Congress of the United States
Washington, DC 20515

September 26, 2017

The Honorable Jay Clayton
Chairman
U.S. Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549

Dear Chairman Clayton:

As members of the House Financial Services Committee, we write in regard to your statement from September 20, 2017, regarding cybersecurity and the U.S. Securities and Exchange Commission's (SEC) Electronic Data Gathering, Analysis, and Retrieval (EDGAR) system.

According to your statement, a "software vulnerability" in the EDGAR system was exploited and led to the unauthorized access of nonpublic information. This raises serious concerns for all market participants regarding the fairness of the capital markets and the security and accuracy of information stored on the EDGAR system.

As you know, the EDGAR system is the central location in which companies must file SEC registration statements, periodic reports, and other required forms. In total, the system receives and processes approximately 1.7 million filings each year. Given the amount of information filed, disseminated, and stored through the system, the EDGAR system maintains an important role in the capital markets by increasing efficiency and fairness for all investors and companies while promoting transparency. However, the system only benefits all market participants when market participants are assured that the information contained on the system is properly safeguarded and that the underlying reports are accurate.

In light of this cybersecurity breach, we request that you provide us answers to the following questions:

1. When was the software vulnerability discovered and what steps did the SEC take to address this particular vulnerability?
2. When did the SEC learn of potentially illicit trades using the information accessed through the software vulnerability? Please provide us with an overview of the potentially illicit trading activity, including the size and scope of the trades and number of companies involved.
3. What types of information and/or filings were accessed through this software vulnerability?
4. How many companies' filings and/or data were improperly accessed through this breach?

PRINTED ON RECYCLED PAPER

5. Has the SEC notified companies and shareholders affected by the unauthorized access of information? If not, does the SEC plan to do so and when?
6. While you state that the SEC does not currently believe the breach resulted in the unauthorized access of personally identifiable information (PII) of investors, this is not guaranteed in future breaches. What steps does the SEC plan to take to ensure individuals' identities are protected in the future?
7. What steps, if any, does the SEC plan to take to better address cybersecurity vulnerabilities in the EDGAR system?

Cybersecurity is a growing threat in the financial services industry, and we look forward to working with you to better address cyber vulnerabilities moving forward. Thank you in advance for your timely responses to our questions.

Sincerely,

John K. Delaney

Maxine Waters

Carolyn B. Maloney

Josh Gottheimer

David Scott

Nydia M. Velázquez

Juan Vargas

Brad Sherman

Kyrsten Sinema

James A. Himes

Wm. Lacy Clay

Ed Perlmutter

Gregory W. Meeks

Joyce Beatty

Vicente Gonzalez

Stephen F. Lynch

Gwen Moore

Al Green

Ruben J. Kihuen

Keith Ellison

Daniel T. Kildee

Charlie Crist