



AIG
28 Liberty Street,
22nd Floor
New York, NY 10005-1445
www.aig.com

Steven R. Harris
Deputy General Counsel
T 212 458 2441
F 866 663 0580
steven.harris@aig.com

October 13, 2023

BY EMAIL

Office of the Attorney General
200 St. Paul Plaza
Baltimore, MD 21202
Idtheft@oag.state.md.us

To Whom It May Concern:

Pursuant to Md. Code Ann., Com. Law § 14-3504(h), American International Group, Inc. ("AIG") on behalf of its indirect wholly owned subsidiaries, AIU Insurance Company, American Home Assurance Company, National Union Fire Insurance Company of Pittsburgh, Pa., and New Hampshire Insurance Company (collectively, the "AIG Insurers") provides notice of a cybersecurity incident that occurred at Ricoh USA, Inc. on June 1, 2023 caused by the broadly publicized MOVEit zero-day vulnerability (the "Ricoch Security Incident" or "Incident"). To be clear, the Ricoch Security Incident did not impact AIG's own systems or network.

The Incident occurred at Ricoh, which provides mailroom services to vendors, and in some cases vendors of vendors, to three AIG third-party administrators ("TPAs"), Cannon Cochran Management Services, Inc. ("CCMSI"), Broadspire Services, Inc. and Sedgwick Claims Management Services, Inc. AIG's TPAs, through its vendors, provide Ricoh with AIG claims documents that contain claimant data for imaging and processing, in connection with claims administration. Ricoh's principal place of business is 300 Eagleview Boulevard, Exton PA, 19341.

As explained to AIG, on June 1, 2023, Ricoh was informed of the MOVEit zero-day vulnerability. Ricoh took immediate actions to address the vulnerability and initially determined that it did not impact its own systems. On July 10, 2023, after further investigation, Ricoh discovered that it had been a victim of the MOVEit zero-day vulnerability. Upon review of the affected data, Ricoh informed AIG's TPAs that it determined that certain AIG claimant data was affected by the Incident.

After receiving and reviewing the impacted data, on August 30, 2023, AIG determined that the personal information associated with 1 Maryland resident was affected by the Incident. AIG has determined that the affected information included: date of birth, diagnostic and/or treatment code, and health insurance policy number.

AIG anticipates that formal notice will be sent via U.S. Mail pursuant to Md. Code Ann., Com. Law § 14-3504(b)-(g). This notice was not delayed by a law enforcement investigation. A sample notification letter is enclosed. As stated in the attached sample notice, Ricoh is offering to provide individuals 12 months of free identity theft and credit monitoring services through Equifax. Ricoh has also established a call center to respond to individuals' questions.

AIG understands that Ricoh is among many companies impacted by the MOVEit vulnerability. To date, AIG has not received any reports of identity theft, fraud, or financial losses from the affected individuals.

AIG takes the protection of personal information very seriously and is committed to answering any questions that your office may have. Please do not hesitate to contact me at 212-458-2441 or steven.harris@aig.com.

Respectfully yours,

A handwritten signature in black ink, appearing to read "Steve Harris", is positioned below the "Respectfully yours," text.

Enclosure



<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>><<State>><<Zip>>

<<Date>>

Dear <<Name1>>:

Ricoh USA, Inc. ("Ricoh") provides workplace solutions and digital transformation services to help businesses manage optimization. Ricoh is providing notice of a data incident that may have involved some of your personal information. This letter explains the incident, how Ricoh is responding, and some steps you may consider taking in response.

On June 1, 2023, Progress Software Corporation, which developed and supports the MOVEIt managed file transfer software and platform ("MOVEIt"), notified all customers across the globe, including Ricoh, of a zero-day vulnerability in MOVEIt that could allow an unauthorized party to access systems using MOVEIt and acquire data from them. Ricoh uses MOVEIt and, upon learning of the MOVEIt vulnerability, Ricoh took immediate measures to secure its MOVEIt instance. Ricoh also conducted an investigation and determined that information in Ricoh's MOVEIt instance had been accessed and acquired by an unauthorized party.

Ricoh determined that the information involved in the incident includes your [insert data fields]. Ricoh had your information as a result of services it was providing to either your employer or some other entity to which you provided the information.

Ricoh is offering you a complimentary two-year membership for Equifax Credit Watch Gold credit monitoring and identify theft support. This service helps detect possible misuse of your personal information and provides you with identity protection support. Information about Equifax Credit Watch Gold and instructions on how to activate your complimentary two-year membership are included with this letter on the following page.

You have until <<Enrollment Deadline>> to activate your complimentary Equifax Credit Watch Gold service.

In addition, we have enclosed information about additional steps you may consider taking to protect your personal information.

To help prevent a similar future incident, Ricoh has implemented additional safeguards and technical security measures to protect and monitor the MOVEIt environment. We have established a dedicated call center to help answer your questions about the incident. Please call << number>>, Monday through Friday, between X:00 a.m. and X:00 p.m. <<time zone>> for up-to-date information about the incident.

Sincerely,

Ricoh USA



Enter your Activation Code: <<ACTIVATION>>

Equifax Credit Watch™ Gold

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

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications¹ 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 alerts², which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock³
- 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 theft⁴

Enrollment Instructions

Go to www.equifax.com/activate

Enter your unique Activation Code of **<<ACTIVATION 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.

¹WebScan 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. ²The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC. ³Locking 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.com ⁴The 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 **[Insert Phone Number]**.

Additional information for residents of the following states:

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 12244-0341, 1-800-771-7755, <https://ag.ny.gov>