



55 East Monroe Street  
37th Floor  
Chicago, IL 60603

312 346 7500 main  
312 580 2201 fax  
thompsoncoburn.com

STATE OF NH  
DEPT OF JUSTICE  
2018 JAN 19 AM 11:07

**Melissa K. Ventrone**  
312 580 2219 direct  
[mventrone@thompsoncoburn.com](mailto:mventrone@thompsoncoburn.com)  
January 12, 2018

**Attorney General Joseph Foster**  
Office of the Attorney General  
33 Capitol Street  
Concord, NH 03302

Dear Attorney General Foster:

We represent PharMerica Corporation (“PharMerica”) with respect to a recent security incident involving PharMerica’s specialty pharmacies, Onco360 Oncology Pharmacy (“Onco360”) and CareMed Specialty Pharmacy (“CareMed”). This incident potentially impacted certain personal information of individuals receiving pharmacy services from Onco360 and CareMed as described in more detail below.

**1. Nature of security incident.**

On November 14, 2017, suspicious activity involving an employee’s email account was identified. Independent computer forensic experts were engaged to assist with the investigation. On November 30, 2017, the forensic investigation determined that an unauthorized user appeared to have gained access to email accounts of three employees. A detailed review of the impacted email accounts was performed, and on January 8, 2018, it was determined that a limited number of those e-mails may have contained demographic information, medication and clinical information, health insurance information and Social Security numbers of some of the patients receiving services from Onco360 and CareMed Specialty Pharmacy. A very small number of individuals may have had their financial account information affected impacted as well.

**2. Number of New Hampshire residents affected.**

Two hundred and sixty-three (263) New Hampshire residents were notified of the incident. A notification letter was sent to the affected individuals on January 12, 2018 via regular mail (a copy of the form notification letter is enclosed).

**3. Steps taken or plan to take relating to the incident.**

Steps have been taken to help prevent a similar occurrence in the future. Passwords to all Onco360 and CareMed personnel e-mail accounts were changed and the compromised e-mail accounts were secured. The incident was reported to law enforcement. To help prevent such an incident from reoccurring, additional e-mail security enhancements were implemented and additional training was provided to employees on recognizing and appropriately responding to

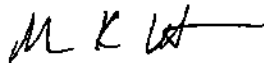
suspicious emails and other security threats. Additionally, affected individuals were offered credit monitoring and identity restoration services free of charge for one year through ID Experts. The credit reporting agencies have also been notified of this incident.

**4. Contact information.**

PharMerica remains dedicated to protecting the confidential information in its possession. If you have any questions or need additional information, please do not hesitate to contact me at [MVentrone@ThompsonCoburn.com](mailto:MVentrone@ThompsonCoburn.com) or (312) 580-2219.

Very truly yours,

Thompson Coburn LLP

A handwritten signature in black ink, appearing to read "M K Ventrone", with a horizontal line extending to the right.

Melissa K. Ventrone

Enclosure



C/O ID Experts  
P.O. Box 10444  
Dublin, OH 43017-4044

To Enroll, Please Call:  
(800) 761-7902  
Or Visit:  
<https://ide.myidcare.com/onco360caremed>  
Enrollment Code: [XXXXXXXXXX]

<<Name>>  
<<Address1>>  
<<Address2>>  
<<City>><<State>><<ZIP>>

January 12, 2018

Dear <<Name>>:

We are writing this letter to notify you of a recent data security incident involving PharMerica's specialty pharmacies, Onco360 and CareMed Specialty Pharmacy, which may have impacted information of patients receiving services from these pharmacies. We sincerely apologize for this incident and want you to know that we take our responsibility of protecting your information very seriously. This letter contains details about this incident, steps you can take to protect your personal information and resources we are making available to help you.

**What happened:**

On November 14, 2017, we discovered suspicious activity involving an employee's email account. We immediately engaged independent computer forensic experts to assist with investigating this matter. On November 30, 2017, the forensic investigation determined that an unauthorized user appeared to have gained access to email accounts of three employees. A detailed review of the impacted e-mail accounts was performed and on January 8, 2018, we determined that the emails in those e-mail accounts contained your name and Social Security number and may have potentially contained your address, medication and clinical information, and health insurance information. For a very small number of individuals, credit or debit card or financial account information may also have been impacted.

**What we are doing and what you can do:**

Although there is no indication that any of your information has been misused and even if the risk of misuse may be low, to help protect you from any potential negative consequences from this incident, we have arranged for you to receive credit monitoring and identity protection services from ID Experts, which we are offering at no cost to you for one year. You are automatically covered for the fully managed identity resolution services, so there is no need to enroll for this benefit. If you have an identity theft issue, simply call ID Experts at (800) 761-7902 for immediate assistance.

We also encourage you to enroll in the free credit monitoring and insurance services by using the enrollment code at the top of this letter and going to <https://ide.myidcare.com/onco360caremed> or calling (800) 761-7902. MyIDCare experts are available Monday through Friday from 8 am - 8 pm Eastern Time. Please note the deadline to enroll in credit monitoring and insurance services is April 12, 2018.

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling on the website, so please do not discard this letter.

In addition, as a precaution, you should monitor your credit and debit card statements, billing statements and other financial account statements in the upcoming months. Please immediately notify your bank if you notice any suspicious activity. More information on how to protect your identity is enclosed with this letter.

We also want you to know that we took appropriate measures to promptly address this incident. Passwords to all Onco360 and CareMed personnel e-mail accounts were changed and the compromised e-mail accounts were secured. We notified law enforcement of the incident and are cooperating with their investigation. To help prevent such an incident from reoccurring, we implemented additional e-mail security enhancements and also provided additional training to our employees on recognizing and appropriately responding to suspicious emails and other security threats.

**For more information:**

Again, we are very sorry that this incident occurred. We want to emphasize that protecting the confidentiality and security of patient information entrusted to us is our utmost priority. If you have any questions about this letter or would like any additional information, please contact the dedicated call center at (800) 761-7902 which we set up to help answer your questions regarding this incident. The call center is available Monday through Friday from 8:00 am to 8:00 pm Eastern Time. You may also submit your questions in writing to Onco360/CareMed Specialty Pharmacy, Compliance Officer, 1901 Campus Place, Suite 100, Louisville, KY 40299.

Sincerely,

A handwritten signature in black ink that reads "Paul E. Jardina". The signature is written in a cursive style with a large, prominent initial "P".

Paul E. Jardina, President & CEO  
Onco360 and CareMed Specialty Pharmacy

Enclosure



### Recommended Steps to help Protect your Information

**Please Note: Minors, under the age of 18, should not have a credit history established and are under the age to secure credit. Therefore credit monitoring may not be applicable at this time. All other services provided in the membership will apply. No one is allowed to place a fraud alert on your credit report except you, please follow the instructions below to place the alert.**

**1. Website and Enrollment.** Go to <https://ide.myidcare.com/onco360caremed> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Once you have completed your enrollment, you will receive a welcome letter by email (or by mail if you do not provide an email address when you sign up). The welcome letter will direct you to the exclusive MyIDCare Member Website where you will find other valuable educational information.

**2. Activate the credit monitoring** provided as part of your MyIDCare membership, which is paid for by PharMerica Corporation. Credit and CyberScan monitoring are included in the membership, but you must personally activate it for it to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.

**3. Telephone.** Contact MyIDCare at (800) 761-7902 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

**4. Review your credit reports.** We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to [www.annualcreditreport.com](http://www.annualcreditreport.com) or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in MyIDCare, notify them immediately by calling or by visiting their Member website and filing a theft report.

If you file a theft report with MyIDCare, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

**5. Place Fraud Alerts** with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

## Credit Bureaus

Equifax Fraud Reporting  
1-800-525-6285  
P.O. Box 105069  
Atlanta, GA 30348  
[www.alerts.equifax.com](http://www.alerts.equifax.com)

Experian Fraud Reporting  
1-888-397-3742  
P.O. Box 9554  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)

TransUnion Fraud Reporting  
1-800-680-7289  
P.O. Box 2000  
Chester, PA 19022-2000  
[www.transunion.com](http://www.transunion.com)

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review.

**6. Security Freeze.** By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above in writing to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. The cost of placing the freeze varies by the state you live in and for each credit reporting bureau. The Credit Bureau may charge a fee of up to \$5.00 to place a freeze, lift, or remove a freeze. However, if you are a victim of identity theft and have filed a report with your local law enforcement agency or submitted an ID Theft Complaint Form with the Federal Trade Commission, there may be no charge to place the freeze.

**7. You can obtain additional information** about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

**California Residents:** Visit the California Office of Privacy Protection ([www.privacy.ca.gov](http://www.privacy.ca.gov)) for additional information on protection against identity theft.

**Kentucky Residents:** Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, [www.ag.ky.gov](http://www.ag.ky.gov), Telephone: 1-502-696-5300.

**Maryland Residents:** Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, [www.oag.state.md.us/Consumer](http://www.oag.state.md.us/Consumer), Telephone: 1-888-743-0023.

**North Carolina Residents:** Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, [www.ncdoj.com/](http://www.ncdoj.com/), Telephone: 1-919-716-6400.

**Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, [www.doj.state.or.us/](http://www.doj.state.or.us/), Telephone: 877-877-9392

**Rhode Island Residents:** Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, [www.riag.ri.gov](http://www.riag.ri.gov), Telephone: 401-274-4400

**All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft), 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.



C/O ID Experts  
P.O. Box 10444  
Dublin, OH 43017-4044

To Enroll, Please Call:  
(800) 761-7902  
Or Visit:  
<https://ide.myidcare.com/onco360caremed>  
Enrollment Code: [XXXXXXXXXX]

<<Name>>  
<<Address1>>  
<<Address2>>  
<<City>><<State>><<ZIP>>

January 12, 2018

Dear <<Name>>:

We are writing this letter to notify you of a recent data security incident involving PharMerica's specialty pharmacies, Onco360 and CareMed Specialty Pharmacy, which may have impacted information of patients receiving services from these pharmacies. We sincerely apologize for this incident and want you to know that we take our responsibility of protecting your information very seriously. This letter contains details about this incident, steps you can take to protect your personal information and resources we are making available to help you.

**What happened:**

On November 14, 2017, we discovered suspicious activity involving an employee's email account. We immediately engaged independent computer forensic experts to assist with investigating this matter. On November 30, 2017, the forensic investigation determined that an unauthorized user appeared to have gained access to email accounts of three employees. A detailed review of the impacted e-mail accounts was performed and on January 8, 2018, we determined that the emails in those e-mail accounts contained your name and may have potentially contained your address, medication and clinical information, and health insurance information. For a very small number of individuals, credit or debit card or financial account information may also have been impacted. We confirmed that your Social Security number was not affected and remains secure.

**What we are doing and what you can do:**

Although there is no indication that any of your information has been misused and even if the risk of misuse may be low, to help protect you from any potential negative consequences from this incident, we have arranged for you to receive credit monitoring and identity protection services from ID Experts, which we are offering at no cost to you for one year. You are automatically covered for the fully managed identity resolution services, so there is no need to enroll for this benefit. If you have an identity theft issue, simply call ID Experts at (800) 761-7902 for immediate assistance.

We also encourage you to enroll in the free credit monitoring and insurance services by using the enrollment code at the top of this letter and going to <https://ide.myidcare.com/onco360caremed> or calling (800) 761-7902. MyIDCare experts are available Monday through Friday from 8 am - 8 pm Eastern Time. Please note the deadline to enroll in credit monitoring and insurance services is April 12, 2018.

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling on the website, so please do not discard this letter.

In addition, as a precaution, you should monitor your credit and debit card statements, billing statements and other financial account statements in the upcoming months. Please immediately notify your bank if you notice any suspicious activity. More information on how to protect your identity is enclosed with this letter.

We also want you to know that we took appropriate measures to promptly address this incident. Passwords to all Onco360 and CareMed personnel e-mail accounts were changed and the compromised e-mail accounts were secured. We notified law enforcement of the incident and are cooperating with their investigation. To help prevent such an incident from reoccurring, we implemented additional e-mail security enhancements and also provided additional training to our employees on recognizing and appropriately responding to suspicious emails and other security threats.

**For more information:**

Again, we are very sorry that this incident occurred. We want to emphasize that protecting the confidentiality and security of patient information entrusted to us is our utmost priority. If you have any questions about this letter or would like any additional information, please contact the dedicated call center at (800) 761-7902 which we set up to help answer your questions regarding this incident. The call center is available Monday through Friday from 8:00 am to 8:00 pm Eastern Time. You may also submit your questions in writing to Onco360/CareMed Specialty Pharmacy, Compliance Officer, 1901 Campus Place, Suite 100, Louisville, KY 40299.

Sincerely,

A handwritten signature in black ink that reads "Paul E. Jardina". The signature is written in a cursive, flowing style.

Paul E. Jardina, President & CEO  
Onco360 and CareMed Specialty Pharmacy

Enclosure





### Recommended Steps to help Protect your Information

**Please Note: Minors, under the age of 18, should not have a credit history established and are under the age to secure credit. Therefore credit monitoring may not be applicable at this time. All other services provided in the membership will apply. No one is allowed to place a fraud alert on your credit report except you, please follow the instructions below to place the alert.**

**1. Website and Enrollment.** Go to <https://ide.myidcare.com/onco360caremed> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Once you have completed your enrollment, you will receive a welcome letter by email (or by mail if you do not provide an email address when you sign up). The welcome letter will direct you to the exclusive MyIDCare Member Website where you will find other valuable educational information.

**2. Activate the credit monitoring** provided as part of your MyIDCare membership, which is paid for by PharMerica Corporation. Credit and CyberScan monitoring are included in the membership, but you must personally activate it for it to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.

**3. Telephone.** Contact MyIDCare at (800) 761-7902 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

**4. Review your credit reports.** We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to [www.annualcreditreport.com](http://www.annualcreditreport.com) or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in MyIDCare, notify them immediately by calling or by visiting their Member website and filing a theft report.

If you file a theft report with MyIDCare, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

**5. Place Fraud Alerts** with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

## Credit Bureaus

Equifax Fraud Reporting  
1-800-525-6285  
P.O. Box 105069  
Atlanta, GA 30348  
[www.alerts.equifax.com](http://www.alerts.equifax.com)

Experian Fraud Reporting  
1-888-397-3742  
P.O. Box 9554  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)

TransUnion Fraud Reporting  
1-800-680-7289  
P.O. Box 2000  
Chester, PA 19022-2000  
[www.transunion.com](http://www.transunion.com)

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review.

**6. Security Freeze.** By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above in writing to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. The cost of placing the freeze varies by the state you live in and for each credit reporting bureau. The Credit Bureau may charge a fee of up to \$5.00 to place a freeze, lift, or remove a freeze. However, if you are a victim of identity theft and have filed a report with your local law enforcement agency or submitted an ID Theft Complaint Form with the Federal Trade Commission, there may be no charge to place the freeze.

**7. You can obtain additional information** about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

**California Residents:** Visit the California Office of Privacy Protection ([www.privacy.ca.gov](http://www.privacy.ca.gov)) for additional information on protection against identity theft.

**Kentucky Residents:** Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, [www.ag.ky.gov](http://www.ag.ky.gov), Telephone: 1-502-696-5300.

**Maryland Residents:** Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, [www.oag.state.md.us/Consumer](http://www.oag.state.md.us/Consumer), Telephone: 1-888-743-0023.

**North Carolina Residents:** Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, [www.ncdoj.com/](http://www.ncdoj.com/), Telephone: 1-919-716-6400.

**Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, [www.doj.state.or.us/](http://www.doj.state.or.us/), Telephone: 877-877-9392

**Rhode Island Residents:** Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, [www.riag.ri.gov](http://www.riag.ri.gov), Telephone: 401-274-4400

**All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft), 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.