KCI Health Care Compliance (HCC)
6103 Farinon Drive
San Antonio, TX 78249

December 21, 2010

New Hampshire Attorney General
Michael A. Delaney
33 Capitol Street
Concord, NH 03301

Dear Mr. Delaney:

In accordance with N.H. Rev. Stat. Ann. § 359-C:20, I am writing to provide you with notification regarding the nature and circumstances of a recent data security incident.

We recently became aware of an incident involving the possible compromise of payment card information of certain KCI USA, Inc. ("KCI") customers. At this time we believe that payment card information of several KCI customers may have been used by an individual who previously worked in our call center to make unauthorized purchases. While working at our call center, the individual had authorized access as part of the individual's job responsibilities, to a database that contained KCI customers' personal information, including customer name, address, date of birth, insurance information and, in some instances, payment card information and Social Security number. While we believe the individual may have misused payment card information of several KCI customers, we have no reason to suspect at this time that the individual used other sensitive personal information in an unauthorized manner. The individual has been terminated and we are working with law enforcement authorities on this matter. In addition, when we discovered this incident, our supervisors reminded call center personnel of their existing information security obligations.

Approximately 2 persons who may be affected by this incident reside in New Hampshire.

Attached for your reference is a copy of the notice KCI sent to affected individuals on December 21, 2010. If you have any questions, please do not hesitate to contact me at

Very truly yours,

Nancy M. Scheifele
Vice President Global Health Care Compliance

Enclosure

KCI Health Care Compliance (HCC)
6103 Farinon Drive
San Antonio, TX 78249

December 21, 2010

«First_and_Last_Name»
«Patient_Address_1»
«Patient_City», «Patient_State» «Patient_Zip»

Dear Valued KCI Customer:

We recently became aware of an incident involving the possible compromise of payment card information of certain KCI USA, Inc. ("KCI") customers. At this time we believe that payment card information of several KCI customers may have been used by an individual who previously worked in our call center to make unauthorized purchases in the San Antonio area. While working at our call center, the individual had authorized access, as part of that individual's job responsibilities, to a database that contained KCI customers' personal information, including customer name, address, date of birth, insurance information and, in some instances, payment card information and Social Security number. We take our obligation to safeguard our customers' personal information very seriously. We are notifying KCI customers whose personal information included payment card information and whose accounts were accessed by this individual while working in KCI's call center. While we believe the individual may have misused payment card information of several KCI customers, we have no reason to suspect at this time that the individual used other sensitive personal information in an unauthorized manner. The individual has been terminated and we are working with law enforcement authorities on this matter.

We encourage you to remain vigilant and to carefully review and monitor your account statements, as well as your credit reports. If you believe your payment card was affected, we recommend that you immediately contact your payment card company and KCI.

Furthermore, although we do not suspect at this time that other personal information has been misused, as a reminder, you are entitled under U.S. law to one free credit report annually from each of the three national credit bureaus. To order your free credit report, call toll-free at (877) 322-8228 or visit www.annualcreditreport.com. The Reference Guide below provides details on these and other steps you may wish to consider, including recommendations by the U.S. Federal Trade Commission on how to further protect your personal information.

If you have any questions or would like additional information about this situation, please call our KCI Compliance Hotline at (866) 290-8605 toll-free, Monday through Friday, between 9 a.m. CST and 4:30 p.m. CST.

We sincerely regret any inconvenience this may cause you.

Sincerely,

Nancy M. Scheifele
Vice President Global Health Care Compliance

Reference Guide

We encourage individuals receiving KCI USA, Inc.'s letter dated December 21, 2010, to consider the following steps, in addition to remaining vigilant in reviewing and monitoring your payment card information:

Order Your Free Credit Reports. To order your free credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three national credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store or commercial names. The credit bureau will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing.

If you find items you don't understand on your report, call the credit bureau at the number given on the report. Credit bureau staff will review your report with you. If the information can't be explained, then you will need to call the creditors involved. Information that can't be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Contact the U.S. Federal Trade Commission. If you detect any unauthorized transactions in your financial account, promptly notify your payment card company or financial institution.

In addition, if you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authority, your state Attorney General and the FTC. If you believe your identity has been stolen, the FTC recommends that you take these additional steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit (available at www.ftc.gov/idtheft) when you dispute new unauthorized accounts.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft:

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

Place a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free fraud numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three credit bureaus.

Equifax	P.O. Box 740241 Atlanta, Georgia 30374-0241	877-478-7625	www.equifax.com
Experian	P.O. Box 9532 Allen, Texas 75013	888-397-3742	www.experian.com
TransUnion	Fraud Victim Assistance Division P.O. Box 6790 Fullerton, California 92834-6790	800-680-7289	www.transunion.com

For Maryland Residents. You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You can contact the Maryland Attorney General at:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
888-743-0023 (toll-free in Maryland)
410-576-6300
www.oag.state.md.us

For North Carolina Residents. You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at:

North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
877-566-7226 (toll-free in North Carolina)
919-716-6400
www.ncdoj.gov