RON WYDEN
OREGON

RANKING MEMBER OF COMMITTEE ON FINANCE

221 DIRKSEN SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-5244

United States Senate
WASHINGTON, DC 20510-3703

COMMITTEES:
COMMITTEE ON FINANCE
COMMITTEE ON BUDGET
COMMITTEE ON ENERGY & NATURAL RESOURCES
SELECT COMMITTEE ON INTELLIGENCE
JOINT COMMITTEE ON TAXATION

August 5, 2019

Mr. Jeff Bezos
Chief Executive Officer
Amazon, Inc.
410 Terry Avenue North
Seattle, WA 98109

Dear Mr. Bezos:

I write to better understand how default configuration settings for Amazon's cloud computing products may have contributed to recent data breaches of servers used by Capital One Financial Corporation ("Capital One") and several other large organizations.

On July 29, Capital One revealed that its systems had been breached, and that personal data on 100 million Americans had been stolen. A criminal complaint filed by the Federal Bureau of Investigation (FBI) alleged that, due to a firewall misconfiguration, a hacker was able to access sensitive data stored on servers rented by Capital One from a cloud computing company. While the name of that cloud computing service is not named in the complaint, Amazon revealed that it provides cloud computing services for Capital One in a marketing document published on Amazon's website.

According to media reports, Ford Motor Company, the Ohio Department of Transportation, Michigan State University, and the Italian bank UniCredit SpA are all investigating possible related breaches impacting their own organizations.

When a major corporation loses data on a hundred million Americans because of a configuration error, attention naturally focuses on that corporation's cybersecurity practices. However, if several organizations all make similar configuration errors, it is time to ask whether the underlying technology needs to be made safer, and whether the company that makes it shares responsibility for the breaches.

With more than a million active customers, Amazon is one of the largest cloud computing providers in the world. If Amazon's cloud computing services are found to be the common element in a series of high-profile hacks targeting large corporations, it would raise serious questions about whether other corporations and government entities that use Amazon's cloud computing products are also vulnerable. To that end, please provide me with answers to the following questions about the security of Amazon's cloud computing products by August 13, 2019:

1. A number of cybersecurity experts have publicly speculated that the Capital One hacker exploited a Server-Side Request Forgery (SSRF) vulnerability, a flaw about which experts have been warning for years. To the best of Amazon's knowledge, was a SSRF attack used to gain access to Capital One's customer data?
2. During the past two years, how many of Amazon's customers were compromised through SSRF attacks against their Amazon cloud computing servers? How many of these breaches involved Amazon's metadata service?
3. What guidance, if any, has Amazon provided to its cloud computing customers about the potential for SSRF attacks, particularly against Amazon's metadata service, and how such attacks can be identified and mitigated?
4. According to a July 31, 2019 tweet from a senior security software engineer at Netflix, a major customer of Amazon's cloud computing services, the company previously asked Amazon to add a security header to protect Amazon's metadata service from SSRF attacks. According to that Netflix engineer's public tweet, which has since been deleted, Netflix did not get "a satisfactory response." Please confirm whether or not Amazon in-fact received a request from Netflix to add such a security protection and describe what steps, if any, Amazon took after receiving this feature request.

Thank you for your prompt attention to this important matter. If you have any questions about this request, please contact Chris Soghoian in my office.

Sincerely,

Ron Wyden
United States Senator