DAVID PERDUE
GEORGIA

United States Senate

October 4, 2017

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

Dear Chairman Clayton,

We write to you today to express concerns with the implementation of the Consolidated Audit Trail ("CAT") as part of the National Market System ("NMS"). In light of the recent revelation of a cyber breach of the Securities and Exchange Commission's ("SEC") Electronic Data Gathering, Analysis, and Retrieval ("EDGAR") filing system, we urge the Commission to delay the reporting and collection of data under the CAT NMS Plan until a full investigation can be conducted and proper countermeasures taken. Furthermore, we hope you will reexamine and possibly scale the amount of personally identifiable information ("PII") collected and kept in the CAT database.

We support the creation of the CAT NMS Plan because it represents a step forward for both the supervision of the capital markets and consolidation of the current fragmented and duplicative financial regulatory reporting. However, over the past few years, our nation has endured successful cyber-attacks on government computer systems at the Federal Deposit Insurance Corporation, the Internal Revenue Service, the Federal Reserve, and the Office of Personnel Management. Beyond the federal government, the recent revelation of the theft of over 143 million Americans' PII from Equifax brings into focus the importance of cybersecurity for any organization that oversees the wholesale collection and storage of sensitive information.

In your recent statement on Cybersecurity,[1] we appreciate your earnest efforts to "promote effective cybersecurity practices." As you've stated "when determining when and how to collect data, it is important that we regularly review whether our related data projections are appropriate in light of the sensitivity of the data and the association risks of unauthorized access."[2] We wholeheartedly agree with that statement and therefore hope that you will review the implementation of the CAT NMS Plan and the severe consequences that could result from a breach of the CAT database.

Less than a year ago, Chinese hackers penetrated the servers of several prominent U.S. law firms including Cravath, Swaine & Moore and Weil Gotshal & Manges.[3] Using non-public information on mergers & acquisitions, these hackers were able to earn more than $4 million in illegal profits before the authorities put a stop to the illegal actions. While it is too early to assess the damage caused by the penetration of EDGAR, the SEC has admitted that rogue traders may have used the non-public data from EDGAR to make illicit trading profits similar to how hackers exploited the information at the U.S law firms.[4]

---

[1] https://www.sec.gov/news/public-statement/statement-clayton-2017-09-20#_ftnref3
[2] *Id.*
[3] https://www.wsj.com/articles/u-s-charges-three-chinese-traders-with-hacking-law-firms-1482862000
[4] https://www.ft.com/content/f5292994-9f09-11e7-8cd4-932067fbf946

455 Russell Senate Office Building
Washington, DC 20510

3280 Peachtree Road, NE, STE 2640
Atlanta, GA 30305

We stress the hacking of the law firms and the EDGAR breach because the CAT NMS Plan is a far more comprehensive database in comparison to either of the aforementioned databases that have been breached and if there were a significant hacking, the culprits would have access to the crown jewels of the U.S capital markets. In the most extreme case, the detailed information found within the CAT database could be used to reconstruct the closely guarded trading algorithms of Wall Streets' most prominent hedge funds. Even a minor breach would give unauthorized parties' access to market moving information that could be exploited for criminal gain.

According to the FAQs on the CAT NMS Plan, there will be 3,000 authorized users with access to the CAT database.[5] The CAT NMS Plan recognizes the risks of a potential breach and established rigorous standards for every authorized user of the CAT database, all authorized users except SEC staff who are specifically exempted from the rigorous requirements. Recently, we read that the Department of Homeland Security detected five "critical" cyber security weaknesses on the SEC's computers dating back to January 23rd.[6] We recognize this problem predates your term at the SEC, but we want to highlight the past two GAO reports regarding the SEC's control over financial systems and data. Over the past year the SEC has made attempts to close the identified cybersecurity gaps, but much work is still left to be done and therefore we are forced to question the ability for the SEC to adhere to the very standards it imposes on external parties.[7] Issues such as the SEC not always sufficiently restricting access to financial systems, not fully encrypting sensitive information, and not fully implementing an intrusion detection capability on key financial systems highlight actionable items the SEC would find unacceptable if these were found in a supervisee firm.

We understand that you were only sworn into office this May and nearly all the issues we've raised preceded your chairmanship. However, we have confidence you possess the unique perspective to understand the concerns we've raised. Therefore, we strongly urge you to 1) delay the reporting and collection of data under the CAT NMS Plan until a full investigation on the EDGAR breach can be conducted and the SEC has taken steps to improve its cybersecurity infrastructure and 2) reexamine and possibly scale back the amount of PII collected and kept in the CAT database.

Thank you in advance for the consideration of our requests. We hope to continue working with you to ensure that our financial markets are secure from cyber-intrusion. If you have any questions, please have your staff contact Gerald Huang, Elad Roisman, or Michelle Mesack.

Sincerely,

David A. Perdue
United States Senator

Mike Crapo
United States Senator

[5] http://www.catnmsplan.com/faq/

[6] https://www.reuters.com/article/us-sec-cyber-weaknesses-exclusive/exclusive-u-s-homeland-security-found-sec-had-critical-cyber-weaknesses-in-january-idUSKCN1BW27P

[7] https://www.gao.gov/assets/680/676876.pdf & https://www.gao.gov/assets/690/686192.pdf