



WESCO Distribution, Inc.
225 W. Station Square Dr.
Pittsburgh, PA 15219
October 22, 2024

Via e-mail

Office of the Attorney General
Attn: Security Breach Notification
Idtheft@oag.state.md.us

To Whom It May Concern:

I represent WESCO Distribution, Inc. ("Wesco"), and I am writing on Wesco's behalf to notify your office of an incident that affects the security of personal information relating to two Maryland residents.

On August 13, 2024, Wesco learned that an employee's e-mail account was compromised by an unknown actor. Wesco immediately launched an investigation utilizing a third-party firm to determine the nature and scope of the incident. From that investigation, Wesco learned that an employee's e-mail account was compromised through a phishing e-mail from a Wesco business partner on August 8, 2024. Further, the unknown actor synced the mailbox in question to create a copy of the mailbox.

Wesco has performed the following activities to remove the third party's access from the environment:

- Reset the user's password
- Revoked all active Microsoft 365 sessions
- Validated any multi-factor authentication devices as appropriate

At this time, Wesco and its outside investigator believe that the third party's access to the email account has been remediated, and there is no evidence of ongoing activity within the Wesco network.

These incident-specific responsive measures are in addition to the security measures Wesco already has in place. Wesco uses ProofPoint as its e-mail security provider, which provides e-mail filtering, attempts to prevent e-mail phishing, and removes malware attachments. This tool blocks threats before they reach Wesco's environment, protects thousands of individual mailboxes from attacks, has the ability to quickly respond to zero-day threats, manages spam and quarantine messages in a cloud platform, re-writes links so that as soon as maliciousness is identified, all clicks from that point forward are blocked, and inserts the word [EXTERNAL] on message from outside the company. Finally, Wesco uses Microsoft's security center's recommended best practices.



Additionally, Wesco conducts periodic trainings on information security, requires its employees to acknowledge relevant cybersecurity policies, and engages in simulated phishing attacks to test employees. Any employee who falls for such a simulated attack is required to undergo further training. Lastly, as a result of this incident, Wesco has strengthened existing multi-factor authentication practices to make it more difficult for threat actors to access Wesco's environment—even if an employee is tricked into providing their credentials.

The categories of personal information varied based on the e-mail content and attachments that were comprised, but for the Maryland residents, the compromised records contained passport information.

The one resident of Maryland whose information was affected by this incident will soon receive written notification via mail pursuant to Md. Code Ann. Comm. Law 14-3504. Wesco will e-mail this notification to the Maryland resident on or about October 23, 2024. A template copy of the letter is attached hereto as Exhibit A.

If you have any questions about this situation, please do not hesitate to contact me at (219) 765-7986.

Sincerely,

Brandon Thompson
Senior Counsel
bthompson@wescodist.com



wesco

WESCO Distribution, Inc.
225 W. Station Square Dr.
Pittsburgh, PA 15219
October 23, 2024

[Recipient's Name]
[Recipient's Address]
[City, State, Zip Code]

Dear [Recipient's Name],

We are writing to inform you of a recent incident that may have impacted your personal information. On August 8, 2024, we discovered that an unauthorized individual gained access to an email account in our system that contained personal information.

Upon discovery of the incident, we immediately took steps to secure the affected account and have initiated an investigation to determine the scope of the incident. We wanted to inform you of the situation out of an abundance of caution.

As a precautionary measure and to protect against potential identity theft, we recommend you:

1. Monitor your financial accounts for any suspicious activity.
2. Monitor your free credit report for any suspicious activity.
3. Consider placing a fraud alert or security freeze on your credit file with major credit reporting agencies.

Additionally, on the following page we have provided resources that you can use to obtain information about steps that you can take to avoid identity theft.

We sincerely regret any concern or inconvenience this incident may cause. Protecting the privacy and security of your personal information is of the utmost importance to us, and we are taking every step to prevent this from happening in the future.

Should you have any questions or require additional information, please do not hesitate to contact our dedicated response team at me at the address below.

Sincerely,

Brandon Thompson
Senior Counsel
bthompson@wescodist.com



wesco

Major Credit Reporting Agencies

Experian
475 Anton Blvd.
Costa Mesa, CA 92626
1-888-397-3742

Equifax
P.O. Box 740241
Atlanta, GA 30348
1-888-378-4329

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

Federal Government Resources

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-382-4357
<https://consumer.ftc.gov/features/identity-theft>

For residents of Maryland only:

Maryland Attorney General Attorney General's Identity Theft Unit
200 St. Paul Place, 25th Floor
Baltimore, MD 21202
1-888-743-0023
idtheft@oag.state.md.us
<https://www.marylandattorneygeneral.gov/pages/identitytheft/default.aspx>

For residents of North Carolina only:

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
1-877-566-7226
<https://ncdoj.gov/protecting-consumers/protecting-your-identity/>