

TABLE OF CONTENTS

Table of Authoritiesiii

Interests of Amici Curiae and Summary of Argument 1

Argument 3

 I. The Commission’s massive surveillance program poses grave
 and unnecessary risks to American investors. 3

 A. Massive repositories of personal information—like the
 CAT—are massive targets for hackers. 3

 B. The Commission’s own history of security breaches
 does not inspire confidence that it can keep the CAT
 secure. 5

 C. Citizens remain vulnerable to being targeted by rogue
 federal officials and contractors. 6

 II. The Commission’s massive surveillance program is contrary to
 law. 7

 A. The Commission has never identified any specific
 statutory authority for its massive surveillance of retail
 investors. 8

 B. The Commission’s decision to require investors to
 ultimately bear the cost of its surveillance program
 further underscores the program’s shaky foundation. 11

 C. The Supreme Court’s major-questions doctrine requires
 courts to cast a skeptical eye on new assertions of
 previously unexercised authority like the Commission’s
 massive repository of retail-investors’ personal
 information. 15

 D. The Commission failed to consider whether storing
 retail-investor information is necessary to further the
 CAT’s goal of providing the Commission with access
 to real-time market information. 18

Conclusion 20

Additional States Represented 22

TABLE OF AUTHORITIES

Cases

Ala. Ass’n of Realtors v. Dep’t of Health & Hum. Servs.,
141 S. Ct. 2485 (2021)..... 22, 24

Biden v. Nebraska,
143 S. Ct. 2355 (2023)..... 21

Geier v. Am. Honda Motor Co.,
529 U.S. 861 (2000)..... 19

Laird v. Tatum,
408 U.S. 1 (1972)..... 18

OPM v. Richmond,
496 U.S. 414 (1990)..... 17

Spirit Airlines, Inc. v. FAA,
997 F.3d 1247 (D.C. Cir. 2021)..... 25

United States Forest Serv. v. Cowpasture River Pres. Ass’n,
140 S. Ct. 1837 (2020)..... 23

United States Telecom Ass’n v. FCC,
855 F.3d 381 (D.C. Cir. 2017)..... 21

West Virginia v. EPA,
142 S. Ct. 2587 (2022)..... 20, 23-24

Whitman v. Am. Trucking Ass’ns, Inc.,
531 U.S. 457 (2001)..... 14

Statutes

15 U.S.C 78k-1(a)(3) 10

15 U.S.C. 78k-1(a)(1)(C)..... 10, 14

15 U.S.C. 78k-1(a)(2) 10

Personal Information Protection Act
Ark. Code Ann. 4-110-101 *et seq* 1

Regulations

17 C.F.R. 240.17a-25..... 12

17 C.F.R. 264.613(c)(7)(viii)..... 11

17 C.F.R. 264.613(j)(4)..... 11

Amends. to the Nat’l Mkt. Sys. Plan Governing the Consol. Audit Trail to Enhance Data Sec., 85 Fed. Reg. 65990, (Aug. 21, 2020)..... 13

Consolidated Audit Trail, 77 Fed. Reg. 45722 (Aug. 1, 2012)..... 11

Joint Indus. Plan; Ord. Approving an Amend. to the Nat’l Mkt. Sys. Plan Governing the Consol. Audit Trail, 88 Fed. Reg. 62628, (Sept. 6, 2023)..... 14-15

Joint Indus. Plan; Ord. Approving the Nat’l Mkt. Sys. Plan Governing the Consol. Audit Trail, 81 Fed. Reg. 84696, (Nov. 15, 2016)..... 12, 25

Ord. Granting Conditional Exemptive Relief, Pursuant to Section 36 & Rule 608(e) of the Sec. Exch. Act of 1934, from Section 6.4(d)(II)(c) & Appendix D Sections 4.1.6, 6.2, 8.1.1, 8.2, 9.1, 9.2, 9.4, 10.1, & 10.3 of the Nat’l Mkt. Sys. Plan Governing the Consol. Audit Trail, 85 Fed. Reg. 16152, (Mar. 17, 2020)..... 12, 26

Other Authorities

Abner J. Mikva, *Congress: The Purse, the Purpose, and the Power*, 21 Ga. L. Rev. 1 (1986) 17

Amended CAT NMS Plan for Consolidated Audit Trail, LLC, FINRA CAT (Aug. 29, 2019) <https://perma.cc/C9KC-FFEX>..... 12

C. Boyden Gray, *Extra Icing on an Unconstitutional Cake Already Frosted? A Constitutional Recipe for the CFPB*, 24 Geo. Mason L. Rev. 1213 (2017)..... 17

Caitlin Reilly, *CFPB Employee Sent Data of 250,000 Customers to Pers. Email*, Roll Call (April 19, 2023), <https://perma.cc/M6NY-P2E9> 5

CAT NMS Plan, <https://perma.cc/UH3G-9ZFH> 11

Christopher Wray, *Director Wray’s Opening Statement to the House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party*, FBI (Jan. 31, 2024), <https://perma.cc/JBS8-Z9MB> 6

Comm’r Hester M. Peirce, *Statement of Hester M. Peirce in Response to Release No. 34-88890; File No. S7-13-19*, SEC (May 15, 2020), <https://perma.cc/G4HL-M7EU>..... 27

Comm’r Hester M. Peirce, *Statement of Hester M. Peirce in Response to Release No. 34-88890; File No. S7-13-19*, SEC (May 15, 2020), <https://perma.cc/R32N-3JDM>..... 8

Comm’r Hester M. Peirce, *This CAT is a Dangerous Dog*, RealClearPolicy (Oct. 9, 2019), <https://perma.cc/558J-ZWB8>..... 26-27

Comm’r Hester M. Peirce, *Who’s Paying?: Statement on the CAT’s Funding Model*, SEC (Sept. 6, 2023), <https://perma.cc/UJV5-J65D> 21

Comm’r Mark T. Uyeda, *Statement on Consolidated Audit Trail Revised Funding Model*, SEC (Sept. 26, 2023), <https://perma.cc/78RY-KN5Q> 21

David A. Herrman, *To Delegate or Not to Delegate—That Is the Preemption: The Lack of Political Accountability in Administrative Preemption Defies Federalism Constraints on Government Power*, 28 Pac. L.J. 1157 (1997) 19

Devlin Barrett, *FBI misused surveillance tool on Jan. 6 suspects, BLM arrestees and others*, Wash. Post. (May 19, 2023), <https://perma.cc/QRA4-XDD2> 22

Eileen Sullivan, *Former Contractor Who Leaked Trump’s Tax Returns Sentenced to 5 Years in Prison*, N.Y. Times (Jan. 29, 2024), <https://perma.cc/VYF2-CHQY> 8

Eloise Pasachoff, *The President’s Budget as a Source of Agency Policy Control*, 125 Yale L.J. 2182 (2016)..... 18

Emily Cochrane, *Justice Department Settles With Tea Party Groups After I.R.S. Scrutiny* N.Y. Times (Oct. 26, 2017), <https://perma.cc/SYV8-HH6L>..... 9

Findings Regarding the Market Events of May 6, 2010, Joint Advisory Comm. on Emerging Regul. Issues (Sep. 30, 2010), <https://perma.cc/F2BJ-85B3>..... 25

Gallup, *What Percentage of Americans Own Stock?* (May 24, 2023), <https://perma.cc/3XKX-X62N>..... 21

Gillian E. Metzger, *Agencies, Polarization, and the States*, 115 Colum. L. Rev. 1739 (2015) 18, 20

Jack M. Beermann, *Congressional Administration*, 43 San Diego L. Rev. 61 (2006) 20

James B. Stewart, *As A Watchdog Starves, Wall Street Is Tossed a Bone*, N.Y. Times (July 15, 2011), <https://perma.cc/75SJ-UAJM>..... 19

Joseph Story, *Commentaries on the Constitution of the United States* § 1348 (3d ed. 1858) 18

Kyle Chin, *Top 23 Breaches in U.S. History*, UpGuard (July 18, 2023), <https://perma.cc/5LDPLCG7> 6

Laura E. Dolbow, *Agency Adherence to Legislative History*, 70 Admin. L. Rev. 569 (2018)..... 18

Letter from Christopher A. Iacovella, CEO, American Securities Association to Vanessa A. Countryman, Sec’y Commission (Nov. 30, 2020) <https://perma.cc/7BQW-K7KH>..... 13

Letter from Jim Jordan and Mike Johnson to Hon. Merrick B. Garland (May 11, 2022), <https://perma.cc/R9UG-69LD>..... 9

Letter from Lawrence Harris, USC Marshall Sch. of Bus. to Vanessa Countryman, Sec’y Commission, (June 21, 2022), <https://perma.cc/3WG7-3J69> 16

Letter from Virginia and 19 other States to Hon. Merrick B. Garland and
 Hon. Christopher Wray (Feb. 10, 2023), <https://perma.cc/7NXQ-U3H3>..... 9

Matthew Goldstein & David Gelles, *A Phantom Offer Sends Avon’s Shares Surging*, N.Y. Times
 (May 14, 2015), <https://perma.cc/S5VF-ZEJZ> 7

Matthew Goldstein, *S.E.C. Social Media Hack That Sent Bitcoin Soaring
 Prompts Investigation*, N.Y. Times (Jan. 10, 2024),
<https://perma.cc/39MP-WJCX>..... 7

Matthew Goldstein, *U.S. Charges 2 With Hacking Into S.E.C. System in
 Stock-Trading Scheme*, N.Y. Times (Jan. 15, 2019),
<https://perma.cc/R49B-KP33> 6

Paul Larkin, Jr. & Zack Smith, “*Brother, Can You Spare A Million Dollars?*”: *Resurrecting the
 Justice Department’s “Slush Fund,”*
 19 Geo. J. L. & Pub. Pol’y 447 (2021) 17

Rep. Barry Loudermilk, *Rep. Loudermilk, House Republicans Introduce Legislation to Protect
 Investors’ Personally Identifiable Information*
 (July 12, 2023), <https://perma.cc/V799-5X5K> 23

Robert C. Byrd, *The Control of the Purse and the Line Item Veto Act*,
 35 Harv. J. On Legis. 297 (1998)..... 17

Robert E. Cushman, *The Independent Regulatory Commissions* (1972)..... 19

Sam LaGrone, *Navy: Pers. Data of 134K Sailors ‘Compromised’*,
 U.S. Naval Inst. News (Nov. 24, 2016), <https://perma.cc/D82R-4A33>..... 5

Sen. John Kennedy, *Kennedy, Colleagues Introduce Bill to Protect Investor Privacy by
 Prohibiting Vulnerable SEC Database* (July 11, 2023), <https://perma.cc/FT2M-5445> 23

Sen. Mike Lee, *Congress, don’t pass the defense bill without FISA reform*
 (Dec. 11, 2023), <https://perma.cc/3PG6-JSKV>..... 22

Steve Marshall, *ESG Defenders Pose as ‘Free Market’ Disciples*
 (Wall St. J. Op. May 23, 2023), <https://perma.cc/5BLM-VGUA>..... 8

The Equifax Data Breach, U.S. H.R. Comm. on Oversight and Gov’t Reform, 115th Cong. (Dec.
 2018), <https://perma.cc/DT2W-GWN8> 5

The Federalist, No. 58..... 18

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> 4-5

INTERESTS OF AMICI CURIAE AND SUMMARY OF ARGUMENT

Amici curiae are the States of Arkansas, Alabama, Georgia, Idaho, Indiana, Iowa, Kansas, Louisiana, Mississippi, Missouri, Montana, Nebraska, South Carolina, South Dakota, Tennessee, Texas, Utah, Virginia, and West Virginia. *Amici* States submit this brief in support of Plaintiffs because the consolidated audit trail, or CAT, system would represent a massive, unprecedented threat to the liberty, privacy, and security of millions of *Amici* States' citizens, as well as *Amici* States' own investment interests. States are the first line of defense protecting consumers from harm due to data breaches and have a keen interest in preventing such breaches. *See, e.g.*, Personal Information Protection Act, Ark. Code Ann. 4-110-101 *et seq* (requiring prompt disclosure of information regarding data breaches to consumers).

In May 2010, algorithmic trading decisions caused a “flash crash.” That crash sent the markets into an uproar, and in response, the Securities and Exchange Commission began a decade-long push to create the CAT. As ultimately adopted, the CAT would house personal information about every single retail investor and contain real-time information about their investment decisions. The Commission says the CAT will better enable it to reconstruct and analyze events like the flash crash. But its reach isn't so limited.

Rather, the CAT will give thousands of authorized users—and given the Commission's cybersecurity track record who knows how many unauthorized users—access to real-time information about every investor and investment decision. That's a monumental shift from the way things used to work. Before the CAT, if the Commission suspected an individual of wrongdoing, it could request information from the broker-dealers associated with suspicious trades. But no more. Instead, with the CAT, thousands of government employees (and hackers) are free to comb through bulk data on every American investor with a just few clicks of the keyboard—no

individual suspicion needed. That system threatens the security and privacy of the *Amici* States' citizens, and Congress never authorized it. So this Court should preliminarily enjoin (and ultimately set aside) the Commission's Rule 613 and the 2023 order funding and operationalizing the CAT.

I. Not only will the Commission be capable of spying on Americans' trading activity, so will anyone who manages to hack into the CAT database. Given the increasing number of government databases being targeted by hackers, including agents of the Chinese Communist Party, the CAT will be as tempting a target as has ever existed. Ensuring the security of this data would be a tall order for any agency or organization. The Commission—which just this past month suffered an embarrassing (and economically damaging) hack of its X (formerly Twitter) account—has little hope of doing so. The CAT repository will also be a target of attacks from within. Americans have increasingly been targeted by rogue federal officials seeking to advance ideological agendas through the weaponization of confidential information, and the investment information contained in the CAT may well be their next opportunity.

II. Because the CAT endangers personal privacy, one might wonder why Congress gave the Commission the power to create it. The answer is that Congress never gave the Commission the authority to construct this unprecedented surveillance database. Congress never even appropriated funds for it because the Commission chose to fund the CAT through user fees that will ultimately be passed along to the very investors whose information is being put at risk. In the absence of clear language from Congress authorizing such an unprecedented program, the Commission cannot exercise that power.

And even if it could, its decision to do so was arbitrary and capricious. Indeed, the Commission's decision to collect retail investors' personal information makes no sense since

individual retail investors don't cause events like the 2010 flash crash. The Commission could have limited such collection to those investors. But the Commission didn't do that because, along the way, it decided it'd be marginally more convenient for its enforcement division to have this information without needing to explain why it needed information about any specific investor.

ARGUMENT

I. The Commission's massive surveillance program poses grave and unnecessary risks to American investors.

In continuing to insist that the CAT must contain personally identifiable information of every American investor who buys or sells stock, the Commission has given insufficient consideration to the likelihood of a hack. The CAT will be targeted for its economic value, as well as its strategic value to America's foreign adversaries. There is no reason to believe the Commission can ensure the security of the CAT given its own high-profile data-security failures. And investors have every reason to fear being targeted by rogue federal officials pursuing an agenda.

A. Massive repositories of personal information—like the CAT—are massive targets for hackers.

Recent years have shown that the greater the amount of potentially valuable, sensitive data that is stored in a single location, the greater a target it becomes. Numerous large government databases have suffered attacks and data breaches affecting millions of Americans. For example, the Office of Personnel Management's database containing security-clearance background information on 21.5 million people was breached by Chinese state-sponsored hackers in 2015. *See* 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>. This disastrous hack allowed the Chinese Communist Party to

obtain 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.* It also dealt a “significant blow” to American intelligence efforts. *Id.*

The U.S. Navy has been the target of multiple attacks, including the hacking of the names and Social Security numbers of over 134,000 sailors from a Navy contractor. Sam LaGrone, *Navy: Pers. Data of 134K Sailors ‘Compromised’*, U.S. Naval Inst. News (Nov. 24, 2016), <https://perma.cc/D82R-4A33>. And just this year, Congress learned that the Consumer Financial Protection Bureau exposed personally identifiable information of 256,000 customers through an unauthorized transfer of data to an employee’s 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>.

Large private-sector data repositories have been similarly targeted. In another attack by state-sponsored Chinese hackers, Equifax’s database was breached, and the names, Social Security numbers, birth dates, and driver’s license numbers for 148 million Americans were stolen. *The Equifax Data Breach*, U.S. H.R. Comm. on Oversight and Gov’t Reform, 115th Cong. (Dec. 2018), <https://perma.cc/DT2W-GWN8>. Where any large amount of sensitive information is stored, hackers are sure to follow. *See* Kyle Chin, *Top 23 Breaches in U.S. History*, UpGuard (July 18, 2023), <https://perma.cc/5LDPLCG7> (reporting on data breaches at technology companies impacting hundreds of millions of people).

Finally, the databases underlying critical American infrastructure are continuously targeted by foreign actors, the Chinese Communist Party chief among them. As FBI Director Christopher Wray recently remarked, Chinese state-sponsored “hackers are targeting our critical

infrastructure—our water treatment plants, our electrical grid, our oil and natural gas pipelines, our transportation systems.” Director Wray’s Opening Statement to the House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party (Jan. 31, 2024), <https://perma.cc/JBS8-Z9MB>. “Low blows against civilians are part of China’s plan,” as is “target[ing] our businesses” and “engaging in corporate deception.” *Id.* The CAT won’t be overlooked.

B. The Commission’s own history of security breaches does not inspire confidence that it can keep the CAT secure.

The Commission has hardly been immune from hacking. And if history is any indication, the Commission cannot be trusted to keep its important data secure. For example, starting in 2016, hackers compromised the Commission’s “Edgar” system for corporate filings, allowing them to steal non-public reports for over a year. *See* Matthew Goldstein, *U.S. Charges 2 With Hacking Into S.E.C. System in Stock-Trading Scheme*, N.Y. Times (Jan. 15, 2019), <https://perma.cc/R49B-KP33>. And just a few years prior, Edgar was used to submit a fake bid that spurred tens of millions of dollars in trading. *See* Matthew Goldstein & David Gelles, *A Phantom Offer Sends Avon’s Shares Surging*, N.Y. Times (May 14, 2015), <https://perma.cc/S5VF-ZEJZ>.

And more recent events underscore the Commission’s security problems are not limited to Edgar. Indeed, just this past month the Commission’s X (formerly Twitter) account was successfully hacked in an apparent effort to manipulate cryptocurrency markets. *See* Matthew Goldstein, *S.E.C. Social Media Hack That Sent Bitcoin Soaring Prompts Investigation*, N.Y. Times (Jan. 10, 2024), <https://perma.cc/39MP-WJCX>. As one of the Commission’s former enforcement officials noted, the attack was “a glaring failure of basic cyber-hygiene.” *Id.* If the

Commission cannot secure its own social media accounts, it cannot be trusted with Americans' personal data and valuable, real-time information about who is trading what.

C. Citizens remain vulnerable to being targeted by rogue federal officials and contractors.

Even if the Commission could secure the CAT data from profit-seeking hackers and foreign adversaries, the federal government has a poor track record of policing its own employees and contractors. As Commissioner Peirce noted, “[o]ne can imagine a future in which a delectably large database of trades becomes a tool for the government to single people out for making trading decisions that reflect—or are interpreted to reflect—opinions deemed unacceptable in the reigning gestalt.” Comm’r Hester M. Peirce, *Statement of Hester M. Peirce in Response to Release No. 34-88890*; File No. S7-13-19, SEC (May 15, 2020), <https://perma.cc/R32N-3JDM>. It’s easy to imagine because it wouldn’t be novel.

Take the IRS, for example. One of its contractors was just sentenced to prison for stealing and leaking tax records for thousands of wealthy individuals, including former President Donald Trump, Jeff Bezos, and Elon Musk to pursue an ideological agenda. *See Eileen Sullivan, Former Contractor Who Leaked Trump’s Tax Returns Sentenced to 5 Years in Prison*, N.Y. Times Jan 29, 2024), <https://perma.cc/VYF2-CHQY>. Investment records are no less susceptible to ideologically driven attacks than tax records. Indeed, groups like “Climate Action 100+, the Net-Zero Banking Alliance and the Venture Climate Alliance” and other ESG ideologues “have plotted to pressure blacklisted companies into making a priority of decarbonization and other social goals at the behest of the United Nations.” Steve Marshall, *ESG Defenders Pose as ‘Free Market’ Disciples* (Wall St. J. Op. May 23, 2023), <https://perma.cc/5BLM-VGUA>. With the CAT housing data on every American’s investment decisions, it will be a prime target for

ideologically driven leaks. And with thousands of individuals having access to that data, the risk cannot be understated.

Investors are additionally at risk of being targeted by malicious government action. Investors' trading decisions, which provide a window into their values and beliefs, could also be weaponized against them by those with access to the data. After all, the IRS did just that to hundreds of conservative tax-exempt organizations. Emily Cochrane, *Justice Department Settles With Tea Party Groups After I.R.S. Scrutiny* N.Y. Times (Oct. 26, 2017), <https://perma.cc/SYV8-HH6L>. More recently, whistleblowers revealed that the Department of Justice was using the FBI's Counterterrorism Division to target parents protesting actions by their local school boards. *See* Letter from Jim Jordan and Mike Johnson to Hon. Merrick B. Garland (May 11, 2022), <https://perma.cc/R9UG-69LD>. And even more recently the FBI was caught targeting Catholic congregations for treatment as "violent extremists" for their religious beliefs. *See* Letter from Virginia and 19 other States to Hon. Merrick B. Garland and Hon. Christopher Wray (Feb. 10, 2023), <https://perma.cc/7NXQ-U3H3>.

Suffice it to say that Americans have little reason to trust that their personal information is safe with the federal government. The CAT contains more than enough personally identifiable information to help rogue government actors pick their next targets.

II. The Commission's massive surveillance program is contrary to law.

The Supreme Court has made clear that skeptical scrutiny is warranted where an agency relies on decades-old statutory language to claim authority for massive new programs. The CAT bears all the hallmarks of an instance where the major-questions doctrine counsels against an expansive reading of agency authority. And even if the Commission had the authority it claims here, its exercise of it was arbitrary and capricious.

- A. The Commission has never identified any specific statutory authority for its massive surveillance of retail investors.

The Securities and Exchange Act of 1934 provides the Commission authority to regulate the securities markets for “the protection of investors and the maintenance of fair and orderly markets.” 15 U.S.C. 78k-1(a)(1)(C). Section 11A of the Act, added in 1975, directs the Commission “to use its authority . . . to facilitate the establishment of a national market system for securities.” *Id.* 78k-1(a)(2). In furtherance of that directive, Section 11A authorizes the Commission to “authorize or require self-regulatory organizations to act jointly with respect to matters as to which they share authority . . . in planning, developing, operating, or regulating a national market system.” *Id.* 78k-1(a)(3).

In 2012, the Commission sought for the first time to utilize its authority over the national market system to require national securities exchanges and associations (self-regulatory organizations or “SROs”) to create a single consolidated audit trail. With the adoption of Rule 613, “each SRO and its members” would be required “to capture and report specified trade, quote, and order activity in all [national market system] securities to the central repository in real time, across all markets, from order inception through routing, cancellation, modification, and execution.” *Consolidated audit trail*, 77 Fed. Reg. 45722, 45723 (Aug. 1, 2012). The SROs previously established various separate audit trails, but the Commission believed that a single, centralized one would lead to “(1) improved market surveillance and investigations; (2) improved analysis and reconstruction of broad-based market events; and (3) improved market analysis.” *Id.* at 45730.

But the devil was in the details. For Rule 613 required SROs to record and report to the CAT for each order: (1) “information of sufficient detail to identify the customer”; and (2) “customer account information,” which included “account number, account type, customer type, date

account opened, and large trader identifier (if applicable).” *Id.* at 45749, 45813. 17 C.F.R. 264.613(c)(7)(viii), (j)(4). When the SROs in 2015 submitted their CAT proposal, it spelled out the information that would be collected and stored within the CAT for every retail investor trading on the market: every customer’s name, address, date of birth, Social Security number, and account number. *See CAT NMS Plan*, at sec. 1.1, <https://perma.cc/UH3G-9ZFH>; *Joint Industry Plan; Order Approving the National Market System Plan Governing the Consolidated Audit Trail*, 81 Fed. Reg. 84696, Rel. No. 34-79318, File No. 4-698 (Nov. 15, 2016). The Commission eventually narrowed the information to the investor’s name, address, and birth year. *See Ord. Granting Conditional Exemptive Relief, Pursuant to Section 36 & Rule 608(e) of the Sec. Exch. Act of 1934, from Section 6.4(d)(II)(c) & Appendix D Sections 4.1.6, 6.2, 8.1.1, 8.2, 9.1, 9.2, 9.4, 10.1, & 10.3 of the Nat’l Mkt. Sys. Plan Governing the Consol. Audit Trail*, 85 Fed. Reg. 16152, Release No. 88393 (Mar. 17, 2020) (“Exemption Order”).

This was an enormous shift from how retail-investor data was handled. Investors’ broker-dealers kept this type of information previously and were required to report it to the Commission when requested. *See* 17 CFR 240.17a-25. This electronic “blue sheet” process at least ensured that the Commission had a particularized suspicion about a transaction or customer, otherwise it would not expend the effort to request the information. But the CAT allows the Commission access in real-time to a centralized database containing information submitted by every broker-dealer in the country. And at least 3,000 users will have access at any given time, between the Commission and the CAT Participants. *See Amended CAT NMS Plan for Consolidated Audit Trail*, LLC, FINRA CAT 106 n.61 (Aug. 29, 2019) (stating that although the request for proposals “required support for a minimum of 3,000 users, . . . the actual number of users

may be higher based upon regulator and Participant usage of the system”),
<https://perma.cc/C9KC-FFEX>.

Thus, no longer can an average investor expect that their personal information will generally be kept private unless they are suspected of wrongdoing. The Commission has always had the ability to obtain the information it needs for investigations and enforcement actions, but the CAT provides it with the unprecedented capability to engage in massive surveillance of retail investors. And that significant change hasn’t been authorized by Congress, but has come by administrative fiat.

Congress never authorized the Commission to create this type of centralized repository containing personally identifiable retail-investor information. The Commission has never claimed this authority as arising under any specific portion of the Exchange Act. *See, e.g., Amends. to the Nat’l Mkt. Sys. Plan Governing the Consol. Audit Trail to Enhance Data Sec.*, 85 Fed. Reg. 65990, Release No. 89632 (Aug. 21, 2020), at 66096 (claiming authority generally “[p]ursuant to the Exchange Act and, particularly, Sections 2, 3(b), 5, 6, 1A(a)(3)(B), 15, 15A, 17(a) and (b), 19 and 23(a) thereof”). Nor has it engaged with arguments by commenters that it lacks this authority. *See, e.g., Letter from Christopher A. Iacovella, CEO, American Securities Association to Vanessa A. Countryman, Sec’y Commission* (Nov. 30, 2020), at 17, <https://perma.cc/7BQW-K7KH>.

The Commission claims that Section 11A’s authorization to establish a national market system and to direct joint action by SROs impliedly provides the Commission with the power to order the creation of the CAT. But nowhere in Section 11A’s objectives for the creation of a national market system did Congress mention enforcement efforts or any need for the Commission to have easier access to investors’ personal information. *See* 15 U.S.C. 78k-1(a)(1)(C). That

section’s silence cannot authorize the CAT; after all, “Congress . . . does not alter the fundamental details of a regulatory scheme in vague terms or ancillary provisions—it does not, one might say, hide elephants in mouseholes.” *Whitman v. Am. Trucking Ass’ns, Inc.*, 531 U.S. 457, 468 (2001).

Absent clear statutory language, the Court should be skeptical of the Commission’s authority to enact such an unprecedented surveillance effort of Americans’ personal information.

B. The Commission’s decision to require investors to ultimately bear the cost of its surveillance program further underscores the program’s shaky foundation.

The CAT’s funding mechanism casts further doubt on the notion that Congress ever authorized it. Over a decade after the Commission’s initial move to establish the CAT, the Commission has only now determined how to pay for it. *Joint Indus. Plan; Ord. Approving an Amend. To the Nat’l Mkt. Sys. Plan Governing the Consol. Audit Trail*, 88 Fed. Reg. 62628, Release No. 98290 (Sept. 6, 2023). The Commission’s consideration of the funding mechanism for the CAT centered more on how the CAT participants and industry members would split the costs and less on the fact that investors will ultimately pay the price. And just as significant as who *is* paying for the CAT is who is not—the Commission. One would expect the cost for a government surveillance program of this magnitude to be part of the budget of the agency overseeing it, funded by appropriations and subject to ongoing Congressional oversight. That it is instead funded by fees that will ultimately be passed through to investors should give the Court pause.

1. Investors will ultimately bear the costs of the CAT yet have no role in overseeing its spending.

Whatever the ultimate allocation of costs between industry members and CAT participants, both the Commission and the CAT LLC that will run the database acknowledged that they believe these fees can and will be passed through to investors, including retail investors. *Joint*

Indus. Plan; Ord. Approving an Amend. To the Nat'l Mkt. Sys. Plan Governing the Consol. Audit Trail, 88 Fed. Reg. 62628, Release No. 98290 (Sept. 6, 2023) (“Funding Order”). CAT LLC tacitly acknowledged this could occur, noting that industry members would “not hav[e] any funding burden” for the CAT “if they decide to entirely pass-through their allocation to investors.” *Id.* at 62635; *see also id.* (stating that CAT “Participants are permitted by the Exchange Act to charge their member fees to fund the Participants’ share of CAT fees”). The Commission too recognized that CAT participants and industry members “may each elect to pass on . . . operational costs as fees to customers indirectly,” and this “would be true regardless of how” the initial costs are allocated. *Id.* at 62636.

The Commission’s former Chief Economist, Dr. Lawrence Harris, was not so equivocal and explained to the Commission that “[i]n the short run, who must pay these fees matters because prices often take a while to adjust. But eventually, the retail and institutional traders who use the markets *will* bear these fees.” Letter from Lawrence Harris, USC Marshall Sch. of Bus. to Vanessa Countryman, Sec’y Commission, (June 21, 2022), <https://perma.cc/3WG7-3J69> (emphasis added). Neither the Commission nor CAT LLC offered any refutation of that prediction.

Despite being saddled with millions—and, eventually, billions—in fees to support the CAT, investors have no method to control those costs. CAT user fees are adopted by its operating committee members, who are not accountable to retail investors. And while the Commission is perhaps capable of influencing CAT’s overall budget through oversight of the fees CAT members may charge, the Commission has little incentive to closely scrutinize or constrain costs. After all, the CAT will be a tool to support the Commission’s regulatory and enforcement efforts. No one should reasonably expect the Commission to push back when the CAT participants offer the Commission an increasingly expensive tool for which the Commission does not have to pay.

Thus, investors will not only be subject to the Commission’s unprecedented surveillance but forced to pay for it—all without having any say in the process.

2. The Commission’s decision to fund the CAT through user fees sidesteps Congress’s important role in controlling agency spending.

Courts should be skeptical when agencies enact significant, controversial policy measures that are funded outside the congressional appropriations process, thus removing a key oversight tool on spending and executive-branch overreach.

The Appropriations Clause is one way the Constitution ensures that, among our three branches of government, Congress reaches the “difficult judgments” of government. *OPM v. Richmond*, 496 U.S. 414, 428 (1990). Congress is “uniquely qualified to make spending decisions,” Robert C. Byrd, *The Control of the Purse and the Line Item Veto Act*, 35 Harv. J. On Legis. 297, 315-16 (1998), because it is “our most representative of institutions,” Paul Larkin, Jr. & Zack Smith, “*Brother, Can You Spare A Million Dollars?*”: *Resurrecting the Justice Department’s “Slush Fund,”* 19 Geo. J. L. & Pub. Pol’y 447, 457 (2021). Congressionally led spending is thus the surest way to “the most desirable, balanced, and responsive” results. Abner J. Mikva, *Congress: The Purse, the Purpose, and the Power*, 21 Ga. L. Rev. 1, 3 (1986). It also “force[s] Congress to take ownership of the government’s spending choices, in order to promote accountability and fiscal restraint.” C. Boyden Gray, *Extra Icing on an Unconstitutional Cake Already Frosted? A Constitutional Recipe for the CFPB*, 24 Geo. Mason L. Rev. 1213, 1226 (2017).

The Founders knew that the Appropriations Clause would serve as an important check against overreach by the executive branch. James Madison explained that “[t]his power over the purse may [be] the most complete and effectual weapon with which any constitution can arm the immediate representatives of the people.” *The Federalist*, No. 58. Without it, “the executive would possess an unbounded power.” Joseph Story, *Commentaries on the Constitution of the*

United States § 1348 (3d ed. 1858); *see also, e.g., Laird v. Tatum*, 408 U.S. 1, 15 (1972) (noting that the “power of the purse” allows Congress to effectively monitor the “wisdom and soundness of Executive action”).

That is all the more true when it comes to the modern administrative state in general, and independent agencies in particular. “The budget . . . is a key tool for controlling agencies.” Eloise Pasachoff, *The President’s Budget as a Source of Agency Policy Control*, 125 Yale L.J. 2182, 2186 (2016); *see also* Laura E. Dolbow, *Agency Adherence to Legislative History*, 70 Admin. L. Rev. 569, 579-80 (2018) (explaining how the appropriations process provides an “effective oversight technique” for agencies). Appropriations legislation is often a more readily available tool than substantive legislation due to legislative deadlock. *See* Gillian E. Metzger, *Agencies, Polarization, and the States*, 115 Colum. L. Rev. 1739, 1749 (2015) (explaining that the “great advantage of appropriations legislation from Congress’s perspective is its must-pass status”). It is perhaps Congress’s best way to rein in the independent agencies. *See* Robert E. Cushman, *The Independent Regulatory Commissions* 674-75 (1972) (explaining that congressional oversight of an independent agency’s finances is Congress’s “most constant and effective control”). Indeed, Congress not so long ago slashed the Commission’s budget by hundreds of millions of dollars because it was dissatisfied with the Commission’s enforcement efforts. *See* James B. Stewart, *As A Watchdog Starves, Wall Street Is Tossed a Bone*, N.Y. Times (July 15, 2011), <https://perma.cc/75SJ-UAJM>.

The ability to hold independent agencies accountable through appropriations is especially important to States. That is because “unlike Congress, administrative agencies are clearly not designed to represent the interests of States.” *Geier v. Am. Honda Motor Co.*, 529 U.S. 861, 908 (2000) (Stevens, J., dissenting). Independent agencies especially are “virtually insulated from

political forces” through which States might otherwise influence executive agency policy. David A. Herrman, *To Delegate or Not to Delegate—That Is the Preemption: The Lack of Political Accountability in Administrative Preemption Defies Federalism Constraints on Government Power*, 28 Pac. L.J. 1157, 1181-82 (1997). But States do wield influence in Congress and may use that influence to convince Congress to police specific agency actions, such as attaching an appropriations rider to “single out a specific regulatory activity and prohibit the expenditure of funds for carrying [it] out.” Jack M. Beermann, *Congressional Administration*, 43 San Diego L. Rev. 61, 85 (2006). States can also lobby Congress not to act on an agency’s request to fund a program that the States oppose. *See Metzger, supra* at 1750 (explaining that “congressional influence through appropriations is often felt more through budgetary inaction than actual appropriations legislation”).

By funding its surveillance efforts through CAT user fees, the Commission has taken from States an important tool for voicing opposition to intrusion into their citizens’ lives.

- C. The Supreme Court’s major-questions doctrine requires courts to cast a skeptical eye on new assertions of previously unexercised authority like the Commission’s massive repository of retail-investors’ personal information.

The Commission has existed for nearly a century without having real-time access to the personally identifiable information of every retail investor in America. If Congress had authorized the Commission to build this sort of data repository, whether in the digital age or before, it would have spoken clearly. The major-questions doctrine counsels against allowing agencies to discover new sweeping authority in ambiguous language in longstanding statutes.

In “extraordinary cases,” when “the history and the breadth of the authority that [the Commission] has asserted, and the economic and political significance of that assertion” compel it, courts should “hesitate before concluding that Congress meant to confer such authority.” *West*

Virginia v. EPA, 142 S. Ct. 2587, 2608 (2022) (cleaned up). “This expectation of clarity is rooted in the basic premise that Congress normally intends to make major policy decisions itself, not leave those decisions to agencies.” *Biden v. Nebraska*, 143 S. Ct. 2355, 2380 (2023) (Barrett, J., concurring) (quotation omitted). The Commission’s unprecedented sweeping collection and retention of Americans’ private information bears the hallmarks of such an extraordinary case.

The Commission’s surveillance program is economically significant enough to invoke the major-questions doctrine. As Commissioner Uyeda noted, “cumulative costs for CAT may soon be approaching a billion dollars.” Comm’r Mark T. Uyeda, *Statement on Consolidated Audit Trail Revised Funding Model*, SEC (Sept. 26, 2023), <https://perma.cc/78RY-KN5Q>; *see also* Comm’r Hester M. Peirce, *Who’s Paying?: Statement on the CAT’s Funding Model*, SEC (Sept. 6, 2023), <https://perma.cc/UJV5-J65D> (noting the CAT’s “price tag of more than \$500 million to date and billions to come”).

And the economic impact of the CAT is not limited to its price tag. According to polling, approximately 61% of American adults own stock. *See* Gallup, *What Percentage of Americans Own Stock?* (May 24, 2023), <https://perma.cc/3XKX-X62N>. If left intact, the CAT will contain the personal information of well over a hundred million Americans, stored along with the granular details of their investment activity. *Cf. Ala. Ass’n of Realtors v. Dep’t of Health & Hum. Servs.*, 141 S. Ct. 2485, 2489 (2021) (applying major-questions doctrine where the “sheer scope” of the CDC eviction moratorium would affect “between 6 and 17 million tenants at risk of eviction”). The economic value of such centralized detailed information, both commercially and to foreign interests and hackers, cannot be overstated.

The Commission’s collection of the personal information of retail investors is also politically significant. After all, one cannot put a price on peace of mind, nor calculate the dollar

value of the loss of privacy. Section 702 of the Foreign Intelligence Surveillance Act is a helpful comparison. Section 702 has generated significant controversy due to the FBI's admitted misuse of the tool, including targeting American citizens' communications without a warrant. *See* Devlin Barrett, *FBI misused surveillance tool on Jan. 6 suspects, BLM arrestees and others*, Wash. Post. (May 19, 2023), <https://perma.cc/QRA4-XDD2> (noting evidence that the "FBI has misused a powerful digital surveillance tool more than 278,000 times"). The question of whether Section 702 surveillance should be reformed or even reauthorized at all has generated significant debate in Congress. *See, e.g.,* Sen. Mike Lee, *Congress, don't pass the defense bill without FISA reform* (Dec. 11, 2023), <https://perma.cc/3PG6-JSKV>.

Notwithstanding the controversy Section 702 surveillance has generated in recent years, the program *was* authorized by Congress (and reauthorized multiple times). Yet the Commission's collection of personally identifiable investor information will reach many more American citizens than the FBI's use of Section 702 ever could. And—in addition to the myriad opposing comments the Commission's data-collection requirements has generated since their announcement—Congress has now begun to weigh in. *See* Sen. John Kennedy, *Kennedy, Colleagues Introduce Bill to Protect Investor Privacy by Prohibiting Vulnerable SEC Database* (July 11, 2023), <https://perma.cc/FT2M-5445>; *See* Rep. Barry Loudermilk, *Rep. Loudermilk, House Republicans Introduce Legislation to Protect Investors' Personally Identifiable Information* (July 12, 2023), <https://perma.cc/V799-5X5K>. So the Commission's repository of investor information is sure to become even more politically significant in the future.

Finally, the Commission's actions bring about a "radical or fundamental change" to the privacy and security expectations of American investors. *West Virginia*, 142 S. Ct. at 2609 (cleaned up). The Commission has not in its history had the sort of detailed information

collected in the CAT for retail investors. The change from disclosures being driven by electronic “blue sheets” to the CAT repository is momentous. But “when Congress wishes to alter the fundamental details of a regulatory scheme, . . . we would expect it to speak with the requisite clarity to place that intent beyond dispute.” *United States Forest Serv. v. Cowpasture River Pres. Ass’n*, 140 S. Ct. 1837, 1849 (2020) (cleaned up).

Indeed, shifting the Commission’s regulatory scheme from one where an investor’s sensitive personal information must be requested on the basis of individualized suspicion related to an investigation or enforcement action, to the Commission’s ability with the CAT to view the details of individuals not suspected of any wrongdoing, requires grounding in more than “modest words,” “vague terms,” or “subtle device[s].” *West Virginia*, 142 S. Ct. at 2609. Allowing the Commission, along with thousands of other users, instant access to records of Americans’ market activity coupled with their personally identifiable information would upend investor expectations where the statutory regime hasn’t changed. *See Ala. Ass’n of Realtors*, 141 S. Ct. at 2489 (requiring “Congress to enact exceedingly clear language” to shift traditional balances of power, such as “between federal and state power and the power of Government over private property”).

The Commission’s effort to significantly expand its surveillance abilities by relying on newly found authority under the Exchange Act should be rejected.

- D. The Commission failed to consider whether storing retail-investor information is necessary to further the CAT’s goal of providing the Commission with access to real-time market information.

Even if the Commission had the authority to require the collection of personally identifiable investor information within the CAT, its decision to do so was arbitrary and capricious. The Commission’s inclusion of sensitive personal information within the CAT is risky and offers little, if any, regulatory benefit. And by failing to consider whether it actually needed retail

investors' personal information, the Commission entirely failed to consider "an important aspect of the problem." *Spirit Airlines, Inc. v. FAA*, 997 F.3d 1247, 1255 (D.C. Cir. 2021).

Recall that the original impetus for creating a centralized database of real-time market information was the 2010 "flash crash"; retail investors did not cause that crash. Findings Regarding the Market Events of May 6, 2010, Joint Advisory Comm. on Emerging Regul. Issues (Sep. 30, 2010), <https://perma.cc/F2BJ-85B3>. The Commission found it difficult to reconstruct the events of the crash after the fact because there was "no single data source that covers all market activities." 81 Fed. Reg. 84696, 84811 (Nov. 15, 2016), at 205. Instead, the Commission had to combine different data sources such as blue sheets and individual SRO audit trails. *See id.*

The CAT provides the single comprehensive data source that the Commission said was necessary for that purpose. But the inclusion of sensitive personal information, especially that of retail investors, was never something the Commission said it needed in order to effectively reconstruct disruptive market events like the 2010 "flash crash." Nor would that have been plausible given the unlikelihood that retail investors could ever be responsible for a sudden market event of such significance. To its credit, the Commission did—after significant pushback—trim down the personal information that would be collected, including nixing the collection of Social Security numbers. *See Exemption Order*. But the Commission has never defended the collection of customer names, addresses, and birth year as necessary—or even helpful—to further the CAT's original purpose of reconstructing large-scale market disruptive events.

Instead, the Commission has attempted to justify its collection of personal information based on mere convenience. *See Comm'r Hester M. Peirce, This CAT is a Dangerous Dog*, RealClearPolicy (Oct. 9, 2019), <https://perma.cc/558J-ZWB8> (noting that the Commission's "purpose and rationale [for the CAT] have morphed over time"). For instance, the Commission

argued customer information will “allow regulators to identify bad actors who are using retail trading accounts to perform illegal activity” and to identify fraudulent activity targeting senior citizens. Exemption Order at 16156. But as Commissioner Peirce explained, the Commission “already has sufficient tools to get the information it needs to pursue credible leads about market misconduct and to do so quickly.” *Id.* And that is without personally identifiable retail-investor information being available at the fingertips of its enforcement division.

Indeed, the Commission has never claimed—nor could it credibly do so—that omitting this information from the CAT would pose any significant barrier to its enforcement efforts. Rather, at most “the CAT may make it a bit easier to investigate certain types of market misconduct” and may allow the Commission’s enforcement efforts to “avoid the[] occasional problem[]” of broker-dealers responding less than promptly to “blue sheets” requesting customer account information. Comm’r Hester M. Peirce, *Statement of Hester M. Peirce in Response to Release No. 34-88890; File No. S7-13-19*, SEC (May 15, 2020), <https://perma.cc/G4HL-M7EU>.

Mere convenience cannot justify the sweeping collection and retention of personal information from investors whom no one suspects of wrongdoing—let alone putting that information in the hands of an agency with a record of failing to secure its computer systems. As Commissioner Peirce aptly put it, “[t]he risk that a bus driver placing a trade for her daughter’s college fund will cause market turbulence is outweighed by the invasion of privacy and the attendant risk that cybercriminals will deplete the college education fund.” Peirce, *This CAT is a Dangerous Dog*. The Commission’s failure to analyze that important problem was arbitrary and capricious.

CONCLUSION

The Court should grant Plaintiffs’ motion and grant a stay and preliminary injunction halting the CAT program.

Dated: August 16, 2024

Respectfully submitted,

TIM GRIFFIN
Attorney General of Arkansas

/s/ Dylan L. Jacobs

Nicholas J. Bronni (AR2016097)

Solicitor General

Dylan L. Jacobs (AR2016167)

Deputy Solicitor General

OFFICE OF THE ARKANSAS ATTORNEY

GENERAL

323 Center Street, Suite 200

Little Rock, AR 72201

(501) 682-6302

Dylan.Jacobs@ArkansasAG.gov

Counsel for Amici Curiae

ADDITIONAL STATES REPRESENTED

STEVE MARSHALL
Alabama Attorney General

CHRIS CARR
Georgia Attorney General

RAÚL R. LABRADOR
Idaho Attorney General

THEODORE E. ROKITA
Indiana Attorney General

BRENNA BIRD
Iowa Attorney General

KRIS W. KOBACH
Kansas Attorney General

LIZ MURRILL
Louisiana Attorney General

LYNN FITCH
Mississippi Attorney General

ANDREW BAILEY
Missouri Attorney General

AUSTIN KNUDSEN
Montana Attorney General

MICHAEL T. HILGERS
Nebraska Attorney General

ALAN WILSON
South Carolina Attorney General

MARTY JACKLEY
South Dakota Attorney General

JONATHAN SKRMETTI
Tennessee Attorney General and Reporter

KEN PAXTON
Texas Attorney General

SEAN REYES
Utah Attorney General

JASON MIYARES
Virginia Attorney General

PATRICK MORRISEY
West Virginia Attorney General