Trinidad Navarro
Insurance Commissioner

Delaware Department of Insurance

For Immediate Release

Contact: Vince Ryan
Office: (302) 674-7303
Mobile: (302) 387-7670
Email: vince.ryan@state.de.us

19,000 Delaware Consumers Affected by Data Breach

DOVER, DE (January 13, 2017)— As a result of multiple consumer complaints, the Delaware Department of Insurance has been made aware of a security breach, involving Summit Reinsurance Services, Inc. ("SummitRe") and BCS Financial Corporation, both subcontractors of Highmark Blue Cross Blue Shield of Delaware. The breach affects thousands of Delawareans with employer-paid plans. As reported by Karen Kane, Director of Privacy and Information Management for Highmark Blue Cross Blue Shield of Delaware, the breach impacts a total of sixteen current and former Highmark self-insured customers and approximately 19,000 of their members. In response, Commissioner Navarro issued the following statement:

"We are aware of the reported breach. I would like to ensure Delaware consumers that the Department of Insurance takes this matter seriously and is currently investigating how this occurred. I have directed my staff to closely monitor the situation as it develops. Many Delawareans have received mailed correspondence frpom SummitRe explaining the breach (*See Attachment*). Unfortunately, we fear that many may have misinterpreted or inadvertently discarded the letter as some form of a sales ad (due to the fact that they had not purchased any line of insurance from SummitRe). If consumers have received a letter from SummitRe regarding this situation and have questions, they may contact the Delaware Department of Insurance at 1-800-282-8611 or 302-674-7300, or by e-mail at DOI_Consumer_Resource@state.de.us."

The Commissioner has ordered an investigation into the reported breach. Highmark Blue Cross Blue Shield of Delaware is cooperating with the Delaware Department of Insurance to resolve the matter.

###

SummitRe
Return Mail Processing
P.O. Box 205
Claysburg, PA 16625-0205

[redacted]

10034

[redacted]

January 4, 2017

RE: Notice of Data Incident

Dear [redacted]

Summit Reinsurance Services, Inc. ("Summit") is writing to inform you of a data security event that may affect the security of your personal information and to provide you with information on how to better protect against the possible misuse of your information. Summit has your 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 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 insurance company.

We are also providing you with information you can use to better protect against identity theft and fraud, as well as access to one year of credit monitoring and identity restoration services at no cost to you. You can find more information and steps you can take, as well as information on how to enroll in the credit monitoring services, in the enclosed *Steps You Can Take to Prevent Identity Theft and Fraud*.

STEPS YOU CAN TAKE TO PREVENT IDENTITY THEFT AND FRAUD

10034

To help you further safeguard against any potential misuse of your personal information, we are offering you access to one (1) year of **complimentary** membership in Experian's® ProtectMyID® Alert. This product helps detect possible misuse of your personal information and provides you with identity protection support focused on immediate identification and resolution of identity theft. To enroll, please follow the instructions below:

Activate ProtectMyID Now in Three Easy Steps

1. **ENSURE That You Enroll By: March 31, 2017** (Your code will not work after this date.)
2. **VISIT the ProtectMyID Web Site to enroll: www.protectmyid.com/alert**
3. **PROVIDE Your Activation Code: PABWARUJE**

If you have questions or need an alternative to enrolling online, please call (877) 297-7780 and provide engagement #: **PC105331**. A credit card is not required for enrollment. Once your ProtectMyID membership is activated, you will receive the following features:

- **Free copy of your Experian credit report**
- **Surveillance Alerts for: Daily Bureau Credit Monitoring:** Alerts of key changes & suspicious activity found on your Experian credit report.
- **Identity Theft Resolution & ProtectMyID ExtendCARE:** Toll-free access to US-based customer care and a dedicated Identity Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies. It is recognized that identity theft can happen months and even years after a data breach. To offer added protection, you will receive ExtendCARE™, which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **$1 Million Identity Theft Insurance[1]:** Immediately covers certain costs, including lost wages, private investigator fees, and unauthorized electronic fund transfers.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports and explanation of benefits forms for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your 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 your credit report.

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

[1] Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). 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.

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft, and you provide the credit bureau with a valid police report, it cannot charge you to place, list or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	Experian Security Freeze	TransUnion
P.O. Box 105788	P.O. Box 9554	PO Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
1-800-685-1111	1-888-397-3742	1-888-909-8872
www.equifax.com/help/credit-freeze/en_cp	www.experian.com/freeze/center.html	www.transunion.com/securityfreeze

In order to request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence. Fees vary based on where you live, but commonly range from $5 to $10.

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, 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. Instances of known or suspected identity theft should also be reported to 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, 0 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.

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 your information. You can also enroll to receive the credit monitoring and identity restoration services we are offering at no cost.

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,

Mark Troutman
President