15788

Women's Care FLORIDA
North Florida Ob-Gyn

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

[FIRST] [LAST]
[STREET]
[CITY] [STATE] [ZIP]

September 25, 2019

NOTICE OF DATA BREACH

Dear [FIRST] [LAST]:

At North Florida OB/GYN, we understand that the confidentiality and security of your medical and personal information is critically important, and we are committed to protecting it. This letter is to notify you of a recent cyber incident that affected North Florida OB/GYN and may have resulted in a compromise of certain computer systems containing your medical or personal information.

WHAT HAPPENED

On July 27, 2019, North Florida OB/GYN became aware that a portion of its computer systems were being affected by a cyber incident that we suspect may have begun on or before April 29, 2019. Shortly after becoming aware of the incident, North Florida OB/GYN completed a preliminary assessment, in consultation with third party information technology consultants, and determined that there had been improper access to certain portions of its networked computer systems and that a computer virus had encrypted (made unreadable) certain files on its computer systems. North Florida OB/GYN promptly shut down its networked computer systems, initiated its incident response and recovery procedures, notified the Federal Bureau of Investigation, and began a privileged and confidential forensic investigation. Since then, North Florida OB/GYN has decrypted (made readable again) or recovered virtually all of the affected files and has taken actions to strengthen security safeguards for the affected systems and prevent similar incidents.

Though our investigation is ongoing, based on the findings of the investigation to date, we have no evidence that any unauthorized person actually viewed, retrieved, or copied any of your medical or personal information. However, out of an abundance of caution, we are notifying you and other individuals who may have had medical or personal information contained on the affected computer systems.

WHAT INFORMATION WAS INVOLVED

The medical or personal information affected by the incident may have included your name, demographic information, date of birth, Social Security number, driver's license or identification card number, employment information, health insurance information, and health information, including, for example, medical histories, treatment and diagnosis information, and related information and medical images. The affected computer systems did not contain any credit or debit card or financial account information.

WHAT WE ARE DOING

After becoming aware of the incident, we took immediate steps to address the incident and mitigate any impact on our patients. We also promptly notified the Federal Bureau of Investigation of the incident and immediately initiated our privileged and confidential forensic investigation. In addition, we have strengthened our virus detection and other systems and safeguards to prevent unauthorized persons from gaining access to our systems. We have also taken other steps to try to prevent similar incidents in the future. This notification was not delayed as a result of any law enforcement investigation.

We have notified the U.S. Department of Health and Human Services Office for Civil Rights and relevant state regulators of this incident.

As an added precaution to help safeguard your information from potential misuse, we are partnering with Equifax to provide its Equifax® Credit Watch™ Gold for 18 months at no cost to you. A description of this product is provided in the attached material, which also contains instructions about how to enroll (including your personal activation code). If you choose to take advantage of the Equifax Credit Watch Gold product, it will provide you with identity theft detection and resolution of identity theft services as described in the attached material. In order for us to activate this service, you must complete the enrollment process by January 31, 2020.

WHAT YOU CAN DO

It is important to reiterate that, based on the findings of the investigation to date, we have no evidence that any unauthorized person actually viewed, retrieved, or copied any of your medical or personal information. However, we also want to make you aware of certain precautionary measures that you may want to consider. We ask that you review the "Information About Identity Theft Protection" sheet enclosed with this letter. You should always remain vigilant by regularly reviewing your account statements and monitoring free credit reports, and immediately report to your financial institutions any suspicious activity involving one of your accounts. Please also consider enrolling in the Equifax Credit Watch Gold product that we have offered to you.

FOR MORE INFORMATION

For more information, please call 855-913-0607 anytime from 9:00 a.m. to 9:00 p.m. ET, Monday through Friday, excluding major holidays, or visit www.nfobgyn.com.

We apologize for any inconvenience or concern that this incident may have caused you. We take the confidentiality and security of your medical and personal information very seriously and will continue to take steps to help prevent a similar incident in the future.

Sincerely,

C. Cameron Greene, M.D.
Representative,
North Florida OB/GYN,
a division of Women's Care Florida

Enclosures

Y8842 v.02

GENERAL INFORMATION ABOUT IDENTITY THEFT PROTECTION

You should remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

Credit Reports. Under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

You may contact the nationwide credit reporting agencies at:

Equifax	**Experian**	**TransUnion**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
(800) 525-6285	(888) 397-3742	(800) 680-7289

You may contact the Federal Trade Commission (FTC) and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should contact the FTC and/or your state's attorney general office for information on how to prevent or avoid identity theft.

You can contact the FTC at: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20508, www.ftc.gov, 1-877-IDTHEFT (438-4338).

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. 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.

Place a Security Freeze on your Credit Report. You also have the right to place a security freeze on your credit report by contacting any of the credit bureaus listed above. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line or a written request. 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. You can place and lift a security freeze on your credit report free of charge.

Police Reports. You have the right to file or obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

EQUIFAX®

Enter your Activation Code: [CODE]

Product Information

Equifax® Credit Watch™ Gold provides you with the following key features:
- Equifax® credit file monitoring with alerts to key changes to your Equifax Credit Report
- Automatic Fraud Alerts[1] – With a fraud alert, potential lenders are encouraged to take extra steps to verify your ID before extending credit
- Wireless alerts (available online only, data charges may apply)
- Access to your Equifax® credit report
- Up to $25,000 Identity Theft Insurance[2]
- Live agent customer service 7 days a week from 8 a.m. to 3 a.m.

Enrollment Instructions

To sign up online for online delivery go to www.myservices.equifax.com/gold
1. Welcome Page: Enter the Activation Code provided at the top of this page in the "Activation Code" box and click the "Submit" button.
2. Register: Complete the form with your contact information (name, gender, home address, date of birth, Social Security number and telephone number) and click the "Continue" button.
3. Create Account: Complete the form with your email address, create a User Name and Password, check the box to accept the Terms of Use and click the "Continue" button.
4. Verify ID: The system will then ask you up to four security questions to verify your identity. Please answer the questions and click the "Submit Order" button.
5. Order Confirmation: This page shows you your completed enrollment. Please click the "View My Product" button to access the product features.

To sign up for US Mail delivery, dial 1-866-937-8432 for access to the Equifax Credit Watch automated enrollment process. Note that all credit reports and alerts will be sent to you via US Mail only.
1. Activation Code: You will be asked to enter your enrollment code as provided at the top of this letter.
2. Customer Information: You will be asked to enter your home telephone number, home address, name, date of birth and Social Security Number.
3. Permissible Purpose: You will be asked to provide Equifax with your permission to access your Equifax credit file and to monitor your file. Without your agreement, Equifax cannot process your enrollment.
4. Order Confirmation: Equifax will provide a confirmation number with an explanation that you will receive your Fulfillment Kit via the US Mail (when Equifax is able to verify your identity) or a Customer Care letter with further instructions (if your identity can not be verified using the information provided). Please allow up to 10 business days to receive this information.

1. The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

2. Identity theft insurance is underwritten by American Bankers Insurance Company of Florida or its affiliates. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions and exclusions of coverage. Coverage may not be available in all jurisdictions.

Y9644 v.02

Women's Care™
FLORIDA
North Florida Ob-Gyn

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

Parent, Legal Guardian, or Guarantor of
[FIRST] [LAST]
[STREET]
[CITY] [STATE] [ZIP]

September 25, 2019

NOTICE OF DATA BREACH

Dear Parent, Legal Guardian, or Guarantor of [FIRST] [LAST]:

At North Florida OB/GYN, we understand that the confidentiality and security of medical and personal information is critically important, and we are committed to protecting it. This letter is to notify you of a recent cyber incident that affected North Florida OB/GYN and may have resulted in a compromise of certain computer systems containing your minor's medical or personal information.

WHAT HAPPENED

On July 27, 2019, North Florida OB/GYN became aware that a portion of its computer systems were being affected by a cyber incident that we suspect may have begun on or before April 29, 2019. Shortly after becoming aware of the incident, North Florida OB/GYN completed a preliminary assessment, in consultation with third party information technology consultants, and determined that there had been improper access to certain portions of its networked computer systems and that a computer virus had encrypted (made unreadable) certain files on its computer systems. North Florida OB/GYN promptly shut down its networked computer systems, initiated its incident response and recovery procedures, notified the Federal Bureau of Investigation, and began a privileged and confidential forensic investigation. Since then, North Florida OB/GYN has decrypted (made readable again) or recovered virtually all of the affected files and has taken actions to strengthen security safeguards for the affected systems and prevent similar incidents.

Though our investigation is ongoing, based on the findings of the investigation to date, we have no evidence that any unauthorized person actually viewed, retrieved, or copied any of your minor's medical or personal information. However, out of an abundance of caution, we are notifying you, on behalf of your minor, and other individuals who may have had medical or personal information contained on the affected computer systems.

WHAT INFORMATION WAS INVOLVED

The medical or personal information affected by the incident may have included your minor's name, demographic information, date of birth, Social Security number, driver's license or identification card number, employment information, health insurance information, and health information, including, for example, medical histories, treatment and diagnosis information, and related information and medical images. The affected computer systems did not contain any credit or debit card or financial account information.

WHAT WE ARE DOING

After becoming aware of the incident, we took immediate steps to address the incident and mitigate any impact on our patients. We also promptly notified the Federal Bureau of Investigation of the incident and immediately initiated our privileged and confidential forensic investigation. In addition, we have strengthened our virus detection and other systems and safeguards to prevent unauthorized persons from gaining access to our systems. We have also taken other steps to try to prevent similar incidents in the future. This notification was not delayed as a result of any law enforcement investigation.

We have notified the U.S. Department of Health and Human Services Office for Civil Rights and relevant state regulators of this incident.

As an added precaution to help safeguard your minor's information from potential misuse, we are partnering with Equifax to provide its Equifax Child Identity Monitoring for 18 months at no cost to you. A description of this product is provided in the attached material, which also contains instructions about how to enroll (including your minor's personal activation code). If you choose to take advantage of the Equifax Child Identity Monitoring product, it will scan the Equifax credit database for any instances of the minor's Social Security number and look for a copy of the minor's Equifax credit file as described in the attached material. In order for us to activate this service, you must complete the enrollment process by January 31, 2020.

WHAT YOU CAN DO

It is important to reiterate that, based on the findings of the investigation to date, we have no evidence that any unauthorized person actually viewed, retrieved, or copied any of your minor's medical or personal information. However, we also want to make you aware of certain precautionary measures that you may want to consider. We ask that you review the "Information About Identity Theft Protection" sheet enclosed with this letter. You should always remain vigilant by regularly reviewing account statements and monitoring free credit reports, and immediately report to the applicable financial institutions any suspicious activity. Please also consider enrolling in the Equifax Child Identity Monitoring product that we have offered.

FOR MORE INFORMATION

For more information, please call 855-913-0607 anytime from 9:00 a.m. to 9:00 p.m. ET, Monday through Friday, excluding major holidays, or visit www.nfobgyn.com.

We apologize for any inconvenience or concern that this incident may have caused you. We take the confidentiality and security of medical and personal information very seriously and will continue to take steps to help prevent a similar incident in the future.

Sincerely,

C. Cameron Greene, M.D.
Representative,
North Florida OB/GYN,
a division of Women's Care Florida

Enclosures

GENERAL INFORMATION ABOUT IDENTITY THEFT PROTECTION

You should remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your minor's credit report for unauthorized activity.

Credit Reports. Under federal law, you are entitled to one free copy of your minor's credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your minor's credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

You may contact the nationwide credit reporting agencies at:

Equifax	**Experian**	**TransUnion**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
(800) 525-6285	(888) 397-3742	(800) 680-7289

You may contact the Federal Trade Commission (FTC) and State Attorneys General Offices. If you believe your minor is the victim of identity theft or have reason to believe your minor's personal information has been misused, you should contact the FTC and/or your state's attorney general office for information on how to prevent or avoid identity theft.

You can contact the FTC at: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20508, www.ftc.gov, 1-877-IDTHEFT (438-4338).

Fraud Alert. You may place a fraud alert in your minor's file by calling one of the three nationwide credit reporting agencies above. 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 your minor, but also may cause a delay when seeking to obtain credit.

Place a Security Freeze on your Credit Report. You also have the right to place a security freeze on your minor's credit report by contacting any of the credit bureaus listed above. A security freeze is intended to prevent credit, loans and services from being approved in your minor's name without consent. To place a security freeze on your minor's credit report, you may be able to use an online process, an automated telephone line or a written request. The following information must be included when requesting a security freeze: (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 name and current mailing address, and the date of issue. You can place and lift a security freeze on your minor's credit report free of charge.

Police Reports. You have the right to file or obtain a police report in regard to this incident. If your minor is the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

EQUIFAX®

Enter your Activation Code: [CODE]

Product Information

Equifax Child Identity Monitoring will scan the Equifax credit database for any instances of the minor's Social Security number and look for a copy of the minor's Equifax credit file.

- If no SSN match is found and no Equifax credit file exists, Equifax will create an Equifax credit file in the minor's name and immediately "lock" the Equifax credit file. This will prevent access to the minor's Equifax credit file in the future. If Equifax receives a request for your minor's Equifax credit report, you will receive an email alert.
- If there is a match and an Equifax credit file exists, Equifax will immediately "lock" the file and alert you to activity against the file, such as an attempt to open a new line of credit.
- The minor's Equifax credit file will be locked for 12 months from date of activation. After that time, the minor's Equifax credit file will be deleted from our credit database if it contains no credit data.

Enrollment Instructions

To enroll in Equifax Child Identity Monitoring go to http://myservices.equifax.com/efx1_brminor and follow the instructions below:

1. Welcome Page: Enter the Activation Code provided at the top of this page in the "Activation Code" box and click the "Submit" button.

2. Register: Complete the form with **YOUR** contact information first (name, gender, home address, date of birth, Social Security number and telephone number) and click the "Continue" button.

3. Create Account: Complete the form with your email address, create a User Name and Password, after reviewing the Terms of Use, check the box to accept the Terms of Use and click the "Continue" button.

4. Verify ID: The system will then ask you up to four security questions to verify your identity. Please answer the questions and click the "Submit Order" button.

5. Order Confirmation: This page shows you your completed enrollment. Please click the "View My Product" button to access the product features.

6. Click the orange button "Enroll Child" to enter your child's information (child's name, Date of Birth and Social Security number). Note: if you enter the child's SSN incorrectly, you will need to remove the minor by going to your Member Center and clicking on "My Account" to remove the minor from the account. You may then re-enroll the minor with the correct SSN.

7. Check the box confirming you are the child's parent or guardian.

8. Click "Submit" to enroll your child.

Y9874 v.01

Women's Care FLORIDA
North Florida Ob-Gyn

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

To the Estate of
[FIRST] [LAST]
[STREET]
[CITY] [STATE] [ZIP]

September 25, 2019

NOTICE OF DATA BREACH

Dear Estate of [FIRST] [LAST]:

At North Florida OB/GYN, we understand that the confidentiality and security of medical and personal information is critically important, and we are committed to protecting it. This letter is to notify you, as next of kin to our former patient Jane Russell, of a recent cyber incident that affected North Florida OB/GYN and may have resulted in a compromise of certain computer systems containing your kin's medical or personal information.

WHAT HAPPENED

On July 27, 2019, North Florida OB/GYN became aware that a portion of its computer systems were being affected by a cyber incident that we suspect may have begun on or before April 29, 2019. Shortly after becoming aware of the incident, North Florida OB/GYN completed a preliminary assessment, in consultation with third party information technology consultants, and determined that there had been improper access to certain portions of its networked computer systems and that a computer virus had encrypted (made unreadable) certain files on its computer systems. North Florida OB/GYN promptly shut down its networked computer systems, initiated its incident response and recovery procedures, notified the Federal Bureau of Investigation, and began a privileged and confidential forensic investigation. Since then, North Florida OB/GYN has decrypted (made readable again) or recovered virtually all of the affected files and has taken actions to strengthen security safeguards for the affected systems and prevent similar incidents.

Though our investigation is ongoing, based on the findings of the investigation to date, we have no evidence that any unauthorized person actually viewed, retrieved, or copied any of your kin's medical or personal information. However, out of an abundance of caution, we are notifying you, on behalf of your next of kin, and other individuals who may have had medical or personal information contained on the affected computer systems.

WHAT INFORMATION WAS INVOLVED

The medical or personal information affected by the incident may have included your kin's name, demographic information, date of birth, Social Security number, driver's license or identification card number, employment information, health insurance information, and health information, including, for example, medical histories, treatment and diagnosis information, and related information and medical images. The affected computer systems did not contain any credit or debit card or financial account information.

WHAT WE ARE DOING

After becoming aware of the incident, we took immediate steps to address the incident and mitigate any impact on our current or former patients. We also promptly notified the Federal Bureau of Investigation of the incident and immediately initiated our privileged and confidential forensic investigation. In addition, we have strengthened our virus detection and other systems and safeguards to prevent unauthorized persons from gaining access to our systems. We have also taken other steps to try to prevent similar incidents in the future. This notification was not delayed as a result of any law enforcement investigation.

We have notified the U.S. Department of Health and Human Services Office for Civil Rights and relevant state regulators of this incident.

WHAT YOU CAN DO

It is important to reiterate that, based on the findings of the investigation to date, we have no evidence that any unauthorized person actually viewed, retrieved, or copied any of your kin's medical or personal information. However, we also want to make you aware of certain precautionary measures that you may want to consider. We ask that you review the "Protecting Deceased Individuals" sheet enclosed with this letter. You should always remain vigilant by regularly reviewing account statements and monitoring free credit reports, and immediately report to the applicable financial institutions any suspicious activity.

FOR MORE INFORMATION

For more information, please call 855-913-0607 anytime from 9:00 a.m. to 9:00 p.m. ET, Monday through Friday, excluding major holidays, or visit www.nfobgyn.com.

We apologize for any inconvenience or concern that this incident may have caused you. We take the confidentiality and security of personal information very seriously and will continue to take steps to help prevent a similar incident in the future.

Sincerely,

C. Cameron Greene, M.D.
Representative,
North Florida OB/GYN,
a division of Women's Care Florida

Enclosures

Y9852 v.01

PROTECTING DECEASED INDIVIDUALS

You may take certain steps, including the following, when a deceased or incapacitated loved one is affected by a data compromise incident.

Decrease the risk of their identity theft regardless of age by following these steps:

Obtain at least 12 copies of the official death certificate when it becomes available. In some cases you will be able to use a photocopy, but some businesses will request an original death certificate. Since many death records are public, a business may require more than just a death certificate as proof.

If there is a surviving spouse or other joint account holders, make sure to immediately notify relevant credit card companies, banks, stock brokers, loan/lien holders, and mortgage companies of the death. They may require a copy of the death certificate to do this, as well as permission from the survivor, or other authorized account holders.

The executor or surviving spouse will need to discuss all outstanding debts and how they will be dealt with. You will need to transfer the account to another person or close the account. If you close the account, ask them to list it as: "Closed. Account holder is deceased."

Contact all credit reporting agencies (CRAs) **(see contact information below)**, credit issuers, collection agencies, and any other financial institution that need to know of the death using the required procedures for each one. The following are general tips:

- Include the following information in all letters:
  - Name and SSN of deceased
  - Last known address
  - Last 5 years of addresses
  - Date of birth
  - Date of death
  - To speed up processing, include all requested documentation specific to that agency in the first letter
- Send the appropriate Court signed Executive papers.
- Send all mail certified, return receipt requested.
- Keep copies of all correspondence, noting date sent and any response(s) you receive.
- Request a copy of the decedent's credit report. A review of each report will let you know of any active credit accounts that still need to be closed, or any pending collection notices. Be sure to ask for all contact information on accounts currently open in the name of the deceased (credit granters, collection agencies, etc.) so that you can follow through with those entities.
- Request that the report is flagged with the following alert: "Deceased. **Do not** issue credit. If an application is made for credit, notify the following person(s) immediately: (list the next surviving relative, executor/trustee of the estate and/or local law enforcement agency- noting the relationship)."

Note: Friends, neighbors or distant relatives do not have the same rights as a spouse or executor of the estate. They are classified as a third party and a CRA may not mail out a credit report or change data on a consumer file upon their request. If you fall into this classification and are dealing with a very unique situation, you may write to the CRA and explain the situation. They are handled on a case-by-case basis. You may also apply to the courts to be named as an executor of the estate.

Other groups to notify:

- Social Security Administration
- Insurance companies – auto, health, life, etc.
- Veteran's Administration – if the person was a former member of the military
- Immigration Services – if the decedent is not a U.S. citizen
- Department of Motor Vehicles if the person had a driver's license or state ID card. Also make sure that any vehicle registration papers are transferred to the new owners.
- Agencies that may be involved due to professional licenses – bar association, medical licenses, cosmetician, etc.
- Any membership programs- video rental, public library, fitness club, etc.

Legal Notice: The information you obtain herein is not, nor intended to be, legal advice. We try to provide quality information but make no claims, promises or guarantees about the accuracy, completeness or adequacy of the information contained. As legal advice must be tailored to the specific circumstances of each case and laws are constantly changing, nothing provided herein should be used as a substitute for the advice of competent legal counsel.

Specific Credit Reporting Agencies (CRAs) information for ordering a credit report or placing a deceased flag:

Experian, P.O. Box 9701, Allen, TX 75013, 1-888-397-3742	
To order a credit report: A spouse can obtain a credit report by simply making the request through the regular channels – mail, phone and Internet. The spouse is legally entitled to the report. The executor of the estate can obtain a credit report but must write Experian with a specific request, a copy of the executor paperwork and the death certificate.	For requests or changes: A spouse or executor may change the file to show the person as deceased via written request. A copy of the death certificate and, in the case of the executor, the executor's paperwork must be included with the request. After any changes, Experian will send an updated credit report to the spouse or executor for confirmation that a deceased statement has been added to the credit report. This is important as executors and spouses can request other types of "changes" that we may not be able to honor. If identity theft is a stated concern, Experian will add a security alert after the file has been changed to reflect the person as deceased. If there are additional concerns, Experian will add a general statement to the file at the direction of the spouse/executor. The spouse/executor must state specifically what they want the general statement to say, such as "Do not issue credit."
Equifax Information Services LLC, Office of Consumer Affairs, P.O. Box 105139, Atlanta, GA 30348, 1-800-685-1111	
To order a credit report: Equifax requests that the spouse, attorney or executor of the estate submit a written request to receive a copy of the deceased consumer's file. The request should include the following: A copy of a notarized document stating that the requestor is authorized to handle the deceased consumer's affairs (i.e.: Order from a Probate Court or Letter of Testamentary)	For requests or changes: Equifax requests that a spouse, attorney or executor of the estate submit a written request if they would like to place a deceased indicator on the deceased consumer's file. The written request should include a copy of the consumer's death certificate. The request should be sent to the address listed above. Upon receipt of the death certificate, Equifax will attempt to locate a file for the deceased consumer and place a death notice on the consumer's file. In addition, Equifax will place a seven year promotional block on the deceased consumer's file. Once Equifax's research is complete, they will send a response back to the spouse, attorney, or executor of the estate.

TransUnion, P.O. Box 6790, Fullerton, CA 92834, 1-800-888-4213	
To order a credit report: TransUnion requires proof of a power of attorney, executor of estate, conservatorship or other legal document giving the requestor the legal right to obtain a copy of the decedent's credit file. If the requestor was married to the deceased and the address for which the credit file is being mailed to is contained on the decedent's credit file, then TransUnion will mail a credit file to the surviving spouse. If the deceased is a minor child of the requestor, TransUnion will mail a credit file to the parent upon receipt of a copy of the birth certificate or death certificate naming the parent as requestor.	For requests or changes: Placing a "deceased alert" on reports: TransUnion will accept a request to place a temporary alert on the credit file of a deceased individual from any consumer who makes such a request and identifies themselves as having a right to do so. The requestor's phone number is added to the temporary, three month alert. Upon receipt of a verifiable death certificate, TransUnion will entirely suppress the decedent's credit file and so note it as a deceased consumer. TransUnion will not mail out a copy of its contents without the requirements mentioned above. If you suspect fraud, TransUnion suggests a call to their fraud unit at 800-680-7289. It will place the temporary alert over the phone and advise the requestor of what needs to be sent to suppress the credit file and to disclose a copy of its contents. Requests can also be emailed to fvad@transunion.com.