

United States Senate

WASHINGTON, DC 20510

June 5, 2019

Stephen H. Rusckowski
Chairman, President & CEO
Quest Diagnostics
500 Plaza Drive
Secaucus, NJ 07094

Dear Mr. Rusckowski:

We write in response to reports that there has been an eight months-long data breach involving Quest Diagnostics's partner, the American Medical Collection Agency (AMCA). We are deeply concerned that this breach compromised the personal, financial, and medical information of nearly 12 million Quest Diagnostics Inc. patients.

As the nation's largest blood testing provider, this data breach places the information of millions of patients at risk. The months-long leak leaves sensitive personal information vulnerable in the hands of criminal enterprises. Moreover, such breaches force victims to contend with identity theft that may lead to irreparable harm to their credit reports and financial futures, and to confront the real possibility that their confidential medical information and history has been exposed.

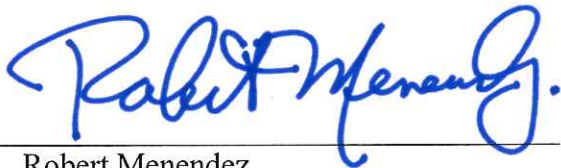
We need to understand exactly how this breach happened and how it impacts patients. We must also ensure that entities with access to patients' personal, medical, and financial information understand their role in protecting patients and are taking both immediate and longer-term steps to mitigate this harm. In light of these concerns, we ask that you please provide responses to the following:

1. Provide a detailed timeline of the breach, including when it began, its discovery, any investigation of its scope and source, notification to authorities, efforts to notify patients, and notification to Quest Diagnostics's senior executives.
2. Please describe Quest Diagnostics's efforts to identify the scope of affected patients and breadth of information compromised.
3. What steps has Quest Diagnostics taken to identify and limit potential patient harm associated with this breach?
4. Does Quest Diagnostics plan to provide notice to each affected consumer, or will it rely on a consumer-initiated checks to inform them?

5. Does Quest Diagnostics have procedures in place to receive and act on vulnerability reports?
 - a. If so, please describe these procedures, when they were implemented, and how frequently the company acts to remediate vulnerabilities.
 - b. When Quest Diagnostics was first notified of a potential breach by AMCA on May 14, 2019, what immediate steps did it take to protect patient's information?
6. What processes does Quest Diagnostics have in place to ensure that the companies it outsources patient information to responsibly protect their patients' information?
7. What new processes will Quest Diagnostics implement to better monitor the information and data security of the companies to which it outsources patient information?
8. Please explain how the breach persisted for eight months without awareness from Quest Diagnostics?
9. Please describe the resources that Quest Diagnostics dedicates to information and data security.
 - a. Does Quest Diagnostics employ a Chief Information Security officer? If so, to whom does this person report?
 - b. Is anyone at Quest Diagnostics responsible for evaluating the information and data security of the companies and to which it outsources patient information?
 - c. How many full-time employees at Quest Diagnostics focus on information and data security?
10. During the past eight months of the breach, how many times has Quest Diagnostics conducted a security test which evaluates both Quest Diagnostics's systems as well as the systems of any companies it outsources to?

We request that Quest Diagnostics respond to this request no later than June 14, 2019. Thank you for your prompt attention to this important issue.

Sincerely,



Robert Menendez
United States Senator



Cory A. Booker
United States Senator