

United States Senate

WASHINGTON, DC 20510

October 5, 2023

The Honorable Gene Dodaro
Comptroller General of the United States
Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Dodaro:

For more than a decade, the Securities and Exchange Commission (SEC) has been working to operationalize the Consolidated Audit Trail (CAT). The SEC adopted Rule 613 in 2012 which established the CAT with the goal of “creating a comprehensive consolidated audit trail that allows regulators to efficiently and accurately track all activity in [Reg] NMS securities throughout the U.S. markets.”¹

Since Rule 613 was adopted, the CAT has gone through several operational delays while market participants, SEC commissioners, and members of Congress have continued to raise concerns over the continually growing costs related to CAT implementation. However, the top concern related to the CAT remains the collection of personally identifiable information (PII) of every investor that trades a single share of stock on a U.S. exchange. This information will be collected and stored in a vast database that will be subject to cyberattacks and which presents concerns about the privacy and protection of Americans’ sensitive personal information.

Even more concerning, the CAT poses fundamental threats to protections from “unreasonable search and seizures” under the Fourth Amendment. The courts have previously held that the mandated production of certain information can violate the Fourth Amendment.² There are many legitimate reasons an individual would not want their financial transactions to be regularly submitted to a government registry. The SEC has failed to appreciate and address these concerns that CAT collection of PII presents.

We request that GAO investigate and report on the potential risks, Constitutional issues, and personal privacy concerns that are presented due to PII collection under the CAT. The GAO’s report should encompass:

- An analysis of the constitutionality and the legality regarding the collection of American investors’ personal and financial information by a regulator in a centralized database without any evidence of wrongdoing;
- The cyber vulnerabilities of the CAT database;

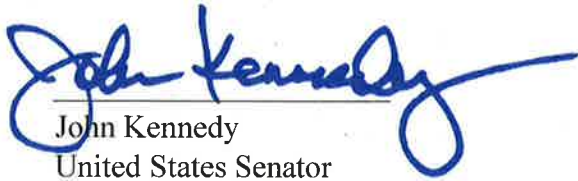
¹ SEC Release No. 67457; File No. S7-11-10

² City of L.A., Calif. v. Patel, 576 U.S. 409, 412; Airbnb, Inc. v. City of N.Y., 373 F. Supp. 3d 467, 483 (S.D.N.Y. 2019)

- An estimation of the total number of individuals that will have regular access to information collected under CAT, the professional affiliation of these individuals, and any screening or background check processes established by the SEC and FINRA to vet any individual that will be able to access the CAT database;
- A list of all publicly reported cyberattacks on federal government agencies over the last three (3) years and analysis of Americans' PII that was compromised or potentially compromised as a result of such cyberattacks including the cost to repair the identities of such individuals;
- An analysis of what entities retail investors may hold legally liable for a cyber-attack on the CAT if the incident results in the theft of American investors account numbers, identities, and/or securities holdings, and what the cost of that liability might be based on previous identity theft cost information.

Thank you for your attention to this matter. We appreciate your response no later than November 15, 2023.

Sincerely,


John Kennedy
United States Senator


Katie Britt
United States Senator