



Return Mail Processing Center  
P.O. Box 6336  
Portland, OR 97228-6336

<<MailID>>  
<<Name 1>>  
<<Name 2>>  
<<Address 1>>  
<<Address 2>>  
<<Address 3>>  
<<Address 4>>  
<<Address 5>>  
<<City>><<State>><<Zip>> <<Date>>  
<<Country>>

***RE: Notice of Data Breach  
Please read this entire letter.***

Dear <<Name 1>>:

We are contacting you regarding an incident that occurred at WESCO Distribution, Inc. (“WESCO”), which may affect the security of some of your personal information. Please be assured that we have taken appropriate steps to address the incident, as described below, and please note that we are not aware of any misuse of your personal information. This notice contains an explanation of the incident (including the relevant dates), a description of the personal information involved, the measures that we have taken in response (including to reduce the risk of harm), some additional steps you may consider taking and contact information for a person who can answer questions about the incident on WESCO’s behalf.

**What Happened:**

On July 1, 2019, we learned that a WESCO employee’s email account was compromised by an unknown actor. We then noticed suspicious activity occurring within certain email accounts and immediately launched an investigation to determine the nature and scope of the incident. From that investigation, we learned that an employee’s email account was compromised through a phishing email on August 15, 2018, which then spread to 28 other user accounts. Further, the unknown actor placed an automatic forwarding rule on the accounts, which forwarded all incoming emails to an unauthorized Gmail account. The rule was disabled on July 1, 2019 immediately upon our discovery of the compromise, and there was no further unauthorized disclosure of personal information in connection with this incident following such date. We then retained an expert consultant to launch an extensive, programmatic review of the contents of the potentially compromised records, followed by a manual review of the documents that the consultant flagged as potentially containing personal information. Due to the volume of emails and the manually intensive review, this process took several months to complete. After analyzing the contents of the emails, we have determined that some of your personal information may have been compromised.

### **What Information Was Involved:**

We determined that records containing the following types of information relating to you were impacted by this data compromise: **[Insert applicable PII]**.

### **What We Are Doing to Reduce Risks and Protect Your Information:**

As soon as we discovered what happened, we immediately took steps to contain the incident by changing the access credentials for the impacted accounts, and we further secured these accounts by disabling the auto-forwarding rule. We also enabled Microsoft's "conditional access" to our email system and are implementing multi-factor authentication to ensure greater security. Protecting the security of your information is of paramount importance to us, and we are continually taking steps to enhance the security of our systems and information.

### **What You Can Do:**

Again, at this time, we are not aware of any misuse of your personal information. However, given that your information was obtained by an unknown third party that intentionally accessed our systems without authorization, we are providing notice to you so that you can take steps to protect yourself. In particular, you should be cautious of phone calls or emails asking for any personal or confidential information, as well as emails with links or attachments that could contain malware.

We are also offering you a complimentary one-year enrollment in Equifax<sup>®</sup> Credit Watch<sup>™</sup> Gold with WebDetect, which includes credit monitoring and other services related to protecting against identity theft. For more information about Equifax<sup>®</sup> Credit Watch<sup>™</sup> Gold with WebDetect, please see the additional information that follows this letter. To activate your enrollment please ensure that you enroll by May 31, 2020 ("**Enrollment Deadline**"). Enrollment instructions are included in the materials that follow this letter. Please provide you **Activation Code: <INSERT ACTIVATION CODE>** when enrolling. Please note that your activation code will not work after the Enrollment Deadline listed above.

We encourage you to take advantage of these services we are offering you. Also, we have enclosed additional general information on how to protect your identity and your sensitive information.

It is important that you remain vigilant to identify and address any possible misuse of your personal information, especially over the next 12 to 24 months. If your personal information is misused or you suspect you are a victim of identity theft, please report the incident to WESCO and law enforcement authorities. You may also contact an Equifax identity restoration specialist, who will work on your behalf to help you restore your identity. To be eligible for identity restoration services, you must complete the enrollment process for the subscription offer by the Enrollment Date listed above. Equifax's phone number for assistance will be listed in your online member center available to you after you complete the enrollment process.

We sincerely apologize for this incident and regret any inconvenience it may cause you. Should you have questions or concerns regarding this matter, please do not hesitate to contact our dedicated assistance line at **<Insert Equifax Call Center Number>**. Assistance is available **Monday to Friday 9 am – 9 pm Eastern (6 am to 6 pm Pacific)**.

Sincerely,

WESCO Distribution, Inc.

## For More Information

### Protecting your identity

- We remind you it is always advisable to remain vigilant for incidents of fraud and identity theft and review your personal account statements and credit reports to detect any errors that may result from this incident. You may place a fraud alert on your credit file by contacting the fraud departments of the three nationwide credit reporting agencies, which prompts any issuer of credit to use additional scrutiny for any request for new or increased credit. This provides a significant layer of protection; however, it may limit your ability to get “instant credit” such as the offers often available at retail stores.
- Check your credit report to ensure all your information is correct. You can obtain a free credit report from each of the nationwide consumer credit reporting agencies every 12 months by visiting [www.annualcreditreport.com](http://www.annualcreditreport.com) or calling 1-877-322-8228. You may want to obtain copies of your credit report to ensure the accuracy of the report information. When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report.
- If you believe you are a victim of identity theft, report it to your local law enforcement and to the FTC (see their contact information below) or your state Attorney General and one of the three nationwide consumer reporting agencies listed below to have it removed from your credit file.
- For more information about steps to take to avoid identity theft, including requesting fraud alerts, security freezes, or credit reports, contact:

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

Equifax:  
1-800-349-9960 or  
[www.equifax.com](http://www.equifax.com)  
P.O. Box 105788  
Atlanta, GA 30348

Experian:  
1-888-397-3742 or  
[www.experian.com](http://www.experian.com)  
P.O. Box 9554  
Allen, TX 75013

TransUnion:  
1-800-680-7289 or  
[www.transunion.com](http://www.transunion.com)  
P.O. Box 160  
Woodlyn, PA 19094

- Learn more about steps you can take to protect against identity theft from the Federal Trade Commission at [www.consumer.ftc.gov/topics/identity-theft](http://www.consumer.ftc.gov/topics/identity-theft). Or call the FTC’s Identity Theft Hotline toll-free at 1-877-IDTHEFT (1-877-439-4339)
- If you are a resident of Maryland, New York or North Carolina, you may contact and obtain information from your state attorney general or state agency at:

Maryland Attorney General’s Office, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023/ 1-410-576-6300, [www.oag.state.md.us](http://www.oag.state.md.us).

New York Attorney General’s Office Bureau of Internet and Technology (212) 416-8433, <https://ag.ny.gov/internet/resource-center>

NYS Department of State's Division of Consumer Protection (800) 697-1220, <https://www.dos.ny.gov/consumerprotection>

North Carolina Attorney General’s Office, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6400/ 1-877-566-7226, [www.ncdoj.gov](http://www.ncdoj.gov).

Enrollment  
Details

## ADDITIONAL DETAILS REGARDING YOUR ENROLLMENT OFFER

### Product Information

#### **Equifax® Credit Watch™ Gold with WebDetect Features**

- Equifax® credit file monitoring and alerts to key changes to your Equifax credit report
- Wireless alerts (available online only). Data charges may apply.
- Access to your Equifax credit report
- Internet Scanning<sup>1</sup> Monitors suspicious web sites for your Social Security, Passport, Credit Card, Bank, and Insurance Policy Numbers, and alerts you if your private information is found there.
- Automatic Fraud Alerts<sup>2</sup> with a fraud alert, potential lenders are encouraged to take extra steps to verify your ID before extending credit
- Up to \$25,000 Identity Theft Insurance<sup>3</sup>
- Live agent Customer Service 7 days a week from 8 a.m. to 3 a.m.

### Enrollment Instructions

To sign up online for online delivery go to [http://myservices.equifax.com/efx1\\_bresngis](http://myservices.equifax.com/efx1_bresngis)

**1. Welcome Page:** Enter the Activation Code provided on page 2 of this letter in the “Activation Code” box and click the “Submit” button.

**2. Register:** Complete the form with your contact information (name, gender, home address, date of birth, Social Security Number and telephone number) and click the “Continue” button.

**3. Create Account:** Complete the form with your email address, create a User Name and Password, check the box to accept the Terms of Use and click the “Continue” button.

**4. Verify ID:** The system will then ask you up to four security questions to verify your identity. Please answer the questions and click the “Submit Order” button.

**5. Order Confirmation:** This page shows you your completed enrollment. Please click the “View My Product” button to access the product features.

### Identity Restoration

If you become a victim of identity theft, an Equifax identity restoration specialist will work on your behalf to help you restore your identity. To be eligible for Identity

<sup>1</sup> Internet scanning, will scan for your Social Security number (if you choose to), up to 5 bank account numbers, up to 6 credit/debit card numbers you provide, up to 3 email addresses, up to 10 medical ID numbers, and up to 5 passport numbers. Internet scanning scans thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and is constantly adding new sites to 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 Internet scanning is able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.

<sup>2</sup> The Automatic Fraud Alert feature made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC

<sup>3</sup> Identity theft insurance is underwritten by American Bankers Insurance Company of Florida or its affiliates. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions and exclusions of coverage. Coverage may not be available in all jurisdictions.

	<p>Restoration, you must complete the enrollment process for the subscription offer by the enrollment deadline above. Call the phone number listed in your online member center for assistance.</p>
Fair Credit Reporting Act	<p>The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. Here is a summary of your major rights under FCRA. For more information, including about additional rights, go to <a href="http://www.consumerfinance.gov/learnmore">www.consumerfinance.gov/learnmore</a> or write to: Consumer Financial Protection Bureau, 1700 G. Street NW, Washington, DC 20552.</p> <ul style="list-style-type: none"><li>• You must be told if information in your file has been used against you.</li><li>• You have the right to know what is in your file.</li><li>• You have the right to ask for a credit score.</li><li>• You have the right to dispute incomplete or inaccurate information.</li><li>• Consumer reporting agencies must correct or delete inaccurate, incomplete or unverifiable information.</li><li>• Consumer reporting agencies may not report outdated negative information.</li><li>• Access to your file is limited.</li><li>• You must give your consent for reports to be provided to employers.</li><li>• You may limit “prescreened” offers of credit and insurance you get based on information in your credit report.</li><li>• You have the right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.</li><li>• You may seek damages from violators.</li><li>• Identity theft victims and active duty military personnel have additional rights.</li></ul>