

**TIM GRIFFIN**  
ATTORNEY GENERAL

August 15, 2023

*Submitted via First Class Mail*

The Honorable Charles Schumer  
Majority Leader  
S-221, U.S. Capitol  
Washington, DC 20510

The Honorable Kevin McCarthy  
Speaker of the House  
H-232, U.S. Capitol  
Washington, DC 20515

The Honorable Mitch McConnell  
Republican Leader  
S-230, U.S. Capitol  
Washington, DC 20510

The Honorable Hakeem S. Jeffries  
Minority Leader  
H-204, U.S. Capitol  
Washington, DC 20515

Re: Letter from the States of Arkansas, Florida, Georgia, Kentucky, Iowa,  
South Carolina, Utah, and West Virginia Supporting the Protecting Investors'  
Personally Identifiable Information Act

Dear Majority Leader Schumer, Republican Leader McConnell, Speaker McCarthy, and  
Minority Leader Jeffries:

The undersigned attorneys general write to respectfully urge you to join us in supporting the Protecting Investors' Personally Identifiable Information Act. The Securities and Exchange Commission's efforts to create a massive surveillance database containing detailed information on every trade by every person with any money in the stock market, regardless of suspicion of wrongdoing, must be stopped. The Commission's Consolidated Audit Trail, or CAT, poses a clear threat to Americans' liberty and privacy, and it will be an easy and irresistible target for cyber thieves. Indeed, our offices routinely assist consumers, retirees, and others who have been victims of identity theft, and the CAT unnecessarily risks exposing millions more to it. We urge you to support the Protecting Investors' Personally Identifiable Information Act.

**Background**

On May 6, 2010, the Dow Jones Industrial Average experienced a "flash crash" precipitated by a "large fundamental trader" executing a rapid algorithmic sell program during "unusually turbulent" trading. Findings Regarding the Mkt. Events of May 6, 2010, Joint Advisory Comm. on Emerging Regul. Issues (Sep. 30, 2010), <https://perma.cc/F2BJ-85B3>. Twenty days

later, the Commission lamented its limited ability “to quickly reconstruct and analyze th[at] severe market disruption” and proposed Rule 613 in response. Consol. Audit Trail, Release No. 34-62174 (May 26, 2010).

Rule 613 ordered self-regulatory organizations (i.e., national securities exchanges and associations) “to create, implement, and maintain a consolidated audit trail that would be more comprehensive than any audit trail currently in existence.” *Id.* It required the organizations (including their members and brokers) to “capture . . . information about each order for” a security, including “the identity of the customer” and “the routing, modification, cancellation or execution of the order,” and provide this information “to a central repository on a real-time basis.” *Id.* The Commission adopted Rule 613 and approved the National Market System plan to implement the CAT. Consol. Audit Trail, Release No. 34-67457 (July 18, 2012); Joint Indus. Plan [and] Ord. Approving the Nat’l Mkt. Sys. Plan Governing the Consol. Audit Trail, Release No. 34-79318 (Nov. 15, 2016). But, due to its unprecedented magnitude, the CAT’s development suffered various setbacks, and its implementation was delayed for years.

After multiple high-profile data breaches by Chinese hackers and others (discussed below), the Commission announced it was examining its need to collect personally identifiable information, or PII, as part of the CAT. Chairman Jay Clayton, Statement on Status of the Consol. Audit Trail (Nov. 14, 2017), <https://perma.cc/35R8-SMXX>; Chairman Jay Clayton, Statement on Status of the Consol. Audit Trail (Sep. 9, 2019), <https://perma.cc/HWQ7-GF5A>. Congress held hearings regarding the cybersecurity risks of creating a massive centralized repository of investor information. *See* Implementation and Cybersecurity Protocols of the Consol. Audit Trail, Hearing before the U.S. H.R. Comm. on Fin. Servs. (Nov. 30, 2017), <https://perma.cc/AB6J-X6LR>.

A coalition of Senators wrote to the Commission concerning the CAT’s national security risks, especially in light of “the aggressive nature of the Chinese Communist Party’s cyber agenda.” Sen. John Kennedy, et al., Letter to U.S. Sec. & Exch. Comm’n (July 24, 2019), <https://perma.cc/JKW4-Y364>. The Senators highlighted that a “single database” that includes the “PII of every American investor” would be a “target too tempting to ignore.” *Id.* It noted that “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.” *Id.* Although the Senators supported the Commission’s use of “non-retail investor information,” it urged the Commission to prohibit collection of “retail investor[s]’” personal information. *Id.*

In response, in testimony before Congress, then-Commission Chairman Jay Clayton conceded that he “share[d] many of the concerns that have been raised about the protection of any investors’ PII that would be stored in the CAT.” Chairman Jay Clayton, Testimony on “Oversight of the Securities and Exchange Commission,” Before the U.S. Senate Comm. on Banking, Housing, and Urb. Affairs (Dec. 10, 2019), <https://perma.cc/GM5S-PXF9>. Ultimately, the Commission determined it would not collect Social Security numbers, account numbers, or complete birth dates, acknowledging that “the most secure approach to addressing any piece of sensitive retail Customer PII would be to eliminate its collection altogether.” Ord. Granting

Conditional Exemptive Relief, Release No. 34-88393, 85 Fed. Reg. 16152 (March 17, 2020). Nevertheless, it plowed ahead, refusing to eliminate the collection of sensitive information about retail investors' trades, including their "name[s], address[es], and birth year[s]." *Id.*

### **Protecting Investors' Personally Identifiable Information Act**

Senators John Kennedy (R-La.), John Boozman (R-Ark.), Jerry Moran (R-Kan.), Tom Cotton (R-Ark.), Steve Daines (R-Mont.), Katie Britt (R-Ala.), Mike Rounds (R-S.D.) and Tommy Tuberville (R-Ala.) have introduced the Protecting Investors' Personally Identifiable Information Act (S. 2230) to protect American investors' sensitive personal information. *See* Sen. John Kennedy, Kennedy, Colleagues Introduce Bill to Protect Inv. Priv. by Prohibiting Vulnerable SEC Database (July 11, 2023), <https://perma.cc/FT2M-5445>. Representatives Barry Loudermilk (R-Ga.), French Hill (R-Ark.), Bill Huizenga (R-Mich.), Ann Wagner (R-Mo.), Dan Meuser (R-Pa.), Young Kim (R-Cal.), and Zach Nunn (R-Iowa) introduced companion legislation in the House (H.R. 4551). *See* Rep. Loudermilk, House Republicans Introduce Legislation to Protect Invs.' Personally Identifiable Information (July 12, 2023), <https://perma.cc/V799-5X5K>. This legislation would prohibit the Commission from requiring market participants to submit investors' PII to the CAT except on a case-by-case basis when the Commission requests it as part of an investigation of a securities-law violation.

#### **I. The CAT is a dire threat to Americans' liberty and privacy.**

The need for legislation to protect Americans' privacy from the CAT is clear. The CAT is truly a panopticon of investor conduct—"a comprehensive surveillance database that will collect and store every equity and option trade and quote, from every account at every broker, by every investor." Commissioner Hester M. Peirce, Statement of Hester M. Peirce in Response to Release No. 34-88890; File No. S7-13-19 (May 15, 2020). It subjects every person with any money in the stock market to constant surveillance of their financial actions without any suspicion of wrongdoing. And it stores this sensitive data in a central repository that will be accessed daily by thousands of people, including the Commission's staff and the employees of a lengthy list of self-regulating organizations: BATS Exchange, Inc.; BATS-Y Exchange, Inc.; BOX Options Exchange LLC; C2 Options Exchange, Inc., Chicago Board Options Exchange, Inc.; Chicago Stock Exchange, Inc., EDGA Exchange, Inc.; EDGX Exchange, Inc.; Financial Industry Regulatory Authority, Inc.; International Securities Exchange, LLC; ISE Gemini, LLC; Miami International Securities Exchange LLC; NASDAQ OMX BX, Inc., NASDAQ OMX PHLX LLC; The NASDAQ Stock Market LLC; National Stock Exchange, Inc.; New York Stock Exchange LLC; NYSE MKT LLC; and NYSE Arca, Inc. *See* Amended CAT NMS Plan for Consol. Audit Trail, LLC (Aug. 29, 2019), <https://perma.cc/3Q4Q-9EFV> (stating that although proposals were for "a minimum of 3,000 users" at one time, the "actual number of users may be higher based upon regulator and Participant usage of the system").

A fundamental expectation of a free society is that citizens are not subject to unwarranted government monitoring. And in America, surveillance of an individual's conduct is justified only for suspected unlawful activity. True, the government may conduct searches and collect

information on individuals, but only in compliance with safeguards like the requirement to show objective “probable cause.” See U.S. Const. amend. 4 (right to be secure against “unreasonable searches and seizures”); *Katz v. United States*, 389 U.S. 347, 356 (1967). Such burdens on government surveillance are necessary to safeguard liberty and privacy. Likewise, here, a retail investor’s trading activity warrants monitoring only when there are objective reasons to believe that he or she is violating the law.

But the CAT isn’t pegged to anything other than ordinary investment decisions investors have every right to make, and it represents a disturbing departure from these deeply moored principles safeguarding Americans’ liberty and privacy. Its collection of retail investors’ PII is unwarranted and raises serious constitutional concerns. Therefore, we urge you to support the Protecting Investors’ Personally Identifiable Information Act.

## **II. The CAT creates an irresistible target for cyber thieves.**

The sheer size of the CAT also makes it an inevitable target for cyber thieves. The history of other massive governmental repositories of personal information is instructive here. In 2014, for example, Chinese state-sponsored hackers breached the Office of Personnel Management’s database, obtaining security-clearance background information on 21.5 million people. The OPM Data Breach: How the Gov’t Jeopardized Our Nat’l Sec. for More than a Generation, U.S. H.R. Comm. on Oversight and Gov’t Reform, 114th Cong. (Sep. 7, 2016), <https://perma.cc/CAX3-B867>. By means of this hack, the Chinese Communist Party obtained highly sensitive “information about everybody who has worked for, tried to work for, or works for the United States government,” including disclosures regarding “some of the most intimate and potentially embarrassing aspects” of their lives. *Id.* (quotation omitted). Former CIA Director Michael Hayden stated that the stolen data “remains a treasure trove of information that is available to the Chinese until the people represented by the information age off. There’s no fixing it.” *Id.* And according to former NSA Senior Counsel Joel Brenner, although “[t]his [wa]s not the end of American human intelligence, . . . it’s a significant blow.” *Id.* Indeed, the damage caused by this hack “cannot be overstated.” *Id.*

The U.S. Navy has similarly suffered a disturbing series of especially troubling data breaches, including a 2016 hack in which the names and Social Security numbers of over 134 thousand sailors were stolen from a Navy contractor with access to the data. Sam LaGrone, Navy: Pers. Data of 134K Sailors ‘Compromised’, U.S. Naval Inst. News (Nov. 24, 2016), <https://perma.cc/D82R-4A33>. And in March of this year, the Consumer Financial Protection Bureau alerted Congress of a breach in which the PII of 256 thousand consumers were exposed in an unauthorized transfer of confidential data to an employee’s personal email address. Caitlin Reilly, CFPB Employee Sent Data of 250,000 Customers to Pers. Email, Roll Call (April 19, 2023), <https://perma.cc/M6NY-P2E9>.

Private-sector holders of massive data repositories have been targeted for the same reasons. In May 2017, state-sponsored Chinese hackers breached the credit reporting agency Equifax, obtaining names, Social Security numbers, birth dates, and driver’s license numbers for 148

million American consumers. The Equifax Data Breach, U.S. H.R. Comm. on Oversight and Gov't Reform, 115th Cong. (Dec. 2018), <https://perma.cc/DT2W-GWN8>. “Equifax had credit information on 820 million consumers and 91 million businesses,” and “[t]his massive amount of sensitive information made Equifax a prime target for hackers.” *Id.* This breach followed two smaller, but still significant, breaches in 2013 and 2015 of consumer data held by Experian, another of the three major credit reporting agencies. *Id.*

Data breaches at technology companies holding large amounts of personal information such as Microsoft, Facebook, and Yahoo!, and financial companies like First American Financial Corp., JPMorgan Chase & Co., and CapitalOne have impacted hundreds of millions of people. See Kyle Chin, Top 23 Breaches in U.S. Hist., UpGuard (July 18, 2023), <https://perma.cc/5LDP-LCG7>.

A breach of the CAT is inevitable, as the Commission itself admits: “[W]e expect we will face the risk of unauthorized access to CAT’s central repository and other efforts to obtain sensitive CAT data,” by “intruders” seeking “the trading activity and personally identifiable information of investors.” Chairman Jay Clayton, Statement on Cybersecurity (September 20, 2017), <https://perma.cc/Q6VT-8SHM>. Indeed, as former Chairman Clayton admitted, “frequent attempts by unauthorized actors” to “access [the] data” the Commission already collects are a problem, and “cyber threat actors have managed to access or misuse our systems” despite “our efforts to protect our systems and manage cybersecurity risks.” *Id.*; see SEC Brings Charges in EDGAR Hacking Case, 2019-1 (January 15, 2019), <https://perma.cc/S3CY-ZM4N> (announcing charges against a foreign hacker and others for breaching the Commission’s systems to obtain nonpublic information for use for illegal trading).

And Commissioner Hester M. Peirce has repeatedly sounded similar warnings about the CAT, explaining that “unauthorized access to, or disclosure of the information contained in the CAT is almost certainly just a matter of time.” Commissioner Hester M. Peirce, Statement of Hester M. Peirce in Response to Release No. 34-88890; File No. S7-13-19 (May 15, 2020), <https://perma.cc/E48J-PDSQ>. As she notes, “[O]ne security lapse involving only one of the CAT’s thousands of users could compromise the entire database,” and “even an honest employee can become the inadvertent conduit for a cyber-breach.” *Id.*

The Commission’s decision to forego the use of Social Security numbers, account numbers, and full birthdates in the CAT does not sufficiently anonymize the data because individual investors can still be easily identified from the remaining PII, including their names, addresses, and birth years. *Id.* And in any case, the Commission “already has sufficient tools to get the information it needs,” and “a more limited version of the program that looked only at the trades of large institutional investors would be almost as useful for reconstructing market events,” without exposing individual investors’ PII. Hester M. Peirce, This CAT is a Dangerous Dog, Real Clear Policy (October 9, 2019), <https://perma.cc/UG4E-77RN>.


The CAT's collection of retail investors' PII poses a clear threat to the security of every American investor. Therefore, we urge you to support the Protecting Investors' Personally Identifiable Information Act.

### Conclusion


Action by Congress is necessary because "the CAT treats every American as a presumptive wrongdoer" and violates fundamental principles safeguarding Americans' liberty, privacy, and security. Commissioner Hester M. Peirce, Statement on Proposed Amends. to the Nat'l Mkt. Sys. Plan Governing the Consol. Audit Trail to Enhance Data Sec. (Aug. 21, 2020), <https://perma.cc/GES6-55K8>. "The CAT will watch everything you do in the securities marketplace, record it for employees of the SEC and self-regulators to monitor, and store it in databases that hackers undoubtedly will attack." *Id.* Congress has never authorized the Commission to create this massive surveillance program, and Congress should stop it.

Therefore, for all the reasons above, we urge you to support the Protecting Investors' Personally Identifiable Information Act.


Sincerely,



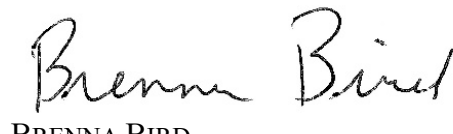
TIM GRIFFIN  
Arkansas Attorney General



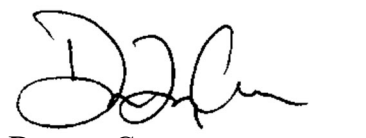
ASHLEY MOODY  
Florida Attorney General




CHRIS CARR  
Georgia Attorney General



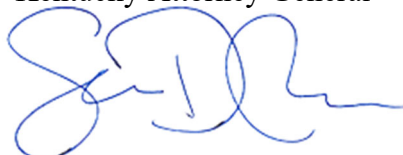
BRENNA BIRD  
Iowa Attorney General




DANIEL CAMERON  
Kentucky Attorney General



ALAN WILSON  
South Carolina Attorney General



SEAN D. REYES  
Utah Attorney General



PATRICK MORRISEY  
West Virginia Attorney General