



Aubrey Weaver, Partner
Cybersecurity & Data Privacy Team
1650 Market Street, Suite 3600
Philadelphia, Pennsylvania 19103
aweaver@constangy.com
Direct: 941.875.5335

August 23, 2023

VIA ONLINE SUBMISSION

Attorney General Aaron Frey
Office of the Attorney General
Consumer Protection Division
Security Breach Notification
111 Sewall Street, 6th Floor
Augusta, ME 04330

Re: Notice of Data Security Incident

Dear Attorney General Aaron Frey:

Constangy, Brooks, Smith & Prophete, LLP, represents Data Media Associates (“DMA”), a Georgia-based payment and value-added solutions provider serving the healthcare industry, in connection with a recent data security incident described in greater detail below. DMA takes the protection of all information within its possession very seriously and has taken measures to reduce the likelihood of a similar incident reoccurring. This notice is being sent on behalf of DMA, because personal information for Maine residents may have been involved in the incident.

1. Nature of the Security Incident

On June 4, 2023, DMA became aware of an alert issued by the Cybersecurity and Infrastructure Security Agency (“CISA”) addressing a critical vulnerability affecting the MOVEit secure file transfer solution, which is used widely by businesses and government agencies, including DMA, to securely transfer data. After becoming aware of the alert, DMA took immediate steps to patch its MOVEit system in accordance with the developer’s instructions. DMA thereafter undertook a comprehensive investigation with the assistance of leading external experts to learn more about the scope of any potentially affected data.

On June 30, 2023, DMA’s investigation revealed that certain data stored within MOVEit may have been acquired without authorization. Since that time, DMA has been working diligently to provide notice to its clients and gather information needed to provide notification to potentially affected individuals.

DMA continues to work through the process of notifying its clients and gathering additional information needed to provide individual notification. If additional Maine residents are identified at the conclusion of these efforts, DMA will provide an update to this letter.

2. Number of Maine Residents Involved

Beginning August 23, 2023, DMA notified 131 Maine residents of this data security incident via U.S. First-Class Mail pursuant to the Health Insurance Portability and Accountability Act of 1996. A sample copy of the notification letter sent to the impacted individuals is included with this correspondence.

The personal information involved in this incident includes individuals' names, addresses, and high-level medical or health insurance information such as would appear on billing statements, invoices, or other claims-related documents. In some instances, the involved data also included health insurance ID numbers, which DMA understands may be the same as individuals' Social Security numbers.

3. Steps Taken to Address the Incident

As soon as DMA discovered this unusual network activity, it took steps to secure the affected system and implemented all remediation measures recommended by the MOVEit software developer and launched an investigation to determine whether, and to what extent, individual information had been accessed or acquired without authorization. DMA is also evaluating additional safeguards that can be put in place to further enhance the security of the data entrusted to it.

DMA has established a toll-free call center through IDX to answer questions about the incident and address related concerns. In addition, DMA is offering twelve (12) months of complimentary credit and identity monitoring services to the potentially affected individuals whose Social Security number may have been used as a health insurance ID number.

4. Contact Information

DMA remains dedicated to protecting the information in its control. If you have any questions or need additional information, please do not hesitate to contact me at aweaver@constangy.com.

Sincerely,



Aubrey Weaver
Partner
Constangy, Brooks, Smith & Prophete, LLP

Enclosure: Sample Notification Letter



DATA MEDIA ASSOCIATES, LLC*

C/O Return Mail Processing Center
P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

Enrollment Code: <<Enrollment Code>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

August 23, 2023

Subject: Notice of Data <<Incident Type>>

Dear <<First Name>> <<Last Name>>,

Data Media Associates, LLC (“DMA”) is writing to inform you of a recent data security incident that may have affected your protected health information. DMA is one of an estimated 2,500 organizations worldwide recently affected by the MOVEit software vulnerability. If you are not familiar with DMA, we work with healthcare organizations<<, including CLIENTNAME>> to provide printing, mailing, and other healthcare billing fulfillment services. Please read this letter carefully, as it contains information regarding the incident and steps you can take to help protect your information.

What Happened? In June 2023, DMA became aware of an alert issued the same day by the Cybersecurity and Infrastructure Security Agency (“CISA”) addressing a critical vulnerability affecting MOVEit Transfer, a managed file transfer solution used widely by businesses and government agencies, including DMA, to securely transfer data. After becoming aware of the alert, DMA took immediate steps to patch its MOVEit system in accordance with the developer’s instructions. DMA thereafter undertook a comprehensive investigation with the assistance of leading external experts to learn more about the scope of any potentially affected data. Our investigation concluded on June 30, 2023, and revealed that certain data stored within MOVEit may have been acquired without authorization. Since that time, we have been working diligently to provide notice to our partner organizations and gather information needed to provide notification to potentially affected individuals.

What Information Was Involved? The information involved in this incident may have included your <<Variable 3: Data Elements>>. The information involved also included your health insurance ID number, which DMA understands may be the same as your Social Security number.

What We Are Doing. As soon as DMA discovered this incident, the above described steps were taken. We have taken all remediation measures recommended by the MOVEit software developers. DMA will also be evaluating additional safeguards that can be put in place to further enhance the security of the data entrusted to us.

In addition, we are offering identity theft protection services through IDX, A ZeroFox Company, a data breach and recovery services expert. IDX identity protection services include: <<12 months/24 months>> of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your information is compromised.

What You Can Do: You can follow the recommendations on the following page to help protect your protected health information. We also encourage you to enroll in the free identity protection services by calling (888) 979-0013, going to <https://app.idx.us/account-creation/protect>, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9:00 am to 9:00 pm Eastern Time. Please note the

deadline to enroll is November 23, 2023. You should also review your account statements and explanation of benefits forms and report any errors or activity you do not recognize to your insurance carrier.

For More Information: Further information on protecting your information appears on the following page. If you have questions about this issue, please call the dedicated call center for this incident at (888) 979-0013 from 9:00 AM to 9:00 PM Eastern Time, Monday through Friday (excluding holidays). Call center representatives are fully versed on this incident and can answer your questions.

DMA takes the privacy and security of individual information very seriously. Our sincerest apologies for any worry or inconvenience this may have caused you.

Sincerely,

Cleve Shultz

Cleve Shultz
CEO/President
Data Media Associates, LLC
1295 Old Alpharetta Road
Alpharetta, GA 30005

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and stays on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This prevents new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you, including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov
1-877-438-4338

New York Attorney General

Bureau of Internet and Technology Resources
28 Liberty Street
New York, NY 10005
ag.ny.gov
1-212-416-8433 / 1-800-771-7755

Maryland Attorney General

St. Paul Plaza
200 St. Paul Place
Baltimore, MD 21202
marylandattorneygeneral.gov
1-888-743-0023

Texas Attorney General

Bureau of Internet and Technology Resources
300 W. 15th Street
Austin, TX 78701
texasattorneygeneral.gov
1-800-621-0508

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
riag.ri.gov
1-401-274-4400

Virginia Attorney General

202 North Ninth Street
Richmond, VA 23219
oag.state.va.us
1-804-786-2071

**Washington D.C. Attorney
General**

400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA and your rights pursuant to the FCRA, visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

Personal Information of a Minor: You can request that each of the three national consumer reporting agencies perform a manual search for a minor's Social Security number to determine if there is an associated credit report. Copies of identifying information for the minor and parent/guardian may be required, including birth or adoption certificate, Social Security card, and government issued identification card. If a credit report exists, you should request a copy of the report and immediately report any fraudulent accounts to the consumer reporting agency. You can also report any misuse of a minor's information to the FTC at <https://www.identitytheft.gov/>. For more information about Child Identity Theft and instructions for requesting a manual Social Security number search, visit the FTC website: <https://www.consumer.ftc.gov/articles/0040-child-identity-theft>. Contact information for the three national credit reporting agencies is above.



DATA MEDIA ASSOCIATES, LLC®

C/O Return Mail Processing Center
P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

August 23, 2023

Subject: Notice of Data <<Incident Type>>

Dear <<First Name>> <<Last Name>>,

Data Media Associates, LLC (“DMA”) is writing to inform you of a recent data security incident that may have affected your protected health information. DMA is one of an estimated 2,500 organizations worldwide recently affected by the MOVEit software vulnerability. If you are not familiar with DMA, we work with healthcare organizations<<, including CLIENTNAME>> to provide printing, mailing, and other healthcare billing fulfillment services. Please read this letter carefully as it contains information regarding the incident and steps you can take to help protect your information.

What Happened? In June 2023, DMA became aware of an alert issued by the Cybersecurity and Infrastructure Security Agency (“CISA”) addressing a critical vulnerability affecting MOVEit Transfer, a managed file transfer solution used widely by businesses and government agencies, including DMA, to securely transfer data. After becoming aware of the alert, DMA took immediate steps to patch its MOVEit system in accordance with the developer’s instructions. DMA thereafter undertook a comprehensive investigation with the assistance of leading external experts to learn more about the scope of any potentially affected data. Our investigation concluded on June 30, 2023, and revealed that certain data stored within MOVEit may have been acquired without authorization. Since that time, we have been working diligently to provide notice to our partner organizations and gather information needed to provide notification to potentially affected individuals.

What Information Was Involved? The information involved in this incident may have included your <<Variable 3: Data Elements>>.

What We Are Doing. As soon as DMA discovered this incident, the above described steps were taken. We have taken all remediation measures recommended by the MOVEit software developers. DMA will also be evaluating additional safeguards that can be put in place to further enhance the security of the data entrusted to us.

What You Can Do: You can follow the recommendations on the following page to help protect your protected health information. You should also review your account statements and explanation of benefits forms and report any errors or activity you do not recognize to your insurance carrier.

For More Information: Further information on protecting your information appears on the following page. If you have questions about this issue, please call the dedicated call center for this incident at (888) 979-0013 from 9:00 AM to 9:00 PM Eastern Time, Monday through Friday (excluding holidays). Call center representatives are fully versed on this incident and can answer your questions.

DMA takes the privacy and security of individual information very seriously. Our sincerest apologies for any worry or inconvenience this may have caused you.

Sincerely,

Cleve Shultz

Cleve Shultz
CEO/President
Data Media Associates, LLC
1295 Old Alpharetta Road
Alpharetta, GA 30005

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and stays on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This prevents new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you, including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov
1-877-438-4338

New York Attorney General

Bureau of Internet and Technology Resources
28 Liberty Street
New York, NY 10005
ag.ny.gov
1-212-416-8433 / 1-800-771-7755

Maryland Attorney General

St. Paul Plaza
200 St. Paul Place
Baltimore, MD 21202
marylandattorneygeneral.gov
1-888-743-0023

Texas Attorney General

Bureau of Internet and Technology Resources
300 W. 15th Street
Austin, TX 78701
texasattorneygeneral.gov
1-800-621-0508

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
riag.ri.gov
1-401-274-4400

Virginia Attorney General

202 North Ninth Street
Richmond, VA 23219
oag.state.va.us
1-804-786-2071

**Washington D.C. Attorney
General**

400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA and your rights pursuant to the FCRA, visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

Personal Information of a Minor: You can request that each of the three national consumer reporting agencies perform a manual search for a minor's Social Security number to determine if there is an associated credit report. Copies of identifying information for the minor and parent/guardian may be required, including birth or adoption certificate, Social Security card, and government issued identification card. If a credit report exists, you should request a copy of the report and immediately report any fraudulent accounts to the consumer reporting agency. You can also report any misuse of a minor's information to the FTC at <https://www.identitytheft.gov/>. For more information about Child Identity Theft and instructions for requesting a manual Social Security number search, visit the FTC website: <https://www.consumer.ftc.gov/articles/0040-child-identity-theft>. Contact information for the three national credit reporting agencies is above.