



Seyfarth Shaw LLP
233 South Wacker Drive
Suite 8000
Chicago, Illinois 60606-6448
T (312) 460-5000
F (312) 460-7000

scarlson@seyfarth.com
T (312) 460-5946

July 7, 2022

VIA FIRST CLASS MAIL

Office of the Attorney General
Department of Justice
Consumer Protection Bureau
33 Capital Street
Concord, NH 03301

RECEIVED

JUL 11 2022

CONSUMER PROTECTION

RE: Notice of Data Incident

Dear Sir or Madam:

We represent BMS CAT, Inc. ("BMS"), a fire, water, and storm damage restoration and reconstruction service company. BMS is located at 5718 Airport Freeway, Haltom City, Texas 76117. We are writing to notify you on behalf of our client of a data security incident that potentially affected the personal information of residents of New Hampshire. This notice may be supplemented upon any further investigation. By providing this notice, BMS does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the relevant state statute, or personal jurisdiction.

Background: BMS first became aware of a potential security incident on February 25, 2022, when it discovered ransomware encryption on company systems. The threat actor identified themselves as part of the Conti Group. An IT forensic services firm was retained to determine the nature and scope of the ransomware attack. By March 11, 2022, the forensic analysis was complete and revealed that the threat actor gained access to the BMS system on February 22, 2022, and likely exfiltrated files that potentially contained personal information. However, the forensic analysis was not able to precisely determine what files were exfiltrated. BMS engaged in negotiations with the threat actor and after making a ransom payment, was able to obtain a decryption key as well as a file listing of exfiltrated data. Thereafter, BMS located on their systems the files that corresponded to the file listing and amounted to approximately 104 GB of diverse information. Between March 24 and April 1, 2022, BMS sent the 104 GB of data, which included over 395,000 individual files for document review. By April 24, 2022, the review revealed 2,149 documents that may have included personal information. However, the initial document review demonstrated that the type of personal information was very diverse and, in the majority of cases, there was no address/residency information. The next issue was trying to determine how to contact the affected individuals. In mid-May, 2022, BMS was able to utilize an Experian service to locate an address based upon an SSN. This resulted in locating 544 individuals. At this point BMS attempted to locate address information for all employees, former employees, applicants, and any other address information to locate other individuals. This resulted in a list of 40,200 individuals with address/residency information, allowing a data analyst to cross reference with potentially affected individuals. The efforts to identify address/residency information was ultimately completed on June 23, 2022. At that point, BMS became aware that New Hampshire residents were affected.



The personal information that may have been impacted for New Hampshire residents may include one or more of the following: full name, address, social security number, identification number, tax identification number, passport number, date of birth, bank account number, debit or credit card numbers, or personal health information.

Upon discovery of the incident, BMS responded quickly to minimize any impacts. After successful restoration and updating of systems, BMS began installing endpoint detection on its systems to monitor the environment for re-compromise and infection. BMS is also implementing policies and procedures regarding privileged access management, complex passwords, multi-factor authentication, email filtering, data loss prevention, and other improvements to the company's cybersecurity program. BMS has been in contact with the FBI regarding this incident.

Notice to New Hampshire Residents: We have determined that the number of New Hampshire residents potentially affected by this security incident is eight (8). BMS mailed notice to impacted individuals on July 7, 2022. Written notice to individuals was provided in substantially the same form as the letter attached here as **Exhibit A**. Please note that we reserve the right to update the draft letter.

Other Steps Taken and To Be Taken: BMS is taking action to provide assistance to potentially affected individuals, even though it currently has no evidence of any misuse of or fraudulent activity relating to anyone's personal information as a result of this incident. BMS is providing individuals whose personal information was potentially affected by this incident with access to credit monitoring services for 24 months through Experian at no cost to the individuals.

Additionally, BMS is providing impacted individuals with guidance on how to better protect against identity theft and fraud. These measures include advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Our client is also providing individuals with information on how to place a fraud alert and security freeze on their credit file, information on protecting against fraud, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information: Should you have any questions regarding this notification or other aspects of the data security incident, please contact us at (312) 460-5946 or scarlson@seyfarth.com.

Very truly yours,

SEYFARTH SHAW LLP

/s/ Scott A. Carlson

Scott A. Carlson

SC/dr

BMS CAT, Inc.
Return Mail Processing
PO Box 999
Suwanee, GA 30024

1 1 1 *****AUTO**MIXED AADC 300
SAMPLE A. SAMPLE - L01



APT ABC
123 ANY ST
ANYTOWN, US 12345-6789



July 7, 2022

RE: Important Security Notification. Please read this entire letter.

Dear Sample A. Sample:

Notice of Data Breach

What Happened: We are writing to notify you that BMS CAT, Inc. ("the Company") experienced an incident that may affect your personal information. On February 25, 2022, the Company initially discovered the incident and began its investigation. Following the initial discovery, the Company hired a forensic expert to investigate the event and uncover any potential impact on personal information. On March 11, 2022, the forensic analysis revealed that the attackers had exfiltrated some files from the Company that potentially contained personal information. The files required individual human review to determine the nature of information and affected individuals.

What Information Was Involved: We have conducted a thorough investigation to determine what personal information might have been impacted. Impacted personal information for affected individuals may include one or more of the following:

- Full Name
- Address
- Social Security Number
- Identification Number
- Tax Identification Number
- Passport Number
- Date of Birth
- Bank Account Number
- Debit or Credit Card Numbers
- Personal Health Information

What We Are Doing: We regret that this incident occurred and take the security of our information very seriously. Upon discovery of the incident, the Company responded quickly to minimize any impacts. After successful restoration and updating of systems, the Company began installing endpoint detection on its systems to monitor the environment for re-compromise and infection. We are also implementing policies and procedures regarding privileged access management, complex passwords, multi-factor authentication, email filtering, data loss prevention, and other improvements to the Company's cybersecurity program. We have been in contact with the FBI regarding this incident.



We are aware of the concern an incident such as this can create. Accordingly, we are offering you monitoring service for two years from the date of this letter. It also would be prudent to notify your bank and monitor your account activity in the event that anyone tries to access your accounts fraudulently.

In order to activate the credit monitoring service, please navigate to the following link:
www.experianidworks.com/credit

The engagement number for this service is Enrollment ends on **10/31/2022**.

Your activation code is:

If you have any questions, or would prefer to enroll over the phone, you may contact Experian at the following toll free number: (833) 671-0412. Please be prepared to provide engagement number **B055301**.

What You Can Do: Please remain vigilant by reviewing your account statements and monitoring credit report information. You can also obtain information about fraud alerts and security freezes from the FTC and the credit reporting agencies listed below:

- Federal Trade Commission, <https://www.ftc.gov>, 600 Pennsylvania Avenue, NW, Washington, DC 20580 1-877-FTC-HELP
- Nationwide Consumer Reporting Companies:
 - Equifax, <https://www.equifax.com>, Equifax Credit Information Services, LLC, P.O. Box 740241, Atlanta, GA 30374, 1-800-525-6285
 - Experian <https://www.experian.com>, Experian National Consumer Assistance Center, P.O. Box 4500, Allen, TX 75013, 1-888-397-3742
 - TransUnion <https://www.transunion.com>, TransUnion Consumer Relations, P.O. Box 2000, Chester, PA 19016-2000, 1-800-680-7289

To the extent you desire to freeze your credit report, you must separately place a credit freeze on your credit file at each of the three credit reporting agencies. There is no charge associated with placing a credit freeze. The following information should be included when requesting a credit freeze:

- 1) Full name, with middle initial and any suffixes;
- 2) Social Security number;
- 3) Date of birth (month, day, and year);
- 4) Current address and previous addresses for the past five (5) years;
- 5) Proof of current address, such as a current utility bill or telephone bill;
- 6) Other personal information as required by the applicable credit reporting agency.

For More Information: Please contact us if you have questions or require additional information about the incident.

Phone: (833) 671-0412

Sincerely,

BMS CAT, Inc.