

Congress of the United States
House of Representatives
Washington, DC 20515-0403

November 2, 2022

The Honorable Gary Gensler
Chair
U.S. Securities and Exchange Commission
100 F Street NE
Washington, DC 20549

Dear Chair Gensler:

We write regarding the Securities and Exchange Commission's (SEC) recent order to again delay the collection of retail investor personal and financial information by the Consolidated Audit Trail (CAT) to July 2024. The ongoing logistical and implementation issues that have come to define the CAT project warrant this delay and we support the SEC's order.

However, we are troubled that the SEC has yet to address the biggest threat that the CAT poses: the collection and stockpiling of the personally identifiable information (PII) of millions of American investors. Despite receiving several warnings from members of Congress and industry participants about the risks associated with collecting PII, the SEC has not acted to prohibit the collection of the sensitive personal and financial information of virtually every American investor.

The CAT will become a soft, highly desirable target for cybercriminals, especially those supported by the Chinese Communist Party (CCP), Russia, and other state actors. Over the last year, the Cybersecurity and Infrastructure Security Agency (CISA) has issued alerts about state-sponsored threats to cybersecurity in the United States.¹ One of these alerts notes that "*Chinese state-sponsored cyber actors aggressively target U.S. and allied political, economic, military, educational, and critical infrastructure (CI) personnel and organizations to steal sensitive data, critical and emerging key technologies, intellectual property, and personally identifiable information (PII).*" These same actors are undoubtedly ready to target the CAT the day it is fully operational.

In addition to these threats, there is also the risk posed by the thousands of individuals who will have daily access to the information stored under the CAT, and by the potential for cybersecurity protocols to be inadequate. The SEC itself has been the victim of a major cybersecurity breach²

¹Alert AA21-200B Chinese State-Sponsored Cyber Operations: Observed TTPs, available at <https://www.cisa.gov/uscert/ncas/alerts/aa21-200b>; Alert AA22-047A Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain Sensitive U.S. Defense Information and Technology, available at <https://www.cisa.gov/uscert/ncas/alerts/aa22-047a>

²Statement on Cybersecurity, Chairman Jay Clayton (September 2017). available at <https://www.sec.gov/news/public-statement/statement-clayton-2017-09-20>

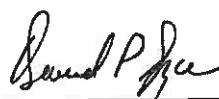
that allowed individuals access to market moving information, and recent SEC inspector general reports have detailed numerous incidents where employees or contractors have misused nonpublic information.³ We believe the most effective way to mitigate these threats is for the SEC to prohibit the collection of *any* PII by the CAT and make clear to financial institutions that they will not be forced to hand over the personal information of their own customers to the CAT.

We expect the SEC to take action to protect the PII of American investors as swiftly as possible. Thank you for your attention to this matter.

Sincerely,



Steve Womack



David Joyce



Mark E. Amodei



Chris Stewart

³ Semiannual report of SEC inspector general through September 20th, 2021 contained at least five incidents of SEC employees or contractors violating data security protocols, including by sending PII and other sensitive information to unsecure email addresses. The most recent inspector general semiannual report described an additional incident involving SEC employees sharing nonpublic information with an individual who was not working at the SEC, leading to the resignation of one of the employees. Report available at <https://www.sec.gov/files/Semiannual-Report-to-Congress-October-1-2021-through-March-31-2022.pdf>