



41 South High Street, Suite 1800
Columbus, OH 43215-6106
Tel: 614.221.2838
taftlaw.com

December 4, 2023

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

RE: BMW Financial Services NA, LLC

To Whom It May Concern,

Pursuant to applicable data security incident response laws, I am providing you notice of a data security incident on behalf of our client, BMW Financial Services NA, LLC ("BMW FS"). A copy of the notice to the affected residents is attached.

NAME AND CONTACT INFORMATION OF THE PERSON REPORTING THE BREACH

Mehmet Munur

Partner

mmunur@taftlaw.com

(614) 220-0253

41 S. High St., Suite 1800, Columbus, Ohio 43215

NAME AND ADDRESS OF BUSINESS WITH DATA BREACH; NAME OF DATA OWNER

BMW Financial Services NA, LLC, located at 1400 City View Dr. Columbus, Ohio 43215

DESCRIPTION OF THE BREACH AND REMEDIAL STEPS TAKEN IN RESPONSE

BMW Financial Services NA, LLC ("BMW FS") hereby provides a description of a data security incident it indirectly experienced due to a MOVEit software vulnerability that impacted one of its service providers. Please note that BMW FS' own systems and databases were not affected by this incident. BMW FS is in the process of notifying individuals, attorneys general, and other governmental entities in accordance with applicable law relating to this incident. We provide additional information below.

BMW FS obtains services from Ricoh USA, Inc. ("Rico") for scanning mail for BMW FS and sending it electronically to BMW FS. After becoming aware of the MOVEit vulnerability, BMW FS reached out to its service providers to determine if they used MOVEit. Ricoh confirmed to BMW FS on June 9, 2023, that it did not use MOVEit to provide BMW FS with its services.

Despite this communication on June 9th, on September 20, 2023, Ricoh notified BMW FS that some of the written communication sent to BMW FS from its customers via mail that had been scanned into Ricoh's systems may have been accessed in an unauthorized manner. Ricoh informed BMW FS that it had been informed of a zero-day vulnerability on June 1, 2023, patched its servers promptly, and worked with a forensics provider to determine the extent of its impact on Ricoh's own systems.

After its notification on September 20th, BMW FS began its own investigation, activated its incident response plan, and worked with Ricoh to determine the extent of the security incident and to analyze the information that may have been accessed. Ricoh notified BMW FS on November 9, 2023 that some personal information for BMW FS's customers had in fact been included in this unauthorized access. Based on this information, BMW FS decided to notify consumers on November 15, 2023. BMW FS is now in the process of notifying individuals and will be offering free credit monitoring.

In order to better protect its systems from similar security incidents, BMW FS requires that MOVEit no longer be associated with any processes for any services provided by Ricoh to BMW FS. Ricoh has also put in place additional safeguards and technical security measures to further protect and monitor its MOVEit environment.

BMW FS will continue to engage with its customers to assist them and answer questions they may have about the incident. BMW FS will continue to engage its service providers to attempt to investigate, review, and improve any data security practices and to reduce the likelihood of a recurrence of similar data security incidents.

STATE RESIDENTS AFFECTED BY THE BREACH

BMW FS's investigation identified 134 total individuals potentially impacted by the incident. Of those individuals, three (3) had a Maryland address that may have been impacted. In the event that BMW FS determines any additional Maryland residents are impacted, BMW FS will strive to update this notice accordingly.

CATEGORIES OF PERSONAL INFORMATION SUBJECT TO THE BREACH

The incident may have impacted the following categories of personal information (sent to BMW FS from its customers via mail that had been scanned into Ricoh's systems):

1. First and last name
2. Address
3. Date of birth
4. Driver's license number
5. Social Security number

NOTIFICATION TO AFFECTED STATE RESIDENTS

Residents will be notified of the breach on December 5, 2023.

Attached, please see a template copy of the notification that will be sent to residents via postal mail.

CREDIT MONITORING

Credit monitoring and identity theft prevention services will be offered via Equifax for 12 months.

December 4, 2023

Page 3 of 3

NO DELAY

BMW FS notes that this notice has not been delayed (due to any law enforcement investigation or for any other reason), nor is any delay to individual notifications anticipated.

Please let me know if you have any further questions.

Respectfully,

Mehmet Munur

Mehmet Munur



Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

[Name and Address of Recipient]

December 5, 2023

Re: Notice of Data Security Incident

Dear [Name of Recipient]:

Ricoh responded to a data security incident that involved some of your information. This letter explains the incident, the measures taken, and some steps you may consider taking in response. Your personal information was affected by this security incident because Ricoh was providing services for BMW Financial Services NA, LLC (“BMW FS”) that included scanning mail for BMW FS and sending it electronically to BMW FS. Please note that BMW FS’ own systems and databases were not impacted by this incident.

What Happened

On May 31, 2023, Progress Software Corporation, which developed and supports the MOVEIt managed file transfer platform, notified all customers, including Ricoh, of a vulnerability that an unauthorized party used to access and acquire data without authorization. Upon learning of the incident, Ricoh took immediate measures to secure its MOVEIt instance. Ricoh also conducted an investigation and determined that there was unauthorized access to and acquisition of Ricoh files in its MOVEIt instance.

On September 20, 2023, Ricoh notified BMW FS of the potential that some of the written communication sent to BMW FS had been accessed by an unauthorized third party. Ricoh confirmed with BMW FS on November 9th that personal information for its customers had been included in this unauthorized access. BMW FS decided to notify consumers on November 15th.

What Information Was Involved

Ricoh determined that files involved in the incident contained the following: [personal information categories involved].

What We Are Doing

Ricoh is notifying you so that you can take immediate action to protect yourself. Ensuring the safety of your data is of the utmost importance to Ricoh and BMW FS. To help prevent something like this from happening again, additional safeguards and technical security measures have been implemented to further protect and monitor the MOVEIt environment. Further, MOVEIt is no longer associated with any processes for any services provided by Ricoh to BMW FS.

What You Can Do

As a best practice, we recommend you remain vigilant and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities.

In response, Ricoh is offering you a complimentary one-year membership for Equifax Complete Premier credit monitoring and identify theft support. This product helps detect possible misuse of your personal information and provides you with identity protection support.

If you have concerns about identity theft, you can contact local law enforcement and file a police report. You can also contact your state's Attorney General, as well as the Federal Trade Commission or one of the credit bureaus for more information about how to protect your identity.

You have until March 30, 2024 to activate your identity monitoring services.

For More Information

Additional information about steps you can take, Equifax Complete Premier, and instructions on how to activate your complimentary one-year membership are included with this letter on the following pages.

We have established a dedicated call center to help answer frequently asked questions you may have about the incident. Please call 833-627-2806, Monday through Friday, between 9:00 a.m. and 9:00 p.m. Eastern Time for up-to-date information about the incident.

Sincerely,

Ricoh USA



[Recipient Name]
Enter your Activation Code: [Code]
Enrollment Deadline: March 30, 2024

Equifax Complete™ Premier

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Annual access to your 3-bureau credit report and VantageScore¹ credit scores
- Daily access to your Equifax credit report and 1-bureau VantageScore credit score
- 3-bureau credit monitoring² with email notifications of key changes to your credit reports
- WebScan notifications³ when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts⁴, which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock⁵
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to \$1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft⁶.
- Lost Wallet Assistance if your wallet is lost or stolen, and one-stop assistance in canceling and reissuing credit, debit and personal identification cards.

Enrollment Instructions

Go to www.equifax.com/activate

Enter your unique Activation Code of [code] then click “Submit” and follow these 4 steps:

1. **Register:**

Complete the form with your contact information and click “Continue”.

If you already have a myEquifax account, click the ‘Sign in here’ link under the “Let’s get started” header.

Once you have successfully signed in, you will skip to the Checkout Page in Step 4

2. **Create Account:**

Enter your email address, create a password, and accept the terms of use.

3. **Verify Identity:**

To enroll in your product, we will ask you to complete our identity verification process.

4. **Checkout:**

Upon successful verification of your identity, you will see the Checkout Page.

Click ‘Sign Me Up’ to finish enrolling.

You’re done!

The confirmation page shows your completed enrollment.

Click “View My Product” to access the product features.

¹The credit scores provided are based on the VantageScore® 3.0 model. For three-bureau VantageScore credit scores, data from Equifax®, Experian®, and TransUnion® are used respectively. Any one-bureau VantageScore uses Equifax data. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness. ²Credit monitoring from Experian and TransUnion will take several days to begin. ³WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded. ⁴The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC. ⁵Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.co ⁶The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877- IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two credit bureaus, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active-Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years unless you ask them not to do so.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Ricoh can be reached at 833-434-0750. Its mailing address is 300 Eagleview Boulevard, Exton, PA 19341.

Additional information for residents of the following states:

Connecticut: You may contact and obtain information from your state attorney general at: *Connecticut Attorney General's Office*, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318

District of Columbia Residents: You may contact the Attorney General for the District of Columbia for more information about how to protect your identity by using the *Attorney General's Office*, 400 6th Street, NW, Washington, DC 20001, 1-202-727-3400, <https://oag.dc.gov/>

Maryland: You may contact and obtain information from your state attorney general at: *Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-410-528-8662, www.marylandattorneygeneral.gov

New York: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov