

[Date]

To the Family of (Name)
(Address)
(Address)
(City), (State) (Zip)

RE: Notice of Data Incident

To the Family of (Name):

Summit Reinsurance Services, Inc. (“Summit”) is writing to inform you of a data security event that may affect the security of your loved one’s personal information and to provide you with information on how to better protect against the possible misuse of this information. Summit has your loved one’s information because we provide underwriting and consulting reinsurance services to certain insurance companies.

What Happened? On August 8, 2016, Summit discovered that ransomware had infected a server containing certain personal information. Summit immediately launched an investigation to determine the nature and scope of this event and to prevent the encryption of data contained on the server. Summit also began working with third-party forensic investigators to assist with these efforts. While our forensic investigation is ongoing, it appears that the unauthorized access to the server first occurred on March 12, 2016. To date, Summit has no direct evidence that such data has been used inappropriately.

What Information Was Involved? The information contained on the affected server may have included your loved one’s name, Social Security number, health insurance information, provider’s name, and/or claim-focused medical records containing diagnosis and clinical information.

What Are We Doing? We take the security of information in our care very seriously. Although the forensic investigation is ongoing, to date, we have found no direct evidence of actual or attempted misuse of personal information on the affected server as a result of this incident. Nevertheless, in an abundance of caution, we are notifying you of this incident. Additionally, we have notified your loved one’s insurance company.

We are also providing you with information on how to better protect against the misuse of this information. You can find more information and steps you can take in the enclosed *Steps You Can Take to Prevent Identity Theft and Fraud*.

We are committed to the security of the information in our system and we have worked, and will continue to work, to enhance the protections in place to protect data in our care.

What Can You Do? You can review the enclosed *Steps You Can Take to Prevent Identity Theft and Fraud* for more information on ways to protect against the potential misuse of personal information.

For More Information. Again, we take the security of sensitive information in our care very seriously and we regret any concern or inconvenience this incident may cause you. We understand you may have questions that are not addressed in this notice. If you have additional questions, please call our dedicated assistance line at (877) 215-9747, Monday through Friday, 9 a.m. to 7 p.m. EST (closed on U.S. observed holidays) and provide Reference Number 2996113016 when calling.

Sincerely,

A handwritten signature in cursive script that reads "Mark Troutman".

Mark Troutman
President

STEPS YOU CAN TAKE TO PREVENT IDENTITY THEFT AND FRAUD

We encourage everyone to remain vigilant against incidents of identity theft and financial loss by:

- **Reviewing account statements, medical bills, and health insurance statements** regularly for suspicious activity, to ensure that no one submitted fraudulent medical claims using your loved one's name and address. Report all suspicious or fraudulent charges to your loved one's account and insurance providers.
- **Contacting the IRS at www.irs.gov** to request a PIN to file your taxes, so that no one can use your loved one's information to submit a fraudulent tax return.
- **Protecting your loved one's credit file.** Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus so long as you verify your authorization to make such a request on behalf of your loved one. To order this one free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of this credit report. We recommend contacting the three credit reporting agencies listed below to discuss your particular situation and obtain specific guidance. Once you establish a relationship with the credit reporting agency and verify your authorization to make a request on behalf of your loved one, you can request a copy of your loved one's credit report. A review of the credit 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 on your loved one's name (credit grantors, collection agencies, etc.) so that you can follow through with these entities.
- **Requesting, in writing, that the credit report list the following alert:**

"Deceased. Do not issue credit. If an application is made for credit, notify the following person(s) immediately [list yourself, and/or another authorized relative, and/or executor/trustee of the estate—noting the relationship of any individual listed to your family member—and/or a law enforcement agency]."

In most cases, this flag will prevent the opening of new credit accounts in your loved one's name. Contact information for the three major credit bureaus is as follows:

Equifax
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19016
800-680-7289
www.transunion.com

- **Educating yourself further** on identity theft, fraud alerts, and the steps you can take to protect against identity theft and fraud by contacting the Federal Trade Commission or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also

encourages those who discover that their information has been misused to file a complaint with them.

- **Reporting instances of known or suspected identity theft and fraud** to the FTC, local law enforcement, or your state Attorney General.

The mailing of this notice was not delayed by law enforcement.

State-Specific Information

Rhode Island residents:

- Have a right to file and obtain a police report. If the police report is then provided to a credit bureau, it cannot charge you to place, lift, or remove a security freeze.
- Have the right to know that, to date, **XXXX** Rhode Island residents have been identified as potentially affected by this incident.
- May contact the RI Attorney General's Office at (401) 274-4400, <http://www.riag.ri.gov/>, or 150 South Main Street, Providence, RI 02903.

North Carolina residents:

- May contact the NC Attorney General's Office, Consumer Protection Division, at 1-877-566-7226, www.ncdoj.com, or 9001 Mail Service Center, Raleigh, NC 27699.

Maryland residents:

- May contact the MD Attorney General's Office, General Consumer Protection Division, at 1-888-743-0023, www.oag.state.md.us, or 200 St. Paul Place, Baltimore, MD 21202.

Puerto Rican residents:

- Have the right to know that, to date, **XXXX** Puerto Rican residents have been identified as potentially affected by this incident.