**Jeanne K. Mason, Ph.D.**
Corporate Vice President
Human Resources

Baxter International Inc.
One Baxter Parkway
Deerfield, Illinois 60015-4633

847.948.3525
Fax: 847.948.3446
jeanne_mason@baxter.com
www.baxter.com

**Baxter**

July 11, 2008

Department of Justice
Attn: New Hampshire Attorney General
33 Capital Street
Concord, New Hampshire 03301

Re: Recent Unauthorized Disclosure of Personal Information

Ladies and Gentlemen:

We write to provide you notice pursuant to the New Hampshire Act Regulating Identity Theft, N.H. Rev. Stat. §§ 359-C: 19 *et seq.*

Recently, a Baxter human resources employee based in the U.S. was attending a human resources conference in Chicago, Illinois. On June 24, 2008, a thief entered the hotel room of the employee while that employee was attending the conference, and stole a laptop computer belonging to Baxter. Subsequently, we learned that two data files on the laptop contained personal information, including names, social security numbers, encoded information regarding background checks, and addresses of certain current, former, and prospective U.S. employees. No customer or patient data was included in these data files. The data files included personal information of roughly 6,900 people, of which 2 reside in New Hampshire. Baxter has notified and is working closely with local law enforcement officials to investigate this matter. Additionally, we are developing policies and procedures to strengthen our data security policies to reduce, if not eliminate, the risk that data losses of this type ever occur again.

We are notifying our employees whose information may have been or may be compromised of this incident on Monday, July 14th by writing to them at their last known addresses. By such communication, a sample of which is attached hereto as Exhibit A, we informed our employees of: (i) the details of this security incident; (ii) the actions we are taking to help them monitor their accounts for any unusual activity; (iii) a toll-free number they can call with inquiries; and (iv) steps they can take to protect against identity theft (including specific guidance on monitoring their credit reports).

We thank you for your time and consideration of this matter. If you have any questions, please contact Jacob Springer; Corporate Counsel, Data Privacy at 847-948-4806.

Sincerely,

Jeanne Mason

EXH. A

Baxter

Secure Processing Center | 600 Satellite Blvd | Suwanee, GA 30024

Urgent Message from Baxter. Please Open Immediately.

<FirstName> <MiddleInitial> <LastName> <Suffix>
<Address> (Line 1)
<Address> (Line 2)
<City> <State> <Zip>
<POSTNET BARCODE>

**RE: Important Information Regarding the Security of Your Personal Information**

Dear <FirstName> <MiddleInitial> <LastName> <Suffix>,

I am writing to inform you of a recent situation that may affect you. We have discovered that, as a result of a data loss incident, some of your personal information may have become exposed. I want to assure you that we are taking this incident seriously and taking steps to ensure that all of our data is as secure as possible. We deeply regret that this incident occurred.

**WHAT HAPPENED?**

On June 24, 2008, a Baxter human resources employee based in the U.S. was attending a conference in Chicago, Illinois. A thief entered the hotel room of the employee and stole a laptop computer belonging to Baxter. Subsequently, we learned that two data files that were created for ongoing projects were stored on the laptop. These data files contained personal information, including names, social security numbers, encoded information regarding background checks, and addresses of roughly 6900 primarily U.S.-based current and former employees and applicants. Your personal information was included in one of these files.

On behalf of the entire Baxter organization and our dedicated human resources staff, I want to express our deepest regret for this unfortunate incident and let you know that we are doing everything we can to address the situation and assist you, as further detailed below.

**WHAT ARE THE RISKS OF THIS INFORMATION BEING ACCESSED AND MISUSED?**

We do not know that this information has been accessed and misused. The stolen laptop required a user to enter certain user credentials, such as a correct username and password, in order to access the laptop computer. Hotel security and law enforcement authorities were contacted, and they are undertaking a vigorous investigation to see if they can identify the thief and locate the stolen laptop. However, because the laptop had personal information, we believe it is important to assist you in taking all appropriate measures practicable to reduce the threat of any identity theft or other potentially resulting loss.

**WHAT STEPS IS BAXTER TAKING TO SAFEGUARD YOUR INTERESTS?**

We are committed to safeguarding your personal information, and we have taken immediate steps to assist you in protecting your identity and to fortify security measures that were already in place. Specifically, we have undertaken the following steps:

(1) We are working with law enforcement to assist them in identifying the thief and recovering the stolen laptop. We will keep you informed of any additional information we receive on any access or use of your personal information.

(2) We have retained Kroll Inc., a New-York based risk consulting firm and a global leader in data security, who has worked with other large corporations under similar circumstances, to provide its ID TheftSmart™ safeguards to you at no charge. Through Kroll, we have made the following services available to you:

- Call Center Assistance: With Kroll's assistance, we have established a bilingual support center that is ready to take your questions and provide you with guidance about safeguarding your identity against misuse as a result of this incident. You can reach the call center, toll-free, at 1-800-588-9839, anytime Monday through Friday from 8 a.m. to 5 p.m. central standard time.

- Credit Monitoring Service: At no charge to you, we are providing you with 24-months of credit monitoring services provided through Kroll's ID TheftSmart service. If you choose to take advantage of this two-year membership paid for by Baxter, Kroll will provide you with an initial copy of your credit report through Experian and then will continuously monitor your credit file through all three national reporting agencies for changes in your credit file that could indicate the kind of unauthorized activity commonly associated with identity theft and fraud. In order to activate this service, either fill out and return the enclosed *Consumer Credit Report and Credit Monitoring Authorization Form* or submit an online authorization at www.idintegrity.com. Please be prepared to provide the membership number included with this letter.

- Proactive idINTEGRITY scan: In addition to monitoring of your credit information, we have arranged with Kroll to provide its idINTEGRITY scan, which routinely scans the Internet for unauthorized use of your personal information. If you choose to enroll in this program, you will be notified of any suspicious activity related to your personal information that is uncovered through an active 24/7 online monitoring process. If suspicious or fraudulent activity is discovered, Kroll's Licensed Investigators will be available to assist you. In order to enroll in these services, please visit www.idintegrityscan.com.

- Enhanced Identity Theft Restoration Service: In the event that your personal data is misused as a result of this event, Kroll's experienced Licensed Investigators are available to you at no charge to assist you with comprehensive identity theft restoration services.

ID TheftSmart is one of the most comprehensive programs available to help protect against identity theft. This package contains additional information about Kroll's services and how to enroll, and we urge you to take the time to review the safeguards now available to you.

(3) We have formed an Information Security Assessment Team, which will assess our data security controls and recommend and implement steps to further strengthen those controls to appropriately reduce the risk of significant data loss, including restricting data access and requiring the use of encryption tools.

**WHAT ALTERNATIVE STEPS CAN YOU TAKE TO SAFEGUARD YOUR INTERESTS IF YOU CHOOSE NOT TO ENROLL IN KROLL'S SERVICES?**

Kroll will be taking the precautions described above on your behalf, if you choose to enroll with Kroll. However, in the event that you decide not to enroll in Kroll's services provided at no charge to you, we would urge you to take the following precautions to guard against identity theft:

- Carefully review your financial account statements over the next 12-24 months, and report any unusual or unauthorized account activity to your financial institution.

- In the event that you have been subject to an actual identity theft, please alert the Company to this fact by calling the Human Resources Call Center at 1-877-BAX-HR4U (1-877-229-4748).

- Contact one of the three (3) nationwide credit reporting agencies and notify them that you have been the possible victim of identity theft and request that they place a fraud alert on your credit files. A fraud alert requires creditors to take reasonable steps to verify your identity before issuing credit in your name. You need call only one of the three nationwide credit reporting agencies at one of the numbers listed below and they will automatically place fraud alerts with the other two agencies:

| **Experian** | **Equifax** | **TransUnion** |
|---|---|---|
| www.experian.com | www.equifax.com | www.transunion.com |
| 888-397-3742 | 800-525-6285 | 800-680-7289 |

- When you contact these nationwide credit-reporting agencies, you should also request a free copy of your credit report. When you receive your credit report, look it over carefully. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. And look for personal information, such as home address and Social Security number, which is not accurate. If you see anything you do not understand, call the credit-reporting agency at the telephone number on the report. The Call Center available through Kroll also is available to assist you in reviewing your credit reports and can be reached at 1-800-588-9839.

  If you do find suspicious activity on your credit reports, call your local police or sheriff 's office and file a police report of identity theft. Get a copy of that police report. You may need to give copies of the police report to creditors to clear up your records. Additionally, report the identity theft to your state's attorney general's office and the Federal Trade Commission.

- Visit the Federal Trade Commission's ("FTC") website (www.ftc.gov), which contains a link to useful information concerning identity theft and steps you can take to avoid identity theft. You can also contact the FTC at their toll-free number, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261.

**For residents of Hawaii, Maryland, Massachusetts, Michigan, North Carolina, Oregon, Vermont, West Virginia, and Wyoming only:** Regardless of whether you enroll in Kroll's services or take your own alternative precautionary steps, please refer to the included insert entitled "U.S. State Notification Requirements" for information that we are required to provide you pursuant to the laws of your state.

Please be assured that we take this issue seriously. We sincerely apologize for any inconvenience this may cause you.

Sincerely,

Jeanne K. Mason
Corporate Vice President, Human Resources

**ID TheftSmart™**

<FirstName> <MiddleInitial> <LastName> <Suffix>
Membership Number: <Membership Number>

Member Services: 1-800-588-9839
8:00 a.m. to 5:00 p.m. (Central Time), Monday through Friday
If you have questions or feel you may have an identity theft issue, please call ID TheftSmart member services

**ID TheftSmart™**

<FirstName> <MiddleInitial> <LastName> <Suffix>
Membership Number: <Membership Number>

Member Services: 1-800-588-9839
8:00 a.m. to 5:00 p.m. (Central Time), Monday through Friday
If you have questions or feel you may have an identity theft issue, please call ID TheftSmart member services

Please detach cards and keep in a convenient place for your reference

U.S. State Notification Requirements

**For residents of *Hawaii, Iowa, Maryland, Michigan, North Carolina, Oregon, Vermont, Virginia, West Virginia*, and *Wyoming*:**
It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity. You may obtain a free copy of your credit report by contacting any one or more of the following national consumer reporting agencies:

**Equifax**
P.O. Box 740241
Atlanta, Georgia 30348
1-800-685-111
www.equifax.com

**Experian**
P.O. Box 2104
Allen, TX 75013
1-888-397-3742
www.experian.com

**TransUnion**
P.O. Box 6790
Fullerton, CA 92834-6790
1-877-322-8228
www.transunion.com

**For residents of *Iowa*:**
State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

**For residents of *Oregon*:**
State law advises you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission.

**For residents of *Maryland*:**
You can obtain information from the Maryland Office of the Attorney General and the Federal Trade Commission about steps you can take to avoid identity theft.

**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

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

**For residents of *Massachusetts* and *West Virginia*:**
It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft. You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent; however, using a security freeze may delay your ability to obtain credit.

To place a security freeze on your credit report, you need to send a request to a consumer reporting agency by certified mail, overnight mail, or regular stamped mail. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The consumer reporting agency may charge a fee of up to $5.00 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and you have submitted a valid police report relating to the identity theft incident to the consumer reporting agency.

**Equifax Security Freeze**
P.O. Box 105788
Atlanta, Georgia 30348
www.equifax.com

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

**TransUnion (FVAD)**
P.O. Box 6790
Fullerton, CA 92834-6790
www.transunion.com