United States Senate
WASHINGTON, DC 20510

July 24, 2019

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

Dear Chairman Clayton:

We write to you regarding the national security risk China poses to all American investors because of the planned collection of their personally identifiable information (PII) by the Consolidated Audit Trail (CAT) database. The CAT is a U.S. Securities and Exchange Commission (SEC) creation that requires broker-dealers, trading venues and stock exchanges to report all trade information and retail investor information to a single database. Given the aggressive nature of the Chinese Communist Party's cyber agenda and the risk this presents to the American people, we are asking the Commission to prohibit the collection of *any* retail investor PII by the CAT. While we support the SEC using the CAT to conduct market surveillance using non-retail investor information, we are worried that including the PII of every American with money in the stock market will create an easy target for China's cyber-attack initiatives.

Nine years have passed since the CAT was conceived, and Americans views on data collection have changed dramatically. Americans have become increasingly concerned about the risks cyberthreats pose to their sensitive personal and financial information and are very worried about identity theft. Massive breaches at government agencies and numerous U.S. companies by China over the last decade have demonstrated that no entity is immune from their attacks.

Intelligence officials recently highlighted, in stark terms, the threat that cybercriminals pose. In its January 2019 "Worldwide Threat Assessment," the U.S. intelligence community noted that state actors "increasingly use cyber operations to threaten both minds and machines in an expanding number of ways – to steal information, to influence our citizens, or to disrupt critical infrastructure."[1] The report called out China in particular, stating that it "remains the most active strategic competitor responsible for cyber espionage against the U.S. Government, corporations, and allies." Another report described China's cyber command as "fully institutionalized" within the Communist Party, employing more than 100,000 soldiers charged with carrying out operations against the U.S. government, its companies, and its people.[2]

China's attacks on American interests illustrate how active their cyber soldiers have become. Just last year, China stole a National Security Agency hacking tool, EternalBlue, to use against "the

[1] Worldwide Threat Assessment of the U.S. Intelligence Community. Statement for the Record – Senate Select Committee on Intelligence. January 29, 2019.
[2] https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

U.S. where it is most vulnerable."[3] The Chinese are widely believed to be behind the hacking of over 20 million personnel records at the Office of Personnel Management in 2015, the theft of the PII of thousands of U.S. Navy personnel, the recent attacks shutting down essential services in American cities around the country, and several breaches of private sector company databases in recent years. Intelligence officials have warned that China's cyber activity has risen in recent months and the Chinese cyber division is targeting critical infrastructure in the financial sector, among others.[4] Secretary of State Mike Pompeo suggested that one goal of China's attacks is to use the sensitive information of susceptible Americans to recruit them to act as double agents against the U.S.[5]

These brazen efforts are part of China's long-term strategy to undermine America's economic and military standing in the world.[6] A single database that includes the PII of every American investor would be a target too tempting to ignore. Chinese hackers could use this information to manipulate or disrupt our equity markets, trade stocks based upon material nonpublic information, steal entire portfolios and sell them on the dark web, or blackmail American citizens. We cannot allow any of those outcomes.

Put simply, the costs of storing the PII of millions of Americans in the CAT and exposing it to Chinese hackers far outweighs any benefit to the SEC in overseeing the equity markets. A hack of this database that leads to identity theft would also diminish the SEC's reputation and its credibility in the eyes of the public – especially given this opportunity to reverse course.

We call on the SEC to put the security of the American people first and end its policy of putting the PII of every American saver and retiree into the largest single database of market-sensitive information in history.

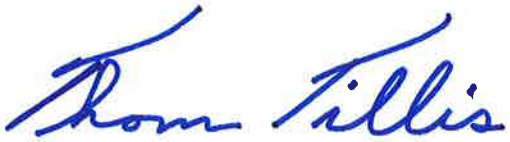
We believe you will agree that the national security risks posed by China and other foreign adversaries are too great to ignore, and we believe the SEC should take the steps necessary to safeguard our markets and protect millions of American investors from the threats posed by cybercriminals.

Sincerely,

John Kennedy
United States Senator

Jerry Moran
United States Senator

[3] https://www.nytimes.com/2019/05/25/us/nsa-hacking-tool-baltimore.html
[4] https://www.reuters.com/article/us-usa-cyber-china/chinas-hacking-against-u-s-on-the-rise-u-s-intelligence-official-idUSKBN1OA1TB
[5] https://www.politico.com/story/2018/12/12/pompeo-says-china-hacked-marriott-1059172
[6] https://www.breitbart.com/national-security/2019/04/25/exclusive-sen-marco-rubio-at-their-own-peril-countries-embrace-china/

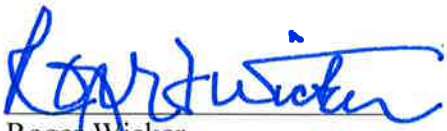


Thom Tillis
United States Senator

Kevin Cramer
United States Senator

Tom Cotton
United States Senator

M. Michael Rounds
United States Senator



Roger Wicker
United States Senator