

North Carolina Security Breach Reporting Form
Pursuant to the Identity Theft Protection Act of 2005

NOV 15 2007
PLEASE SUBMIT FORM TO:
Consumer Protection Division
NC Attorney General's Office
900 Mail Service Center
Raleigh, NC 27699-9001
Telephone: (919) 716-6000
Toll Free in NC: (877) 566-7226
FAX: (919) 716-6050

Name of Business Owning or Licensing Information Affected by the Breach: McKesson Specialty Pharmacy
Address: 4343 N. Scottsdale Road Ste 150
Scottsdale, AZ 85251
Telephone: 480-463-9000
Fax: 480-463-9990
Email: _____

Date Security Breach Reporting Form submitted: 10/15/07
Date the Security Breach was discovered: 7/18/07
Estimated number of affected individuals: 68,779
Estimated number of NC residents affected: 3,757

Name of business maintaining or possessing information that was the subject of the Security Breach, if the business that experienced the Security Breach is not the same entity as the business reporting the Security Breach (pursuant to N.C.G.S. § 75-65(b)): McKesson Specialty Pharmacy

Describe the circumstances surrounding the Security Breach and state whether the information breached was in electronic or paper format: Two laptop computers were stolen from McKesson's offices. The data was contained on the hard drives.

Regarding electronic information breached, state whether the information breached or potentially breached was password protected or encrypted in some manner. Yes If so, please describe the security measures protecting the information: Data was password protected but passwords may have been available.

Describe any measures taken to prevent a similar Security Breach from occurring in the future: Several measures have been taken to prevent future breaches: physical security improvements as well as education and training designed to prevent future occurrence.

Date affected NC residents were/will be notified: 8/31/07

If there has been any delay in notifying affected NC residents, describe the circumstances surrounding the delay pursuant to N.C.G.S. § 75-65(a) and (c): Some delay but residents were notified as soon as practicable.

If the delay was pursuant to a request from law enforcement pursuant to N.C.G.S. § 75-65(c), please include the written request or the contemporaneous memorandum.

How NC residents were/will be notified? (pursuant to N.C.G.S. § 75-65(e))

- written notice
- electronic notice (email)
- telephone notice
- substitute notice

Please attach copy of the notice if in written form or a copy of any scripted notice if in telephonic form.

Signature: Panela Ferrante Date: 10/15/07
Contact Person, Title: Director, Contract Administration
Address: _____
(if different from above)
Telephone: 480-463-9050 Fax: _____ Email: Panela.Ferrante@McKesson.com

McKesson Corporation

LAW DEPARTMENT
One Post Street
San Francisco, CA 94104
415.983.8300 Tel
415.983.9369 Fax

KOA

MCKESSON

Empowering Healthcare

Tienne Lee
Senior Counsel
direct tel: 415-983-8863

September 11, 2007

Via Federal Express

North Carolina Attorney General's Office
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001

To Whom It May Concern:

We are following up our letter dated August 29, 2007 notifying you of a theft that occurred at McKesson Specialty's Scottsdale, Arizona office on July 18, 2007, in which two computers containing personal information were stolen. In that letter we included examples of the letters that were sent to individuals enrolled in various patient assistance programs. At that time, we did not have all the letters finalized. However, we have now sent letters to all individuals who may have had their information on one of the stolen computers. Please find attached examples of all letters:

- 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 for Nemetop and Precose.
- Letter D was sent to individuals who were enrolled in GlaxoSmithKline's Bridges to Access, Commitment to Access and GSK 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.

North Carolina Attorney General's Office

September 11, 2007

Page Two

- 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.

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

Encls.

LETTER A

Date]

[Name]

[Address]

Re: Important Information for Participants in Patient Assistance Programs - Possible Loss of Information

Dear _____:

McKesson Specialty Arizona Inc. (McKesson Specialty) is writing to advise you that we were recently victimized by a computer theft that may have affected a Patient Assistance Program in which you participate. Specifically, two computers were taken from employees' offices in our Scottsdale, Arizona office.

For your background, McKesson Specialty assists with the enrollment process for individuals who wish to enroll in various drug manufacturers' Patient Assistance Programs (PAPs). One of those PAPs is the AstraZeneca AZ Medicine & Me for people in Medicare Part D ("Medicine&Me PAP"), in which you are enrolled or have been in the process of enrolling. As part of the enrollment process, McKesson Specialty receives information regarding patients who are enrolling in the PAP. This patient information, which is necessary for us to assist in the enrollment process, may include name, address, date of birth, Social Security Number, and prescription-related information, such as the prescription name, who prescribed it, the dosage/supply, and the pharmacy that fills it.

As a result of our internal investigation, McKesson Specialty has reason to believe that information provided to us through various PAPs may have been on the computers stolen from our offices. This may have included information in each of the above categories that you provided to us through the AZ Medicine&Me PAP. Importantly, however, we do not have any evidence of any misuse of our patient data or, for that matter, that the incident at issue was anything other than common theft of the personal computers (and not focused on the data thereon). Nevertheless, as a precaution, we are working with our PAP partners, including in your case AstraZeneca, to notify every patient whose information might have been on the computers.

As you would expect, as soon as we became aware of the theft, we took immediate steps to investigate the incident and to determine the scope of information maintained on the computers. In particular, we immediately contacted law enforcement officials and launched an internal investigation. We have continued to work closely with law enforcement on the investigation and we intend to pursue this matter vigorously.

Although we are not aware of any instance of identity theft as a result of this incident, it may still be prudent to take precautions. Accordingly, to assist you in this process and further protect you, you should be advised of the following information:

- ***What should I do upon receiving this letter?*** As a first step, we strongly recommend that you closely monitor your financial accounts and, if you notice any unauthorized activity, promptly contact your financial institution.
- ***How do I learn more about this matter and what you may need to do?*** McKesson Specialty has established a toll-free number (1-866-554-6366) that you may call during the hours of 10 a.m. and 7 p.m., Monday through Friday, if you have any questions and to obtain additional assistance.
- ***What other precautions could you take?*** There are a range of additional steps that, at your discretion, you may take if you have concerns about this incident and/or any risk of financial or other fraud to you. These include:
 - ❖ **Placing a Fraud Alert on Your File.** McKesson has contacted the three major U.S. credit bureaus to inform them of this incident. Upon receiving a request from you, the agencies will place a "fraud alert" on your file, which alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Although this can make it more difficult for someone to get credit in your name, note that it also may delay your ability to obtain credit because it tells creditors to follow certain procedures to protect you. There is no charge for you to place a fraud alert on your credit file. Should you wish to place a fraud alert, contact any one of the following bureaus:

<i>Agency</i>	<i>General Toll-Free</i>	<i>TTY</i>	<i>Website</i>
Experian	888-397-3742	(800) 735-2989	www.experian.com
Equifax	(888) 766-0008	(866) 478-0030	www.equifax.com
TransUnion	800-680-7289	(877) 533-7803	www.transunion.com

- ❖ **Obtaining a Free Credit Report.** You are entitled under U.S. law 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 877-322-8228.
- ❖ **Placing a Security Freeze on Your Credit File.** Depending on the state that you live in, you may be eligible to place a security freeze on your consumer credit file with each of the three national credit bureaus. A security freeze, which is different from a fraud alert, prohibits credit agencies from sharing your credit file with any potential creditors without your consent. Once your files are frozen, even someone who has your personal information should not be able to obtain credit in your name. More information about security freezes is available through the websites of the three national credit reporting agencies — Equifax, Experian, and TransUnion (website addresses are noted above).
- ***Are there other general information resources that I can reference?*** For more information on how to protect yourself against identity theft or fraud, you may visit the website of the Federal Trade Commission at www.consumer.gov/idtheft/.

McKesson Specialty is a conscientious company that takes security issues very seriously. We deeply regret that this incident occurred and apologize for any inconvenience or concern this has caused. We want you to know that McKesson has taken steps to prevent incidents like this from happening again, including increasing our employee's awareness and training on security policies and procedures, policies for handling patient data, and laptop security procedures.

Sincerely yours,

Patrick Blake
 President, McKesson Specialty

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,

A handwritten signature in black ink, appearing to read 'P. Blake', with a long horizontal stroke extending to the right.

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,

A handwritten signature in black ink, appearing to read 'P. Blake', with a long horizontal stroke extending to the right.

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
888-397-3742

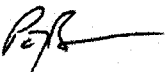
Equifax
800-685-1111

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. 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,

A handwritten signature in black ink, appearing to read 'P. Blake', with a long horizontal stroke extending to the right.

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

[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 yours. 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. The patients who may be affected by this incident include patients who are enrolled in the Pfizer FirstRESOURCE® Patient Assistance Program for Aromasin® or Emcyt®.

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 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 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

In addition, we are offering free credit monitoring and fraud insurance for one year in an effort to protect you in the event of fraudulent activity. Please call us at the number below if you wish to take advantage of this option. 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 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,

A handwritten signature in black ink, appearing to read 'P. Blake', with a long horizontal stroke extending to the right.

Patrick Blake
President, McKesson Specialty

LETTER I

[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 yours. 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. 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. At this point, we have not determined whether your personal information was on either of the stolen computers. Due to the password security we have in place on all our computers, 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. The patients who may be affected by this incident include patients who are enrolled in a total of eight Patient Assistance Programs including the EMD Serono Serocare PAP.

To best protect yourself from the possibility of identity theft, we are suggesting all affected customers place a fraud alert on their 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 we have provided below. When you have confirmed a fraud alert with one of the credit reporting agencies, it will alert the others automatically. There is no charge to place a fraud alert on your own credit files.

Experian – 888-397-3742

Equifax – 800-685-1111

TransUnion Corp – 800-680-7289

We deeply regret that this incident occurred and assure you that we are taking further steps to ensure that this type of incident does not happen again by increasing and improving 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.

If you have any questions regarding this letter, please contact us at 1-866-554-6366.

Sincerely yours,

Patrick Blake
President, McKesson Specialty