

CRC Group
Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<Mail ID>>

<<Name 1>>

<<Name 2>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<Address 4>>

<<Address 5>>

<<City>><<State>><<Zip>>

<<Country>>

<<Date>>

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

Dear <<Name1>>:

We are writing to tell you about a security incident that may have exposed some of your personal information that we have in our possession because of our role as a wholesale insurance distributor. Specifically, we place insurance with a variety of insurance carriers at the request and on behalf of retail insurance agency clients.

Although we have no confirmation that your information was accessed or used by the unauthorized actor involved in the incident, we take the protection and proper use of your information very seriously. For this reason, we are contacting you directly to explain the circumstances of this incident and to inform you of actions you may take to protect yourself.

What Happened. On or about January 18, 2023, CRC Insurance Services, LLC (“CRC”) determined that through a series of phishing emails, an unknown third-party gained unauthorized access for a limited period of time to a small number of employee email accounts and exfiltrated a small percentage of emails in those accounts. CRC immediately activated its incident response team to secure the affected accounts and contain the incident.

What We Are Doing. In conjunction with the security and containment steps above, CRC took immediate steps to conduct a legal and technical investigation of the incident, including engagements with leading forensic and data analytics firms. Additionally, CRC sent timely alert communications to all its employees and provided additional training to CRC employees impacted by the phishing attack in this incident. The investigation noted above has now concluded, and we have no confirmation that your information was actually accessed, acquired, or used for any unauthorized purpose. However, the investigation could not rule out the possibility of a potential impact.

What Information Was Involved. As a result of the thorough forensic investigation and extensive data review noted above, we identified that some files on the impacted systems contained certain individual personal information. The information that may have been exposed could have included your name, address, <<Breached Elements>>. Again, we have no confirmation that your information was actually accessed or used by the unauthorized actor involved in the incident.

What You Can Do. We do not believe, and there are no facts to indicate, that this incident has resulted in a significant risk to you of identity theft or fraud. However, we recommend that you remain vigilant, review your account statements and credit reports regularly and report any concerns to your financial services provider. In addition, CRC is offering complementary credit monitoring services from Equifax for <<12/24>> months. Please see the attached for instructions on how to access those services.

For More Information. If you have any questions regarding this incident, please contact 1-888-828-7567 from 9:00 a.m. to 9:00 p.m., Monday through Friday, Eastern Time. Protecting your information is paramount to us and we hope that the services we are offering to you demonstrate our commitment in this regard.

Sincerely,

CRC Group



Enter your Activation Code: <<Activation Code>>
Enrollment Deadline: <<Enrollment Deadline>>

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 Information and U.S. State Notification Requirements

There are a number of steps you should consider to guard against identity theft.

Review Your Account Statements and Credit Report: It is recommended that you remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and monitoring your credit reports. Report any fraudulent transactions to the creditor or credit reporting agency from whom you received the statement or report. You may obtain a free copy of your credit report from each credit reporting agency once every 12 months, whether or not you suspect any unauthorized activity on your account, by visiting <https://www.annualcreditreport.com>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form available at that website and mailing it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also purchase a copy of your credit report at any time by contacting any one or more of the national credit reporting agencies listed below.

Equifax

P.O. Box 740241
Atlanta, Georgia 30374
www.equifax.com
1-800-685-1111 Credit Reports
1-888-766-0008 Fraud Alert
1-800-685-1111 Security Freeze

Experian

P.O. Box 2002
Allen, TX 75013
www.experian.com
1-888-397-3742 Credit Reports
1-888-397-3742 Fraud Alert
1-888-397-3742 Security Freeze

TransUnion (FVAD)

P.O. Box 105281
Atlanta, GA 30348-5281
www.transunion.com
1-800-888-4213 Credit Reports
1-800-680-7289 Fraud Alert
1-800-680-7289 Security Freeze

Federal Trade Commission (FTC) and State Resources: General guidance on protecting yourself from identify theft is available from the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Ave. NW, Washington D.C. 20580, by phone at 877-ID-THEFT (438-4338), and/or from the FTC website at <http://www.ftc.gov/bcp/edu/microsites/idtheft>. In many states, additional information is also available from your state's Attorney General's Office.

Fraud Alerts and Security Freezes: You may obtain information about fraud alerts and security freezes (also referred to as credit freezes), including how to place a fraud alert or security freeze, from the Federal Trade Commission or credit reporting agencies at the contact information provided above. However, be aware that a fraud alert or security freeze may require fees to be paid, may interfere with or delay legitimate requests for credit approval. You'll need to supply your name, address, date of birth, Social Security number and other personal information in order to place a security freeze on your credit.

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 (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

D.C.: You have the right to place a fraud alert or security freeze. For more information on how to place a fraud alert or security freeze, you can contact the Federal Trade Commission or any of the consumer reporting bureaus as described above. You can also contact the D.C. Attorney General at (202) 442-9828 or consumer.protection@dc.gov.

Iowa: You should report suspected incidents of identity theft to your local law enforcement or the Iowa Attorney General.

Maryland: For more information on steps you can take to prevent identity theft, you can contact the Federal Trade Commission or any of the consumer reporting bureaus as described above. You can also contact the Maryland Attorney General at 1-888-743-0023, Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, and <https://www.marylandattorneygeneral.gov>.

Massachusetts: State law advises you that you have the right to obtain a police report. You also will not be charged for seeking a security freeze, as described above in this document.

New Mexico: You have the right to place a fraud alert or security freeze. For more information on how to place a fraud alert or security freeze, you can contact the Federal Trade Commission or any of the consumer reporting bureaus as described above. You should review your personal account statements and credit reports, as applicable, to detect any errors that may or may not be a result of a security incident.

New York: The New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

North Carolina: For more information on steps you can take to prevent identity theft, you can contact the Federal Trade Commission or any of the consumer reporting bureaus as described above. You can also contact the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

Oregon: State law advises you to report any suspected identity theft to law enforcement, as well as the FTC.

Rhode Island: You can contact the Rhode Island Attorney General at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.