SMITH & DOWNEY
A PROFESSIONAL ASSOCIATION
3801 PGA BLVD
SUITE 600
PALM BEACH GARDENS, FL 33410
(561) 337-5391
FAX: (561) 337-5201
http://www.smithdowney.com

HOWARD S. KIRKPATRICK
Of Counsel

E-mail: hkirkpatrick@smithdowney.com

Baltimore
New York
Washington, D.C.
Charleston
Sarasota

April 6, 2019

VIA US MAIL AND EMAIL

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301
attorneygeneral@doj.nh.gov

RE: Notice of Data Security Incident

Dear Attorney General MacDonald:

We represent the Main Street America Group ("MSA") in connection with a recent data security incident relating to the NGM Insurance Company Pension Share Account (the "Plan"), a retirement plan sponsored by MSA, that may affect New Hampshire residents as described in detail below. MSA reserves the right to supplement this notice with additional facts. This notice does not waive any rights or defenses that MSA or the Plan may have regarding the applicability of New Hampshire law, the New Hampshire data event notification statute, or personal jurisdiction.

I. Nature of the Security Incident

On or about September 22, 2018, SEI Private Trust Company ("SPTC"), the Plan's third-party pension payment administrator, updated its web-based reporting tool that allows SPTC's customers, institutional retirement plan sponsors and their third-party administrators, to view their plan and participant disbursement payments and generate reports with participant information necessary to administer their plans.

On or about November 29, 2018, SPTC discovered a software coding error in this web-based reporting tool that allowed eleven (11) of its customers' employees to view and generate a report with Plan information, including the names and social security numbers of Plan participants and retirees.

II. Number of New Hampshire Residents Affected

MSA notified one hundred seventy (170) New Hampshire residents about this data security incident by letter dated March 2019, delivered by first-class mail. A sample of the letter is enclosed.

III. Steps Taken to Remedy the Incident

In response to this incident, SPTC immediately disabled the web-based reporting tool that allowed its customers to view Plan information and conducted an internal investigation to determine exactly how and why this error occurred. The investigation identified the internal software coding error responsible for this data security incident and SPTC rolled out a correction for the error on or about November 29, 2018. SPTC also is creating a knowledge-based tracking system to detail the existing data security and functional security features of this tool and will review and upgrade baseline deployment standards as necessary for the remediation effort.

SPTC's investigation also determined that the software coding error did not result from a malicious attack by external parties and that this data security incident presents a very low risk of identity theft, fraud or other harm to the affected persons because the only SPTC customers who gained access to the Plan's confidential information were employees of retirement plan sponsors or their third-party administrators authorized to access confidential information on SPTC's system and who do so routinely during the course of their employment with fiduciary obligations to protect such information under federal law.

As an extra measure of security, SPTC obtained written certifications from each of its customers that accessed the Plan's information where they represented, under the pains and penalties of perjury, that they did not download, copy, distribute or otherwise misuse any of the Plan's confidential information and that they destroyed any and all copies of the information.

Finally, MSA notified all persons potentially affected by this data security incident in writing, and at MSA's request, SPTC agreed to provide all potentially affected persons with a one-year membership to Experian's® ProtectMyID® Alert to protect them from identity theft and fraud.

As sponsor of the Plan, MSA has communicated extensively with SPTC on this issue and has monitored SPTC's remedial actions to ensure that this kind of security incident does not happen again.

IV. Contact Information

If you have any questions or if you would like additional information, please feel free to contact me.

Sincerely,

Howard S. Kirkpatrick /cc

Howard S. Kirkpatrick

Enclosures

SEI Private Trust Company

1 Freedom Valley Drive
P.O. Box 1100
Oaks, PA 19456
T 610 676 1000
seic.com

March 2019

Notice of Breach of Confidential Information Regarding the NGM Insurance Company Pension Share Account

Dear Pensioner:

NGM Insurance Company Pension Share Account (the Plan) utilizes SEI Private Trust Company (SPTC) to provide payment services to the Plan such as pension payments and income tax withholding. We are writing to notify you about a breach of the Plan's confidential information as a result of a system enhancement. Set forth below is the reason this breach occurred, the steps that have been taken to ensure this never occurs again and an offer of free credit monitoring for one-year to give you peace of mind that your confidential information is not being misused.

SPTC uses software programs and systems to provide these payment services to the Plan and these systems require updates from time-to-time. During a recent update to our benefit payment system, a coding error occurred that resulted in some of our other customers (employer sponsors of retirement plans) being able to view the Plan's confidential information relating to participants, including names and social security numbers.

Upon discovering this error, we informed the Plan that we took the following steps to ensure the confidentiality of this information:

- Immediately disabled the report that allowed our other customers to view the Plan's confidential information;
- Conducted an internal investigation to determine exactly how and why this error occurred;
- Identified exactly how and why this error occurred and took the necessary steps to correct it; and
- Contacted all of our customers that received the Plan's confidential information and obtained a written certification from each client and authorized user stating they did not download, copy, distribute or otherwise misuse any of the Plan's confidential information and that they destroyed any and all copies of the information.

We have communicated extensively with the Plan on this issue, including a review of our explanation of the error and our actions to ensure this never happens again. We have assured the Plan that this incident presents a very low risk of harm to you as it was not the result of a malicious attack by hackers, but was caused by an internal software coding error and the

information was able to be viewed only by a limited number of our authorized customers sponsoring retirement plans, just like NGM Insurance.

Despite the very low risk of harm to you, as a sign of SPTC's and the Plan's commitment to protecting confidential information, we have agreed to offer all Plan participants a one-year membership to Experian's® ProtectMyID® Alert, a product that helps detect misuse of personal information and provides you with identity protection.

To take advantage of this offer, please follow the steps below:

- To activate your membership, go to: https://www.experianidworks.com/3bcredit
- Enter your engagement number: [redacted]
- Enter your Activation Code: [redacted]
- Toll-free number for enrollments/questions is 877-890-9332
- Enrollment end date: 4/30/2019

We apologize for this issue and hope that this information will provide reassurance that we take your security seriously and hold ourselves to a high standard to maintain your trust.

If you have additional questions, please contact SEI Benefit Payment Services directly at 888-734-8922.