



Freeman
Mathis & Gary LLP

1600 Market Street
Suite 1210
Philadelphia, PA 19103-7240

Tel: 267.758.6009

www.fmglaw.com

Robert H. Bender, Jr.
Senior Counsel
D: 215.650.6619
Robert.bender@fmglaw.com

September 1, 2023

VIA Email

Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

Subject: Notice of MoveIt Data Event

Dear Sir or Madam,

We represent Radius Global Solutions located at 7831 Glenroy Suite 250, Edina, MN 55439 and we write to notify your Office of 276 Maryland whose information may have been impacted by the MoveIt vulnerability exploitation event. Radius is a leading provider of integrated omnichannel customer engagement services and technology and this notice is provided on behalf of Radius and its respective clients. Radius reserves the right to supplement this notice if it subsequently learns any new significant facts. By providing this notification, Radius does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of Data Event

On June 1, 2023, Radius learned of a vulnerability in the MoveIt web transfer application that Radius utilizes for transferring documents with its clients and business partners. Upon learning cybercriminals exploited the vulnerability, Radius immediately investigated its MoveIt database to assess its security and to identify any documents that may have been accessed by unauthorized actors. After determining some documents were accessed between May 29, 2023 and May 30, 2023, Radius conducted a comprehensive review of the impacted files to determine what information was present in the impacted files and to whom the information related. Radius then worked with its clients to confirm contact information so it could notify applicable individuals, which continued through August 2, 2023. The impacted information included individual name, address, and Social Security number.

Notice to Maryland residents

On September 1, 2023, Radius provided written notice of this incident to 276 Maryland residents. Notice is being provided on behalf of Radius and its clients in substantially the same form as the letter attached as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon learning of the MoveIt vulnerability exploitation, Radius took prompt steps to investigation the scope of risk to information in the database. Radius reviewed impacted files and coordinated with its clients as necessary so it could notify applicable individuals. Radius also requested additional information from Progress Software to assess the nature of the vulnerability. Radius continues to ensure the security of its MoveIt application, including implementing new patches as available and assessing its policies and procedures.

Additionally, Radius is providing notified individuals access to complimentary identity monitoring services. Radius is also provided individuals with guidance on how to protect against identity theft and fraud, including information on how to place a fraud alert and/or security freeze, the contact details for the national consumer reporting bureaus, information on how to obtain a free credit report, a reminder to remain vigilant against possible identity theft and identify by reviewing account statements and free 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.

For Additional Information

If you have questions about this notification or the data security event, please contact us at 215-650-6619.

Very Truly Yours,

FREEMAN MATHIS & GARY, LLP

A handwritten signature in blue ink, reading "Robert H. Bender, Jr.", written in a cursive style.

Robert H. Bender, Jr.

Enclosures

Exhibit A



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Subject: Notice of Data Event

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Radius Global Solutions LLC is a leading provider of customer engagement and technology services on behalf of companies. We obtained your information from one of our business clients in connection with ongoing or past collection efforts. This letter is not sent in furtherance of those collection efforts. Rather, we are notifying you of a recent event involving the MOVEit web transfer application that may impact the privacy of your information. This letter provides a summary of the event, our response, and steps you can take to help protect your information, should you feel it appropriate to do so. We are also providing you with access to complimentary identity monitoring services at no cost. Activation instructions are included with this letter.

What Happened? On June 1, 2023, Radius learned of a vulnerability in the MOVEit web transfer application that Radius, along with several thousand other companies and government agencies, utilizes for transferring documents. Upon learning cybercriminals exploited the vulnerability, Radius immediately investigated its MOVEit database to assess its security and to identify any documents that may have been accessed by unauthorized actors. After determining some documents were accessed, Radius conducted a comprehensive review of the impacted files to determine what information was present in the impacted files, to whom the information related, and contact information for applicable individuals. We are notifying you because our review recently determined some of your information was present in the files accessible to the unauthorized actors due to the MOVEit vulnerability exploitation.

What Information Was Involved? The potentially impacted information included your <<b2b_text_1(name, data elements)>>.

What We Are Doing. Upon learning of the MOVEit vulnerability, we immediately investigated to determine any risk to information in the database. We promptly reviewed the identified documents so we could notify relevant individuals. We continue to implement necessary patching and measures to secure the MOVEit database as we learn new information. As an added precaution, we are offering you 24 months of complimentary identity monitoring services. Activation instructions are included on the following pages.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing account statements and monitoring free credit reports for suspicious activity and errors. We also encourage you to review the information contained in the *Steps You Can Take to Help Protect Information* section and to activate the complimentary identity monitoring services we are offering.

For More Information. If you have additional questions, please call our dedicated assistance line at [TFN](#), which is available from 9:00 AM to 6:30 PM Eastern Time Monday through Friday (excluding major U.S. holidays).

Sincerely,

Radius Global Solutions LLC

STEPS YOU CAN TAKE TO HELP PROTECT INFORMATION

Activate Complimentary Identity Monitoring Services

We have secured the services of Kroll to provide identity monitoring at no cost to you for two years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people whose information may be affected by a data incident. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until *<<b2b_text_6(activation deadline)>>* to activate your identity monitoring services.

Membership Number: *<<Membership Number s_n>>*

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Monitor Your Accounts

We recommend that you remain vigilant by reviewing personal account statements and monitoring credit reports to detect any errors or unauthorized activity. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call (877) 322-8228. You can also contact the three major credit reporting bureaus listed below to obtain a free copy of your credit report.

Consumers have the right to place a fraud alert on a credit file at no cost. A fraud alert tells businesses that check your credit that they should check with you before opening a new account and an initial alert lasts for one year with the option for an extended fraud alert for seven years. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. To place a fraud alert, contact the nationwide credit reporting agencies by phone or online. For more information, visit <https://www.consumer.ftc.gov/articles/0275-place-fraud-alert>.

As an alternative to a fraud alert, consumers have the right to place a free security freeze on a credit report. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can also get a free freeze for your children who are under 16, and if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too. To place a security freeze, contact the nationwide credit reporting agencies by phone or online. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets

your request. Under federal law, you cannot be charged to place or to lift the freeze. For more information, visit <https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs>. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as suffixes);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card;
7. A copy of any police report, investigative report, or complaint to law enforcement concerning identity theft if you are a victim of identity theft.

To place a fraud alert or credit freeze, please contact the three major consumer reporting bureaus:

Equifax
1-888-298-0045
P.O. Box 105069
Atlanta, GA 30348
www.equifax.com

Experian
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion
1-800-916-8800
P.O. Box 2000
Chester, PA 19016
www.transunion.com

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC, 20580; www.identitytheft.gov; 1-877-ID-THEFT; and TTY 1-866-653-4261. The Federal Trade Commission encourage those who discover their information has been misused to file a complaint. You can obtain additional information by way of the contact information above. You have the right to file a police report if you ever experience identity fraud. Please note that to file a crime report or incident report with law enforcement for identity theft, you may need to provide some proof that you have been a victim. You should report suspected incidents of identity theft to local law enforcement, your state's Attorney General, and/or the Federal Trade Commission. This notice has not been delayed by law enforcement.

Residents of the below states can obtain additional information about the steps you can take to avoid identity theft:

- ***District of Columbia residents:*** District of Columbia Attorney General, 400 6th Street, NW, Washington, DC 20001; oag@dc.gov; 202-727-3400.
- ***Maryland residents:*** Maryland Attorney General, 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; <https://www.marylandattorneygeneral.gov> or 1-410-528-8662 or 1-888-743-0023. Radius Global Solutions is located at 7831 Glenroy Suite 250, Edina, MN 55439.
- ***New Mexico residents:*** You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what information is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting bureaus may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to your employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have additional specific rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by contacting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf; Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave NW, Washington, DC 20580.
- ***New York residents:*** Office of the New York Attorney General, The Capitol, Albany, NY 12224-0341; <https://ag.ny.gov>; or 1-800-771-7755.
- ***North Carolina residents:*** North Carolina Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; <https://ncdoj.gov>; and toll-free at (877) 566-7226 or (919) 716-6000.

- ***Rhode Island residents:*** Rhode Island Attorney General, 150 South Main Street, Providence, RI 02903; www.riag.ri.gov or 401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in this matter. There are approximately [XX] Rhode Island residents potentially impacted by this incident.