**Appendix**

Barracuda Networks provides enterprise security, networking, and storage appliances and services to organizations worldwide. Wescom utilized Barracuda’s Email Security Gateway (ESG) appliance for email security. Barracuda recently identified a vulnerability in the ESG, patched vulnerable systems, and issued an alert to customers who used the ESG appliance. On May 30, 2023, Wescom’s IT team identified evidence that the vulnerability was potentially exploited by an unauthorized person prior to its identification by Barracuda.

Wescom immediately launched an investigation to determine whether any data stored in or passing through the ESG appliance had been accessed by an unauthorized person. The investigation determined that the ESG had been accessed and that some emails and attachments stored on the appliances between October 30, 2022, and May 30, 2023, were potentially at risk. The investigation could not determine which emails and attachments stored on the appliances were accessed or acquired.

Wescom reviewed the contents of the emails and attachments that were potentially accessible to the unauthorized person for personal information. On September 18, 2023, Wescom determined that one or more emails or attachments stored on the ESG appliances included the name, financial account number, Social Security number, and/or driver’s license number of eleven (11) Maine residents.

On October 20, 2023, Wescom mailed notification letters via United States Postal Service First-Class mail to the individuals whose information was involved, including the Maine residents pursuant to Me. Rev. Stat. Tit. 10, §1348[[1]](#footnote-1). A copy of the notification is enclosed. Wescom has established a dedicated call center for individuals to call with questions about the incident.

To help prevent a similar incident from occurring in the future, Wescom has discontinued the use of the ESG appliances.

1. This report does not waive Wescom’s objection that Maine lacks personal jurisdiction over Wescom related to this matter. [↑](#footnote-ref-1)