Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

25909

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

[redacted]

[redacted]

Dear Representative of the Estate of [redacted]:

We are writing with important information regarding a recent security incident. The privacy and security of the personal information we maintain is of the utmost importance to Radius Financial Group. We wanted to provide you with information about the incident and let you know that we continue to take significant measures to protect the decedent's personal information.

Upon learning of the incident, which occurred on or about July 7, 2021, we immediately commenced an investigation. In addition to a thorough forensic examination, our investigation also included an extensive manual document review exercise. Our investigation concluded on January 7, 2022 that the incident impacted the decedent's [redacted]

This letter provides precautionary measures you can take to protect the decedent's personal information, including placing a "deceased alert" on the decedent's credit files. Additionally, you should always remain vigilant in reviewing the estate's financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of personal information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [redacted]. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, 9 a.m. to 9 p.m. Eastern.

Sincerely,

Radius Financial Group

– OTHER IMPORTANT INFORMATION –

1. Protecting Deceased Individuals

1. Notification of Death

The following steps are recommended for all deaths, regardless of age. It is best to notify all entities by telephone but such notifications **must** be followed-up in writing. Mail all correspondence certified, return receipt requested. Keep photocopies of all correspondence, including letters that you send.

1) 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.
2) Immediately contact the credit reporting agencies (CRAs) in writing and request a "deceased" alert be placed on their credit report. You should also request a copy of the credit report.
3) Contact all credit issuers, collection agencies, the CRAs and any other financial institutions that need to know of the death using the required procedures for each one. Include the following information on 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 all mail certified, return receipt requested. Keep copies of all correspondence, noting date sent and any response(s) you receive.
   Contact each of the CRAs. 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 grantors, 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)*."
   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.

2. Specific Instructions from the 3 Credit Reporting Agencies

A. Experian
P.O. 9701
Allen, TX 75013

Ordering reports

- □ 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.

Requesting changes or voicing concerns

- □ 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 spouse can request other types of "changes" that we may not be able to honor.
- □ If ID 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."

B. Equifax
P.O. Box 105139 Atlanta, GA 30348

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 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.

C. TransUnion (TU)
P.O. Box 2000 Chester, PA 19016

Ordering reports

- TU 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 TU will mail a credit file to the surviving spouse.
- If the deceased is a minor child of the requestor, TU 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.

Requesting changes or voicing concerns
- Placing a "deceased alert" on reports: TU 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, TU will entirely suppress the decedent's credit file and so note it as a deceased consumer.
- TU will not mail out a copy of its contents without the requirements mentioned above.

If you suspect fraud, TU 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**.

3. Addressing Suspected Fraud

In the event the estate suspects that the decedent's information has been misused, the estate can take the following steps:
- Request a copy of the decedent's credit report as outlined above.
- Place a "deceased alert" on the report as outlined above.
- Notify the police in the decedent's jurisdiction if you have evidence of fraud (collection notice, bills, credit report). A suspicion (especially of identity theft by a family member) is best when backed with concrete evidence.
- Notify any creditor, collection agency, credit issuer, utility company that the person is deceased and date of death. Be sure to include a copy of the death certificate. Request an immediate investigation and that they contact you with the results of the investigation. Insist on letters of clearance, which you should keep with the other estate papers.

In the event that the thief is a family member or relative, if the family is unable to decide on a course of action, it may be best to seek the advice of an attorney that specializes in estate or family law.

If this notice letter states that the decedent's financial account information was impacted, we recommend that you contact the financial institution to inquire about steps to take to protect the account, including whether you should close the account or obtain a new account number.

Protecting the Decedent's Medical Information

If this notice letter states that the decedent's medical information was impacted, the following practices can help to protect the decedent from medical identity theft.

- Only share the decedent's health insurance cards with the decedent's health care providers and other family members who are covered under the decedent's insurance plan or who helped the decedent with medical care.
- Review the decedent's "explanation of benefits statement" which you receive from the decedent's health insurance company. Follow up with the decedent's insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask the decedent's insurance company for a current year-to-date report of all services paid for the decedent as a beneficiary. Follow up with the insurance company or the care provider for any items you do not recognize.

Massachusetts Residents: Under Massachusetts law, you have the right to 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.

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

[redacted]

[redacted]

Dear [redacted]:

We are writing with important information regarding a recent security incident. The privacy and security of the personal information we maintain is of the utmost importance to Radius Financial Group. We wanted to provide you with information about the incident and let you know that we continue to take significant measures to protect your personal information.

Upon learning of the incident, which occurred on or about July 7, 2021, we immediately commenced an investigation. In addition to a thorough forensic examination, our investigation also included an extensive manual document review exercise. Our investigation concluded on January 7, 2022 that the incident impacted your [redacted]

This letter provides precautionary measures you can take to protect your personal information, including placing a Fraud Alert and Security Freeze on your credit files, and obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [redacted]. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, 9 a.m. to 9 p.m. Eastern.

Sincerely,

Radius Financial Group

– OTHER IMPORTANT INFORMATION –

1. Placing a Fraud Alert on Your Credit File.

We recommend that you place an initial one-year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
(800) 525-6285

Experian
P.O. Box 9554
Allen, TX 75013
https://www.experian.com/fraud/center.html
(888) 397-3742

TransUnion LLC
P.O. Box 6790
Fullerton, PA 92834-6790
https://www.transunion.com/fraud-alerts
(800) 680-7289

2. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-freeze/
(800) 349-9960

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
http://experian.com/freeze
(888) 397-3742

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19016
https://www.transunion.com/credit-freeze
(888) 909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

3. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

4. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If this notice letter states that your financial account information and/or credit or debit card information was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number.

Massachusetts Residents: Under Massachusetts law, you have the right to 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.