McDermott
Will&Emery

Boston Brussels Chicago Düsseldorf Houston London Los Angeles Miami Milan
Munich New York Orange County Rome San Diego Silicon Valley Washington, D.C.
Strategic alliance with MWE China Law Offices (Shanghai)

Daniel F. Gottlieb
Attorney at Law
dgottlieb@mwe.com
+1 312 984 6471

December 10, 2012

VIA FEDERAL EXPRESS

New Hampshire Department of Justice
33 Capitol Street
Concord, New Hampshire 03301

Re: Report of Potential Security Breach

Dear Sir/Madam:

We are writing on behalf of our client, CCS Medical, Inc., a Delaware corporation ("CCS Medical"), to report a potential security breach of personal information maintained by CCS Medical. CCS Medical is providing this report to the New Hampshire Department of Justice pursuant to New Hampshire statutes governing security breach notification. We also enclose a copy of the form of notice that CCS Medical is sending to individuals who are New Hampshire residents that could be affected by the potential breach.

On September 20, 2012, a CCS Medical employee reported that another employee may have accessed, recorded and disclosed Social Security Numbers and other personal information in order to submit false tax returns to the IRS and collect fraudulent tax refunds. CCS Medical immediately initiated an internal investigation of the alleged wrongful access and disclosure, suspended the suspected employee and promptly reported the allegations to the U.S. Department of Justice and the Internal Revenue Service (IRS). On October 17, 2012, following discussions with the IRS, CCS Medical determined that the employee *potentially* engaged in the alleged wrongful access and disclosure. However, CCS Medical's investigation is ongoing and CCS Medical has not definitively determined that the wrongful access and disclosure in fact occurred. Out of an abundance of caution and in the interest of protecting our customers, CCS Medical terminated the suspected employee and is notifying customers who may have been affected by the alleged wrongful access and disclosure.

In addition to reporting the alleged misconduct to the U.S. Department of Justice and the IRS, CCS Medical has filed a police report regarding the potential misuse of personal information and tax fraud with the Pinellas County, Florida Sheriff's Department and are reporting the incident to the Office of Civil Rights of the U.S. Department of Health and Human Services and other state authorities in accordance with state and federal law.

In response to the potential unauthorized disclosure, CCS Medical has provided additional mandatory privacy training to all of its employees and made modifications to its customer

service information systems to reduce the risks of misuse of personal information. CCS Medical reviews its security practices on an ongoing basis to identify additional safeguards for its customer service information systems

On December 7, 2012, CCS Medical sent the enclosed security breach notice letter to a total of 23 affected New Hampshire residents. CCS Medical's notice letter advises the individuals to remain vigilant and consider taking the following steps to avoid identity theft: (1) place a fraud alert on their credit files; (2) review their credit reports; (3) monitor their financial and other accounts; and (4) place a security freeze on their credit files. The letter directs individuals to other resources for further information and describes actions to take if an individual suspects that his or her information is being misused. The letter provides a toll-free phone number for individuals with questions about the incident.

CCS Medical takes protection of the privacy and security of personal information in its possession very seriously. If you have any questions regarding the potential security breach, please do not hesitate to contact me.

Sincerely,

Daniel Gottlieb

Daniel F. Gottlieb

Enclosure

cc: W. Bradley Bickham
Monica Raines

CCS MEDICAL
Processing Center • PO Box 3825 • Suwanee, GA 30024

Clear

Free Identity Protection
Redemption Code: 9999999999
Enroll at enroll.allclearid.com
Assistance Hotline: 877-615-3792

December 7, 2012

John Q Sample
123 Main Street
Anytown, US 12345-6789

Dear John Q Sample,

We are writing to inform you that there may have been an unauthorized disclosure of your personal information that we maintained between May 1, 2012, and September 21, 2012. Although we are not aware of any confirmed identity theft or other misuse of your information, out of an abundance of caution we are notifying you of the potential disclosure so that you can take steps to protect yourself from any misuse of your personal information. The potential disclosure is further described below.

CCS Medical takes protection of the privacy and security of your personal information very seriously. We regret that an unauthorized disclosure may have occurred and apologize for any inconvenience and concern that it causes you.

Description of the Incident and CCS Medical's Response

A CCS Medical employee reported that another employee may have accessed, recorded and disclosed Social Security Numbers and other personal information about CCS Medical customers in order to submit false tax returns to the IRS and collect fraudulent tax refunds in the customer's name. CCS Medical immediately initiated an internal investigation of the alleged wrongful access and disclosure, suspended the suspected employee and promptly reported the allegations to the U.S. Department of Justice and the Internal Revenue Service (IRS). On October 17, 2012, following discussions with the IRS, we determined that the employee *potentially* engaged in the alleged wrongful access and disclosure. However, CCS Medical's investigation is ongoing and we have not definitively determined that the wrongful access and disclosure in fact occurred. Out of an abundance of caution and in the interest of protecting our customers, CCS Medical terminated the suspected employee and is notifying customers who may have been affected by the alleged wrongful access and disclosure.

In addition to reporting the alleged misconduct to the U.S. Department of Justice and the IRS, we have filed a police report regarding the potential misuse of personal information and tax fraud with the Pinellas County Sheriff's Department and are reporting the incident to the Office of Civil Rights of the U.S. Department of Health and Human Services and state authorities in Louisiana, Maine, Maryland, Massachusetts, New Hampshire, New Jersey and New York in accordance with state and federal law. You have the right to obtain a copy of the police report filed with the Sheriff's Department once the Sheriff's Department completes the investigation. If you are the victim of identity theft, you also have the right to file your own police report and obtain a copy of it.

In response to the potential unauthorized disclosure, CCS Medical has provided additional mandatory privacy training to all of its employees and made modifications to its customer service information systems to reduce the risks of misuse of personal information. CCS Medical reviews its security practices on an ongoing basis to identify additional safeguards for its customer service information systems.

Personal Information Involved

Although we have been unable to confirm whether the alleged misuse of your personal information actually occurred, the employee alleged to be involved in the fraud had access to the following types of information about you in CCS Medical's customer service systems: your name; address and phone number; Social Security Number; date of birth; Medicare or other health plan identification number; secondary insurance information; and information about CCS Medical products and services that you have received.

What Steps Can You Take to Protect Yourself?

We want to make you aware of steps you may take to guard against identity theft or fraud. Please review the enclosed information about identity theft protection.

To help safeguard you from misuse of your personal information, we have arranged for you to receive identity protection from AllClear ID at no cost to you. AllClear ID offers credit monitoring services that deliver secure, actionable credit alerts to you by phone. AllClear ID Protection also includes $1,000,000.00 Identity Theft Insurance Coverage and AllClear ID Fraud Resolution Services. The AllClear ID service will be valid for one year from the date you register.

You must register with AllClear ID to receive this complimentary identity protection service. You will need to provide the redemption code that is listed at the top of the first page. You may register online at https://enroll.allclearid.com or by phone by calling 877-615-3792. Please note that additional action after registration may be required by you in order to activate certain features of the service. Please see the enclosure to learn more about AllClear ID.

If you have any questions, please contact one of our customer service representatives at 877-615-3792 between Monday through Saturday from 8:00am to 8:00pm Central Time. If you receive a busy signal due to high call volume, please call back. If you are able to leave a voice mail, we will return your call promptly. If you prefer, you can contact CCS Medical at our mailing address: CCS Medical, Attn: Privacy Officer, 1505 LBJ Freeway, Suite 600, Farmers Branch, TX 75234.

CCS Medical is committed to protecting your privacy and to maintaining a relationship based on trust and excellent customer service. We apologize for any inconvenience that this may have caused you and we hope that the steps outlined in this letter will alleviate any concerns.

Very truly yours,

Monica Raines

Monica Raines
CCS Medical
Compliance and Privacy Officer

Information about Identity Theft Prevention

Although we are not aware of any instances of identity theft or other misuse of your personal information, we advise you to remain vigilant and consider taking the following steps:

What Steps Can You Take to protect Yourself?

- *Order a Copy of Your Credit Reports.* We highly recommend that you periodically obtain your credit report from one or more of the national credit reporting bureaus. 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 contact the three national credit reporting bureaus directly at the toll-free numbers below to order a free credit report once per year.

  Equifax, P.O. Box 740241, Atlanta, Georgia 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 6790, Fullerton, CA 92834-6790, 1-800-916-8800, www.transunion.com

  You should review credit reports carefully for any sign of fraud, such as unfamiliar accounts or credit inquires, debts that you cannot explain, medical debt collection notices from health care providers, or other unusual activity that you did not initiate or do not recognize. Even if you do not find any suspicious activity on your credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports regularly. Identity thieves sometimes hold victims' information for a period of time before using it or sharing it among a group of thieves at different times. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

- *Read the Explanation of Benefits (EOB) Statements From Medicare and other Insurers.* Read the EOBs that you receive from your insurers. Make sure the health care claims to your insurers match the items and services that you received. Look for the name of the provider, the date of service and the service provided. If there is a discrepancy, contact your insurer immediately to report the problem.

- *Request Medical Records.* You may also want to request a copy of your medical records from your health care providers or billing records from Medicare or other insurers to identify any health care items or services that were not provided to you. If you are a California resident, we suggest that you visit the web site of the California Office of Privacy Protection at www.privacy.ca.gov to find more information about your medical privacy.

- *Monitor Your Medical, Financial and other Accounts.* We recommend that you closely monitor your account statements from CCS Medical, other health care providers and suppliers, financial institutions and other account holders and, if you notice any unauthorized activity, promptly contact the account holder.

- *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 above.

- *Credit Freezes*. You may have the right to put a credit freeze, also known as a security freeze, on your credit file. A credit freeze, which is different than a fraud alert, prevents new credit from being 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 creditors 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. Consequently, 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. 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. Information for Massachusetts residents is included at the end of this letter.

  Equifax, P.O. Box 105788, Atlanta, GA 30348, www.equifax.com

  Experian, P.O. Box 9554, Allen, TX 75013, www.experian.com

  TransUnion, Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790, www.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.

What if You Find Evidence of Identity Theft or Other Suspicious Activity?

We recommend that you promptly report any suspicious activity or suspected identity theft to CoaguChek and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the 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 Maryland residents. 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 North Carolina residents. You may also obtain information about preventing and avoiding identity theft from 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

Security Freeze Attachment for Massachusetts Residents

Massachusetts law also allows consumers to place a security freeze on their credit reports. A security freeze prohibits 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.

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.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com) by regular, certified or overnight mail at the addresses below:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348	Experian Security Freeze P.O. Box 9554 Allen, TX 75013	TransUnion Security Freeze Fraud Victim Assistance Department P.O. Box 6790 Fullerton, CA 92834

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 (5) 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;
8. 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.

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.