no evidence that this occurred.

Due to the forensic investigation firm's findings, Care.com retained an additional forensic firm to review all available data within the e-mail account, which, after addition of contact information, was completed on April 8, 2019, and revealed some e-mails and attachments contained personally identifiable information. With respect to the two New Hampshire residents, the personal information was either a first and last name in conjunction with a Social Security

number, or both Social Security and other government identification numbers. While we have no knowledge that any personally identifiable information was accessed or acquired by an unauthorized individual, Care.com has decided to provide notice proactively to ensure any potentially impacted consumers can protect themselves. A copy of the May 8, 2019, notices are enclosed with this letter.

Please let me know if you have any additional questions regarding the notification.

Very truly yours,

 for

Lynda R. Jensen

Enclosure: Consumer Notice Letters

Return Mail Processing Center
P.O. Box 9349
Dublin, OH 43017

<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

May 8, 2019

NOTICE OF DATA BREACH

Dear <<Name 1>>:

Care.com, Inc. respects the privacy of your information, which is why we are writing to tell you about a data security incident that may have exposed some of your personal information. We take the protection and proper use of your information very seriously. For this reason, we are contacting you directly to explain the circumstances of the data security incident.

What Happened

On January 28, 2019, we became aware that we were the victim of a single e-mail account compromise by unauthorized user(s). Specifically, our team was informed of an unauthorized e-mail campaign involving an employee's e-mail account, which was quickly isolated and locked down by our IT team.

As a result of this incident, we engaged an industry-leading forensic investigation cybersecurity firm to investigate the nature and circumstances of the compromise. The investigation revealed that unauthorized user(s) gained access to the subject e-mail account between January 26 and 28, 2019. Based upon the type of Internet connection protocol utilized by the unauthorized user(s), it is possible the unauthorized user(s) were capable of accessing and acquiring the entire contents of the e-mail account, although we have no evidence that this occurred.

Due to the forensic investigation firm's findings, we retained an additional forensic firm to review all available data within the e-mail account, which, after addition of contact information, was completed on April 8, 2019, and revealed some e-mails and attachments contained personally identifiable information. While we have no knowledge that any of your personally identifiable information was accessed or acquired by an unauthorized individual, we have decided to provide notice to you proactively to ensure you can protect yourself.

What Information Was Involved

As a result of this security incident, an unauthorized individual may have accessed or acquired some of your personal information, which may have included your first and last name and Social Security number.

We are notifying you so you can take appropriate steps to protect your personally identifiable information.

What We Are Doing

To help relieve concerns following this incident, we have secured Equifax to provide identity monitoring at no cost to you for one year. Equifax, as a credit bureau with over a billion updates to data sets daily, functions as a first point of contact

for credit related issues, which allows it to efficiently furnish timely notification to individuals enrolled in its identity monitoring product.

Visit www.myservices.equifax.com/gold to activate and take advantage of your identity monitoring product.

You have until July 31, 2019 to activate your identity monitoring product.

Equifax Credit Watch Gold Activation Code Number: <*INSERT ACTIVATION CODE*>

Additional information describing this product is included with this letter. We encourage you to review the description and to consider enrolling in this product.

What Else Can I Do To Protect My Information

We recommend that you remain vigilant, review your relevant account statements, and monitor your credit reports for suspicious activity. Some state laws advise you to report any suspected identity theft to law enforcement, your state's Attorney General, and the Federal Trade Commission. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report:

Equifax	**Experian**	**TransUnion**
P.O. Box 740241 Atlanta, Georgia 30374 1-800-685-1111 www.equifax.com	P.O. Box 9554 Allen, Texas 75013 1-888-397-3742 www.experian.com	P.O. Box 6790 Fullerton, CA 92834 1-800-680-7289 www.transunion.com

Fraud Alerts: At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. This can be done by contacting the credit bureaus by phone and also via Experian's or Equifax's or Transunion's websites. Once you place a fraud alert at one credit bureau, that bureau is required to notify the other two and have alerts placed on your behalf. Note, however, that because the alert tells creditors to follow certain procedures to protect you, it may also delay your efforts to obtain credit while the agency verifies your identity.

If you wish to place a fraud alert, contact any one of the credit bureaus using the contact information below:

Equifax Fraud Alert	**Experian Fraud Alert**	**TransUnion Fraud Alert**
P.O. Box 105069 Atlanta, GA 30348 1-888-766-0008 www.equifax.com/personal/credit-report-services	P.O. Box 2002 Allen, TX 75013 1-888-397-3742 www.experian.com/fraud/center.html	P.O. Box 2000 Chester, PA 19106 1-800-680-7289 www.transunion.com/fraud-victim-resource/place-fraud-alert

Security Freezes: You have the right to place a security freeze on your credit report. A security freeze is intended to prohibit a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail in order for the freeze to be effective. In order to request a security freeze, you will need to provide the following information: (1) full name (including middle initial and any suffixes); (2) Social Security number; (3) date of birth; (4) current address and previous addresses for the past five years; (5) proof of current address, such as a current utility bill, bank statement, or insurance statement; (6) a legible photocopy of a government issued identification card (state driver's license, military identification, etc.); (7) Social Security Card, pay stub, or W2; and (8) any applicable incident report or complaint with a law enforcement agency. If you have been a victim

of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $5.00 each to place, temporarily lift, or permanently remove a security freeze.

You may obtain a security freeze from each of the three credit bureaus by written request, through the telephone, or by accessing their websites, using the contact information below:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
P.O. Box 105788 Atlanta, GA 30348 1-800-349-9960 www.equifax.com/personal/credit-report-services	P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	P.O. Box 160 Woodlyn, PA 19094 1-888-909-8872 www.transunion.com/credit-freeze

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based upon the method of your request. 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. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must make a request to each of the credit reporting agencies by mail, through their websites, or by phone (using the contact information above). You must provide proper identification (including 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. You may also temporarily lift a security freeze for a specified period of time rather than for a specific entity or individual, using the same contact information above. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for requests made by mail) 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 make a request to each of the credit reporting agencies by mail, through their websites, or by phone (using the contact information above). You must provide 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 between one (1) hour (for requests made online) and three (3) business days (for requests made by mail) after receiving your request to remove the security freeze.

You may wish to review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit www.identitytheft.gov or call 1-877-ID-THEFT (877-438-4338). IdentityTheft.gov is the federal government's one-stop resource for identity theft victims. The site provides streamlined checklists and sample letters to guide you through the recovery process.

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 the Attorney General's office in your state. You can also obtain information from these sources about additional methods to prevent identity theft, and you can obtain information from the Federal Trade Commission and the consumer reporting agencies for more information regarding fraud alerts and security freezes. Contact information for the Federal Trade Commission is as follows:

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

For California residents: If you have been the victim of identity theft or believe your personal or financial information may have been compromised, you may contact the Attorney General to enroll in the identity theft registry by calling the Identity Theft Hotline 1-888-880-0240, or visit https://oag.ca.gov/idtheft/criminal.

For Colorado residents: If you have been the victim of identity theft or believe your personal or financial information may have been compromised, you may contact the Attorney General by calling 1-855-443-3489, or visit https://www.stopfraudcolorado.gov/fraud-center/identity-theft.html.

For Missouri residents: If you have been the victim of identity theft or believe your personal or financial information may have been compromised, you may contact the Attorney General by calling 1-800-392-8222, or visit https://ago.mo.gov/civil-division/consumer/identity-theft-data-security/data-breaches.

For New Hampshire residents: If you have been the victim of identity theft or believe your personal or financial information may have been compromised, you may contact the Attorney General by calling 1-888-468-4454, or visit https://www.doj.nh.gov/consumer/identity-theft/index.htm.

For New Jersey residents: If you have been the victim of identity theft or believe your personal or financial information may have been compromised, you may contact the New Jersey Cybersecurity & Communications Integration Cell by calling 1-609-963-6900 ext. 7865, or visit https://www.cyber.nj.gov/contact.

For Ohio residents: If you have been the victim of identity theft or believe your personal or financial information may have been compromised, you may contact the Attorney General by calling 1-800-282-0515, or visit www.ohioattorneygeneral.gov.

For Texas residents: If you have been the victim of identity theft or believe your personal or financial information may have been compromised, you may visit the Attorney General's website for assistance at https://www2.texasattorneygeneral.gov/identitytheft/if-you-become-a-victim.

For Vermont residents: If you have been the victim of identity theft or believe your personal or financial information may have been compromised, you may contact the Attorney General by calling 1-800-649-2424, or visit https://ago.vermont.gov/consumer-information/.

For More Information

For further information, please call (855) 821-6784. We take the protection of your personal information very seriously and apologize for any inconvenience.

Sincerely,

David Krupinski
Chief Safety & Cybersecurity Officer

Return Mail Processing Center
P.O. Box 9349
Dublin, OH 43017

<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

May 8, 2019

NOTICE OF DATA BREACH

Dear <<Name 1>>:

Care.com, Inc. respects the privacy of your information, which is why we are writing to tell you about a data security incident that may have exposed some of your personal information. We take the protection and proper use of your information very seriously. For this reason, we are contacting you directly to explain the circumstances of the data security incident.

What Happened

On January 28, 2019, we became aware that we were the victim of a single e-mail account compromise by unauthorized user(s). Specifically, our team was informed of an unauthorized e-mail campaign involving an employee's e-mail account, which was quickly isolated and locked down by our IT team.

As a result of this incident, we engaged an industry-leading forensic investigation cybersecurity firm to investigate the nature and circumstances of the compromise. The investigation revealed that unauthorized user(s) gained access to the subject e-mail account between January 26 and 28, 2019. Based upon the type of Internet connection protocol utilized by the unauthorized user(s), it is possible the unauthorized user(s) were capable of accessing and acquiring the entire contents of the e-mail account, although we have no evidence that this occurred.

Due to the forensic investigation firm's findings, we retained an additional forensic firm to review all available data within the e-mail account, which, after addition of contact information, was completed on April 8, 2019, and revealed some e-mails and attachments contained personally identifiable information. While we have no knowledge that any of your personally identifiable information was accessed or acquired by an unauthorized individual, we have decided to provide notice to you proactively to ensure you can protect yourself.

What Information Was Involved

As a result of this security incident, an unauthorized individual may have accessed or acquired some of your personal information, which may have included your first and last name and Social Security and other government identification number.

We are notifying you so you can take appropriate steps to protect your personally identifiable information. The information that may have been acquired varies by individual and this letter is intended to communicate the types of information that may have been acquired by unauthorized individual(s).

What We Are Doing

To help relieve concerns following this incident, we have secured Equifax to provide identity monitoring at no cost to you for one year. Equifax, as a credit bureau with over a billion updates to data sets daily, functions as a first point of contact for credit related issues, which allows it to efficiently furnish timely notification to individuals enrolled in its identity monitoring product.

Visit www.myservices.equifax.com/gold to activate and take advantage of your identity monitoring product.

You have until July 31, 2019 to activate your identity monitoring product.

Equifax Credit Watch Gold Activation Code Number: <*INSERT ACTIVATION CODE*>

Additional information describing this product is included with this letter. We encourage you to review the description and to consider enrolling in this product.

What Else Can I Do To Protect My Information

We recommend that you remain vigilant, review your relevant account statements, and monitor your credit reports for suspicious activity. Some state laws advise you to report any suspected identity theft to law enforcement, your state's Attorney General, and the Federal Trade Commission. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report:

Equifax	**Experian**	**TransUnion**
P.O. Box 740241 Atlanta, Georgia 30374 1-800-685-1111 www.equifax.com	P.O. Box 9554 Allen, Texas 75013 1-888-397-3742 www.experian.com	P.O. Box 6790 Fullerton, CA 92834 1-800-680-7289 www.transunion.com

Fraud Alerts: At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. This can be done by contacting the credit bureaus by phone and also via Experian's or Equifax's or Transunion's websites. Once you place a fraud alert at one credit bureau, that bureau is required to notify the other two and have alerts placed on your behalf. Note, however, that because the alert tells creditors to follow certain procedures to protect you, it may also delay your efforts to obtain credit while the agency verifies your identity.

If you wish to place a fraud alert, contact any one of the credit bureaus using the contact information below:

Equifax Fraud Alert	**Experian Fraud Alert**	**TransUnion Fraud Alert**
P.O. Box 105069 Atlanta, GA 30348 1-888-766-0008 www.equifax.com/personal/credit-report-services	P.O. Box 2002 Allen, TX 75013 1-888-397-3742 www.experian.com/fraud/center.html	P.O. Box 2000 Chester, PA 19106 1-800-680-7289 www.transunion.com/fraud-victim-resource/place-fraud-alert

Security Freezes: You have the right to place a security freeze on your credit report. A security freeze is intended to prohibit a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail in order for the freeze to be effective. In order to request a security freeze, you will need to provide the following information: (1) full name (including middle initial and any suffixes); (2) Social Security number; (3) date of birth; (4) current address and previous addresses for the past five years; (5) proof of current address, such as a current utility bill, bank statement, or insurance statement; (6) a legible photocopy of

a government issued identification card (state driver's license, military identification, etc.); (7) Social Security Card, pay stub, or W2; and (8) any applicable incident report or complaint with a law enforcement agency. If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $5.00 each to place, temporarily lift, or permanently remove a security freeze.

You may obtain a security freeze from each of the three credit bureaus by written request, through the telephone, or by accessing their websites, using the contact information below:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
P.O. Box 105788 Atlanta, GA 30348 1-800-349-9960 www.equifax.com/personal/credit-report-services	P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	P.O. Box 160 Woodlyn, PA 19094 1-888-909-8872 www.transunion.com/credit-freeze

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based upon the method of your request. 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. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must make a request to each of the credit reporting agencies by mail, through their websites, or by phone (using the contact information above). You must provide proper identification (including 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. You may also temporarily lift a security freeze for a specified period of time rather than for a specific entity or individual, using the same contact information above. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for requests made by mail) 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 make a request to each of the credit reporting agencies by mail, through their websites, or by phone (using the contact information above). You must provide 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 between one (1) hour (for requests made online) and three (3) business days (for requests made by mail) after receiving your request to remove the security freeze.

You may wish to review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit www.identitytheft.gov or call 1-877-ID-THEFT (877-438-4338). IdentityTheft.gov is the federal government's one-stop resource for identity theft victims. The site provides streamlined checklists and sample letters to guide you through the recovery process.

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 the Attorney General's office in your state. You can also obtain information from these sources about additional methods to prevent identity theft, and you can obtain information from the Federal Trade Commission and the consumer reporting agencies for more information regarding fraud alerts and security freezes. Contact information for the Federal Trade Commission is as follows:

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

For Illinois residents: If you have been the victim of identity theft or believe your personal or financial information may have been compromised, please call the toll-free Identity Theft Hotline at: 1-866-999-5630 or 1-877-844-5461 (TTY), or visit http://illinoisattorneygeneral.gov/consumers/hotline.html.

For New Hampshire residents: If you have been the victim of identity theft or believe your personal or financial information may have been compromised, you may contact the Attorney General by calling 1-888-468-4454, or visit https://www.doj.nh.gov/consumer/identity-theft/index.htm.

For Wisconsin residents: If you have been the victim of identity theft or believe your personal or financial information may have been compromised, you may contact the Attorney General by calling 1-800-422-7128, or visit datcp.wi.gov.

For More Information

For further information, please call (855) 821-6784. We take the protection of your personal information very seriously and apologize for any inconvenience.

Sincerely,

David Krupinski
Chief Safety & Cybersecurity Officer