McKesson Corporation
One Post Street
San Francisco, CA 94104
415.983.8300 Tel

[redacted]

August 30, 2007

McKESSON
Empowering Healthcare

Via Overnight Mail and Facsimile - (603) 271-2110

Attorney General
Department of Justice
33 Capitol Street
Concord, NH 03301

To Whom It May Concern:

Pursuant to state law requirements, we are writing to notify you of a theft that occurred at McKesson Specialty on July 18, 2007, in which two computers containing personal information were stolen. There were 68,767 individuals whose information was maintained on the computers; 987 of those individuals were residents of New Hampshire. We are beginning the process of notifying those individuals of the security breach. This notification process will started on August 29, 2007 and we expect that all affected persons will be notified by August 30, 2007.

Some of the information that was stored on the computer was encrypted and password protected; however, we cannot confirm that all of the personal information was secured. Accordingly, in an abundance of caution, we are notifying all individuals whose information was stored on the computer by letter sent via first class mail. The specific notice that an affected individual will receive is determined by the Patient Assistance Program (PAP) in which they were/are enrolled or were in the process of enrolling. We have included copies of Letters B, C, D, E, F and H, which are examples of the letters sent to individuals enrolled in the specified PAP. We will send you copies of the remaining LettersA, G, and I as they are finalized and sent.

- Letter A was sent to individuals who were enrolled in AstraZeneca's Medicine & Me.

- Letter B was sent to individuals who were enrolled in Axcan's CareFirst for CF/Comprehensive Care Program for CF/Rx Cost Reduction.

- Letter C was sent to individuals who were enrolled in the Bayer Patient Assistance Program or Indigent Patient Program.

- Letter D was sent to individuals who were enrolled in GlaxoSmithKline's Bridges to Access/Commitment to Access.

- Letter E was sent to individuals who were enrolled in the IVAX Patient Assistance Program.

- Letter F was sent to individuals who were enrolled in Johnson & Johnson's Duragesic Patient Assistance Program.

- Letter G was sent to individuals who were enrolled in Pfizer's FirstRESOURCE Program.

- Letter H was sent to individuals who were enrolled in Schering Plough's SP-Cares.

- Letter I was sent to individuals who were enrolled in Serono's Serostim Patient Assistance Program and Saizen Patient Assistance Program.

We have taken this security breach very seriously and are taking steps to prevent this from happening again. If you need additional information regarding this event or any of the notices, please contact me at (415) 983-8863.

Tienne Lee
Senior Counsel
McKesson Corporation

LETTER A

Pending

LETTER B

[Date]

[First Name] [Last Name]
[Address line 1]
[Address line2]
[City] [State] [Zip]

Dear [First Name],

We are writing to inform you of a recent computer theft that occurred in our offices and resulted in the possible inadvertent disclosure of personal information. As you may know, McKesson Specialty administers Patient Assistance Programs (PAPs) for a number of drug manufacturers, including the Axcan CareFirst Program. These programs make many vital drugs more affordable for patients. When you enrolled in the Patient Assistance Program, we received certain information about you, which may include the following:

- Name
- Prescription
- Social security number
- Dosage/Supply
- Address
- Prescriber
- Date of Birth
- Pharmacy

We have sent you this letter because your personal information may have been on one of two computers that were stolen from a McKesson office. At this point, we have not determined whether your personal information was on either of the stolen computers. And if it were, we believe it is unlikely that the information will be accessed or used without your knowledge. However, we are taking the precaution of notifying every patient whose information *might* have been on the computers, just to be safe.

As soon as we became aware of the theft on July 18th, we took immediate steps to investigate the incident and to determine the scope of information maintained on the computers. We have also taken steps to ensure that this type of incident does not happen again by increasing and improving our employee's understanding and awareness of our corporate security policies and procedures, policies for handling patient data, and laptop security procedures. We are also reviewing our internal auditing procedures, standard operating procedures for data handling, disk encryption, and physical security, and will make changes as appropriate or necessary.

What Does This Mean to You? Again, at this point we cannot confirm whether your information was on one of the stolen computers but if it were, we believe it is unlikely that it will be used without your knowledge. However, to best protect yourself from the possibility of identity theft, you may want to consider placing a fraud alert on your credit files. A fraud alert lets creditors know to contact you before opening new accounts. There is no charge to place a fraud alert on your own credit files. In order to place a fraud alert on your file, contact any one of the three credit reporting agencies at the number below. When you have confirmed a fraud alert with one of the credit reporting agencies, it will alert the others automatically. You will then receive letters from all of them, with instructions on how to get a free copy of your credit report from each.

Experian – 888-397-3742
Equifax – 800-685-1111
TransUnion Corp – 800-680-7289

When you receive your credit reports, review them carefully for any suspicious activities and unfamiliar accounts. If you see anything that you do not understand, call the credit reporting agency at the telephone number on the report.

We deeply regret that this incident occurred and want you to know, as more fully described above, that we have taken steps to prevent it from happening again. If you have any questions regarding this letter, please contact our hotline at 866-554-6366.

Sincerely yours,

Patrick Blake
President, McKesson Specialty

LETTER C

[Date]

Dear _____;

We are writing to inform you of a recent computer theft that occurred in one of our offices. Two computers, which contained patient information, were stolen. As you may know, McKesson Specialty administers Patient Assistance Programs (PAPs) for a number of drug manufacturers, including the Nimotop® (nimodipine) 30 mg capsules and Precose® (acarbose) program that we administer on behalf of Bayer HealthCare. As you know, these programs make many vital drugs more affordable for patients. When you enrolled in the Patient Assistance Program, you provided certain information about yourself, which may include the following:

- Name
- Prescription and dosage
- Social security number
- Address
- Prescriber
- Date of Birth
- Pharmacy

We have sent you this letter because your personal information was contained on the hard drive of one of the two stolen computers. Because access to information on the computers was password protected, we believe it is unlikely that the information will be accessed or used for illegal purposes. However, we are taking the precaution of notifying every patient whose information has even a remote potential to be accessed by unauthorized individuals.

As soon as we became aware of the theft on July 18, we took immediate steps to investigate the incident and to determine the scope of information maintained on the computers. We have also taken steps to ensure that this type of incident does not happen again by increasing and improving our employee's understanding and awareness of our corporate security policies and procedures, policies for handling patient data, and computer security procedures. We are also reviewing our internal auditing procedures, standard operating procedures for data handling, disk encryption, and physical security, and will make changes as appropriate or necessary.

What Does This Mean to You?

Because social security numbers were included in the information you provided to us, in order to best protect yourself from the possibility of identity theft, you may want to consider placing a fraud alert on your credit files. A fraud alert lets creditors know to contact you before any accounts can be opened in your name. There is no charge for this service. In order to place a fraud alert on your file, contact one of the three credit reporting agencies at the numbers below. When you have confirmed a fraud alert with one of the credit reporting agencies, that agency will alert the others automatically. You will then receive letters from all of them, with instructions on how to obtain a free copy of your credit report from each agency.

Experian – 888-397-3742
Equifax – 800-685-1111
TransUnion Corp – 800-680-7289

When you receive your credit reports, review them carefully for any suspicious activities or unfamiliar accounts. If you see anything that you do not understand, call the credit reporting agency at the telephone number on the report.

We deeply regret that this incident occurred and want you to know, as more fully described above, that we have taken steps to prevent it from happening again. If you have any questions regarding this letter, please contact our hotline at 866-554-6366.

Sincerely yours,

Patrick Blake
President, McKesson Specialty

LETTER D

[Date]

Dear _____;

We are writing to inform you of a recent computer theft that occurred from our offices that may have resulted in an inadvertent disclosure of personal information. As you may know, McKesson Specialty administers certain aspects of various drug manufacturers' Patient Assistance Programs (PAPs), including GlaxoSmithKline's programs, including Bridges to Access, Commitment to Access and GSK Access. As part of the enrollment process, we receive certain information about you or on your behalf which may include the following data:

• Name (first and last)	• Prescription
• Social security number	• Dosage/Supply
• Address	• Prescriber
• Date of Birth	• Pharmacy

You are receiving this letter because your personal information was among those patients whose information was stored on a stolen computer. While some of the information that was stored on the computer was encrypted; we cannot confirm that all of the personal information was encrypted. Accordingly, in an abundance of caution, we are notifying all individuals whose information was stored on the computer.

As soon as we became aware of the theft on July 18th, we took immediate steps to investigate the incident and to determine the scope of information maintained on the computers. In addition to examining our physical security precautions and procedures, we have also taken steps to ensure that this type of incident does not occur again by increasing and enhancing our employees' understanding and awareness of our corporate security policies, and procedures, procedures for handling patient information, and computer security procedures. We are also looking at our internal auditing procedures, standard operating procedures for data handling, disk encryption, and physical security and will make changes as appropriate or necessary.

At this time we are not aware of any actual identity theft relating to the computer theft. However, to protect yourself from the possibility of identity theft, you may want to consider placing a fraud alert on your credit files. A fraud alert lets creditors know to contact you before opening new accounts. In order to place a fraud alert on your file, contact any one of the three credit reporting agencies at the number below. When you have confirmed a fraud alert with one of the credit reporting agencies, it will alert the others automatically. You will then receive letters from all of them, with instructions on how to get a free copy of your credit report from each.

Experian	Equifax	TransUnion Corp.
888-397-3742	800-685-1111	800-680-7289

When you receive your credit reports, review them carefully for any suspicious activities and unfamiliar accounts. If you see anything that you do not understand, call the credit reporting agency at the telephone number on the report. In addition, we advise you to be vigilant by monitoring your financial accounts and checking your credit reports regularly. Additionally, if you are a resident of the state of Maryland, we are obligated to provide you with the following additional information: The Federal Trade Commission's Identity Theft Hotline 1-877-438-4338; and address: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580; http://www.ftc.gov/bcp/edu/microsites/idtheft/military/detect.html) and the Maryland state Attorney General's telephone number (410) 576-6300 or 1 (888) 743-0023 toll-free in Maryland; Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202; http://www.oag.state.md.us. Residents of Maryland can obtain information from these sources about steps you can take to avoid identify theft.

We regret that this incident occurred and have taken steps to prevent it from happening again. As noted above, we are not aware that any actual identify theft has occurred; however, we recognize that you may have concerns regarding this incident. If you have any questions regarding this letter, please contact us at 866-554-6366.

Sincerely yours,

Patrick Blake
President, McKesson Specialty

LETTER E

[Date]

[First Name] [Last Name]
[Address line 1]
[Address line2]
[City] [State] [Zip]

Dear [First Name],

We are writing to inform you of a recent computer theft that occurred in our offices and resulted in the possible inadvertent disclosure of personal information. As you may know, McKesson Specialty administers Patient Assistance Programs (PAPs) for a number of drug manufacturers, including IVAX Patient Assistance Program. These programs make many vital drugs more affordable for patients. When you enrolled in the Patient Assistance Program, we received certain information about you, which may include the following:

- Name
- Prescription
- Social security number
- Dosage/Supply
- Address
- Prescriber
- Date of Birth
- Pharmacy

We have sent you this letter because your personal information may have been on one of two computers that were stolen from a McKesson office. At this point, we have not determined whether your personal information was on either of the stolen computers. And if it were, we believe it is unlikely that the information will be accessed or used without your knowledge. However, we are taking the precaution of notifying every patient whose information *might* have been on the computers, just to be safe.

As soon as we became aware of the theft on July 18th, we took immediate steps to investigate the incident and to determine the scope of information maintained on the computers. We have also taken steps to ensure that this type of incident does not happen again by increasing and improving our employee's understanding and awareness of our corporate security policies and procedures, policies for handling patient data, and laptop security procedures. We are also reviewing our internal auditing procedures, standard operating procedures for data handling, disk encryption, and physical security, and will make changes as appropriate or necessary.

What Does This Mean to You? Again, at this point we cannot confirm whether your information was on one of the stolen computers but if it were, we believe it is unlikely that it will be used without your knowledge. However, to best protect yourself from the possibility of identity theft, you may want to consider placing a fraud alert on your credit files. A fraud alert lets creditors know to contact you before opening new accounts. There is no charge to place a fraud alert on your own credit files. In order to place a fraud alert on your file, contact any one of the three credit reporting agencies at the number below. When you have confirmed a fraud alert with one of the credit reporting agencies, it will alert the others automatically. You will then receive letters from all of them, with instructions on how to get a free copy of your credit report from each.

Experian – 888-397-3742
Equifax – 800-685-1111
TransUnion Corp – 800-680-7289

When you receive your credit reports, review them carefully for any suspicious activities and unfamiliar accounts. If you see anything that you do not understand, call the credit reporting agency at the telephone number on the report.

We deeply regret that this incident occurred and want you to know, as more fully described above, that we have taken steps to prevent it from happening again. If you have any questions regarding this letter, please contact our hotline at 866-554-6366.

Sincerely yours,

Patrick Blake
President, McKesson Specialty

LETTER F

[Date]

[First Name] [Last Name]
[Address line 1]
[Address line2]
[City] [State] [Zip]

Dear [First Name],

We are writing to inform you of a recent computer theft that occurred in our offices and resulted in the possible inadvertent disclosure of personal information. As you may know, McKesson Specialty has administered or continues to administer certain aspects of various drug manufacturers' Patient Assistance Programs (PAPs). In this instance, our services were limited to transaction processing for the manufacturer and marketer of **DURAGESIC®** 12.5mcg (fentanyl transdermal system) CII and ***DURAGESIC®** (fentanyl transdermal system) CII.

When you enrolled in the Patient Assistance Program, we received certain information about you, which may include the following:

- Name
- Prescription
- Social security number
- Dosage/Supply
- Address
- Prescriber
- Date of Birth
- Pharmacy

We have sent you this letter because your personal information may have been on one of two computers that were stolen from a McKesson office. At this point, we have not determined whether your personal information was on either of the stolen computers. And if it were, we believe it is unlikely that the information will be accessed or used without your knowledge. However, we are taking the precaution of notifying every patient whose information *might* have been on the computers, just to be safe.

As soon as we became aware of the theft on July 18th, we took immediate steps to investigate the incident and to determine the scope of information maintained on the computers. We have also taken steps to ensure that this type of incident does not happen again by increasing and improving our employee's understanding and awareness of our corporate security policies and procedures, policies for handling patient data, and laptop security procedures. We are also reviewing our internal auditing procedures, standard operating procedures for data handling, disk encryption, and physical security, and will make changes as appropriate or necessary.

What Does This Mean to You? Again, at this point we cannot confirm whether your information was on one of the stolen computers but if it were, we believe it is unlikely that it will be used without your knowledge. However, to best protect yourself from the possibility of identity theft, you may want to consider placing a fraud alert on your credit files. A fraud alert lets creditors know to contact you before opening new accounts. There is no charge to place a fraud alert on your own credit files. In order to place a fraud alert on your file, contact any one of the three credit reporting agencies at the number below. When you have confirmed a fraud alert with one of the credit reporting agencies, it will alert the others automatically. You will then receive letters from all of them, with instructions on how to get a free copy of your credit report from each.

Experian – 888-397-3742
Equifax – 800-685-1111
TransUnion Corp – 800-680-7289

When you receive your credit reports, review them carefully for any suspicious activities and unfamiliar accounts. If you see anything that you do not understand, call the credit reporting agency at the telephone number on the report.

We deeply regret that this incident occurred and want you to know, as more fully described above, that we have taken steps to prevent it from happening again. If you have any questions regarding this letter, please contact our hotline at 866-554-6366.

Sincerely yours,

Patrick Blake
President, McKesson Specialty

* Product carries Black Box Warning. Full prescribing information is enclosed.

LETTER G

Pending

LETTER H

[Date]

[First Name] [Last Name]
[Address line 1]
[Address line2]
[City] [State] [Zip]

Dear [First Name],

We are writing to inform you of a recent computer theft that occurred in our offices and resulted in the possible inadvertent disclosure of personal information. As you may know, McKesson Specialty administers Patient Assistance Programs (PAPs) for a number of drug manufacturers, including the manufacturer of some of your drug(s). When you enrolled in the Patient Assistance Program, we received certain information about you, which may have included the following:

- Name
- Prescription
- Social security number
- Dosage/Supply
- Address
- Prescriber
- Date of Birth

We have sent you this letter because your personal information may have been on one of two computers that were stolen from a McKesson office. At this point, we have not determined whether your personal information was on either of the stolen computers. However, we are taking the precaution of notifying every patient whose information *might* have been on the computers, just to be safe. The patients who may be affected by this incident include patients who are/were enrolled in Schering-Plough's SP-Cares Patient Assistance Program.

As soon as we became aware of the theft on July 18th, we took immediate steps to investigate the incident and to determine the scope of information maintained on the computers. We have also taken steps to ensure that this type of incident does not happen again by increasing and improving our employees' understanding and awareness of our corporate security policies and procedures, policies for handling patient data, and computer security procedures. We are also reviewing our internal auditing procedures, standard operating procedures for data handling, disk encryption, and physical security, and will make changes as appropriate or necessary.

What Does This Mean to You? Again, at this point we cannot confirm whether your information was on one of the stolen computers. However, to best protect yourself from the possibility of identity theft, you may want to consider placing a fraud alert on your credit files. A fraud alert lets creditors know to contact you before opening new accounts. There is no charge to place a fraud alert on your own credit files. In order to place a fraud alert on your file, contact any one of the three credit reporting agencies at the number below. When you have confirmed a fraud alert with one of the credit reporting agencies, it will alert the others automatically. You will then receive letters from all of them, with instructions on how to get a free copy of your credit report from each.

Experian – 888-397-3742
Equifax – 800-685-1111
TransUnion Corp – 800-680-7289

When you receive your credit reports, review them carefully for any suspicious activities and unfamiliar accounts. If you see anything that you do not understand, call the credit reporting agency at the telephone number on the report.

We deeply regret that this incident occurred and want you to know, as more fully described above, that we have taken steps to prevent it from happening again. If you have any questions regarding this letter, please contact our hotline anytime Monday through Friday between the hours of 10:00a.m. and 7:00p.m EST at **866-554-6366**.

Sincerely yours,

Patrick Blake
President, McKesson Specialty

LETTER I

Pending