Filed Electronically

November 30, 2020

Ms. Vanessa A. Countryman
Secretary
Securities and Exchange Commission
100 F Street, NE,
Washington, DC 20549-1090.

Re: Proposed Amendments to the National Market System Plan Governing the Consolidated Audit Trail to Enhance Data Security; Release No. 34-89632; File No. S7-10-20; RIN 3235-AM62

Dear Secretary Countryman:

The American Securities Association (ASA)[1] writes to express its opposition to the Commission's proposal to collect "Customer and Account Attributes" through the CAT. These data elements include name, address, year of birth, individual's role in the account, account type, customer type, date account opened, and large trader identifier. The Commission has asked for comments on whether its definition of "Customer and Account Attributes" should be "modified to add or delete data elements." ASA strongly urges the Commission not to collect *any* of the data elements it proposes to collect through "Customer and Account Attributes."

First, collecting "Customer and Account Attributes" would be arbitrary and capricious. The Commission proposes to collect data that will give the government a comprehensive surveillance database of the investment decisions of millions of Americans. The Commission will have real-time knowledge of every investor's trading activity. Thousands of government and private actors will have access to this database, and they may monitor the investment decisions without *any* suspicion of wrongdoing. In fact, at an October 2019 Senate Banking Committee hearing, the Chief Operating Officer of the CAT stated that roughly 3,000 individuals would have access to the confidential personal information collected by the CAT.[2]

[1] The ASA is a trade association that represents the retail and institutional capital markets interests of regional financial services firms who provide Main Street businesses with access to capital and advise hardworking Americans how to create and preserve wealth. The ASA's mission is to promote trust and confidence among investors, facilitate capital formation, and support efficient and competitively balanced capital markets. This mission advances financial independence, stimulates job creation, and increases prosperity. The ASA has a geographically diverse membership base that spans the Heartland, Southwest, Southeast, Atlantic, and Pacific Northwest regions of the United States.

[2] "Oversight of the Status of the Consolidated Audit Trail," Senate Banking Committee (Oct. 22, 2019), https://bit.ly/33nifqw.

This government surveillance will inflict enormous harms on American investors. The data the CAT will collect through "Customer and Account Attributes" is not dry economic data. They may reflect the moral, ethical, or religious beliefs of investors. For example, whether to buy or sell stocks in energy companies, weapons manufacturers, or defense contractors (just to name a few) are often colored by the investors' personal beliefs about the morality of the companies' actions. Government surveillance inevitably chills individuals' investment decisions.

A CAT database that collects "Customer and Account Attributes" also will be an enormously inviting target for cybercriminals. Cybercriminals could learn and exploit the trading strategies or positions of certain investors. Cybercriminals could threaten to expose investors' confidential business relationships or the fact that the Commission has been monitoring their activities. Cybercriminals also could use these data elements to gain access to individuals' brokerage accounts and steal their investments. Government and private actors with authorized access to the CAT could engage in similar misconduct. None of the Commission's recent security decisions alleviate these concerns.

At the same time, the Commission has no need to collect "Customer and Account Attributes." The original impetus of the CAT was to create a single, consolidated audit trail, so that the Commission would no longer need to cobble together separate SRO audit trails into a single database. The CAT remedies these problems. The Commission has no persuasive justification for collecting "Customer and Account Attributes."

Second, collecting "Customer and Account Attributes" violates the Fourth Amendment. The Fourth Amendment protects the people from "unreasonable searches and seizures." Here, the Commission proposes to sweep in voluminous personal data about investment activities without *any* suspicion of wrongdoing. The Commission also offers no opportunity for precompliance review; broker-dealers and others *must* produce this data or face severe penalties. This blunderbuss approach is incompatible with the Fourth Amendment's protections of privacy.

Third, the Commission has no statutory authority to collect "Customer and Account Attributes." Congress never passed legislation ordering the Commission to create the CAT or collect "Customer and Account Attributes." Yet the Commission has barreled ahead by relying on a laundry list of statutory provisions, none of which give the Commission this authority.

Fourth, the non-delegation doctrine prevents the Commission from collecting "Customer and Account Attributes." Under the non-delegation doctrine, Congress must provide agencies with an "intelligible principle" to guide their actions. Any statutory provision the Commission relies on for authority to collect "Customer and Account Attributes" would be so broad and vague as to fail this requirement.

Fifth, the proposed rule is unlawful because the structure of the SEC violates the separation of powers. Article II of the Constitution provides that the "executive Power shall be vested in a President of the United States of America," and that power includes the ability to supervise and remove the agents who wield the executive power. SEC Commissioners, however, are given five-

year terms and can be removed only for cause. This unconstitutional structure prevents the Commission from adopting and enforcing the proposed rule.

Sixth, the proposed rule would violate the Constitutional right to privacy and the First Amendment. There is a constitutionally protected interest in the confidentiality of financial transactions and personal financial information. The Commission's proposed rule would violate these rights by forcing the disclosure of *every* investors' financial transactions without *any* evidence of wrongdoing. The Commission's proposed rule is constitutionally untenable.

Finally, collecting "Customer and Account Attributes" would violate the E-Government Act. The E-Government Act requires federal agencies to conduct a privacy impact assessment before developing or procuring information technology that collects information and before initiating a new collection of information. Despite these requirements, however, the Commission has failed to conduct or publish a privacy impact assessment.

For the foregoing reasons, and as explained further below, ASA urges the Commission to not collect any of the data elements identified as "Customer and Account Attributes."

BACKGROUND

A. Rule 631 and the Creation of the Consolidated Audit Trail

On July 18, 2012, the Commission adopted a new rule, 17 C.F.R §242.613, known as "Rule 613." *See Consolidated Audit Trail*, Rel. No. 34-67457; File No. S7-11-10 (July 18, 2012), bit.ly/2BoXsrZ. Rule 613 required national securities exchanges and associations (self-regulatory organizations or "SROs") to jointly submit a plan to the SEC that would govern the creation, implementation, and maintenance of a consolidated audit trail ("CAT"), including a central repository to receive and store CAT data.

Rule 613 required "each SRO and its members to capture and report specified trade, quote, and order activity in all [National Market System ("NMS")] securities to the central repository in real time, across all markets, from order inception through routing, cancellation, modification, and execution." *Id.* at 7 (citation omitted). In doing so, the CAT would replace the patchwork-quilt of existing SRO audit trails with a single audit trail that the Commission could use to track and monitor all securities trading in the U.S. markets. *See id.* The Commission believed that the CAT 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 34.

To create the CAT, Rule 613 required the SROs to submit a plan to the SEC (the "CAT NMS Plan") that would govern the creation, implementation, and maintenance of the CAT. *See* 17 C.F.R. §264.613(a)(1). Rule 613 set forth minimum requirements that the SROs had to include in the NMS plan. Relevant here, 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 must include "account number, account type, customer type, date account opened, and large trader identifier (if applicable)." *Id.* §264.613(c)(7)(viii), (j)(4).

B. The CAT NMS Plan

In 2015, the SROs submitted the CAT NMS plan required by Rule 613, and on November 15, 2016, the Commission approved the plan. *See Joint Industry Plan; Order Approving the National Market System Plan Governing the Consolidated Audit Trail*, Rel. No. 34-79318, File No. 4-698 (Nov. 15, 2016), bit.ly/2QTl4tR; CAT NMS Plan, bit.ly/3lzQ274. The approved CAT NMS Plan provided for the implementation of the CAT. *Joint Industry Plan* at 5-8. Relevant here, the CAT NMS Plan ordered SROs, through their compliance rules, to require Industry Members[3] to record and report for each order "Customer Identifying Information" and "Customer Account Information" for the relevant "Customer."[4] *See* CAT NMS Plan, §§6.4(d)(ii)(C), 6.4(d)(iv). "Customer Identifying Information" was defined to include "name, address, date of birth, individual tax payer identification number ("ITIN")/social security number ("SSN"), [and the] individual's role in the account (e.g., primary holder, joint holder, guardian, trustee, person with the power of attorney)." *Id.* §1.1. "Customer Account Information" was defined to include, but not be limited to: "account number, account type, customer type, date account opened, and large trader identifier." *Id.* §1.1; *see* 17 C.F.R. §264.613(j)(4).

C. Criticism of the Commission's Collection of Personally Identifiable Information

Following the adoption of the CAT NMS Plan in 2016, the CAT "started to attract an enormous amount of criticism and concern regarding cybersecurity." James Rundle & Anthony Malakian, *CAT's Tale: How Thesys, the SROs and the SEC Mishandled the Consolidated Audit Trail*, WatersTechnology (Feb. 14, 2019), bit.ly/2Z9jvfn. "A number of major breaches had occurred already in 2017: credit agency Equifax had been compromised by criminals, exposing the personal data of tens of millions of Americans, and even the Commission's company filings system was breached, resulting in fears that personally identifiable information had potentially been compromised." *Id.*

Congress took notice, holding multiple hearings into "what information the CAT would be collecting, and how it would be protected." *Id.* In these hearing, witnesses repeatedly raised concerns about the CAT's collection of traders' personal and financial information. *See, e.g.*, *Implementation and Cybersecurity Protocols of the Consolidated Audit Trail*, Hearing before the U.S. H.R. Comm. on Fin. Servs. (Nov. 30, 2017), bit.ly/2ZqAl8p, *id.* (testimony of Lisa Dolly, CEO of the Securities Industry and Financial Markets Association), bit.ly/2ASDlCp (warning

[3] "Industry Member" means "a member of a national securities exchange or a member of a national securities association." CAT NMS Plan §1.1.

[4] "Customer" means "[t]he account holder(s) of the account at a registered broker-dealer originating the order," and "[a]ny person from whom the broker-dealer is authorized to accept trading instructions for such account, if different from the account holder(s)." 17 C.F.R. §242.613(j)(3); *see* CAT NMS Plan §1.1.

Congress that "the CAT will contain a significant amount of sensitive information," including the "personally identifiable information ('PII') of individual customers" and that "the SEC and the SROs should have to make the case that the CAT's collection, storage, and use of PII . . . is required for effective surveillance"); *id.* (testimony of Chris Concannon, President and COO of Cboe Global Markets, Inc.), bit.ly/31PwUuS (raising "concern[s] about the risks associated with storing PII in the CAT database"); *see also id.* (statement of Rep. Bill Huizenga), bit.ly/3dKWFi5 (identifying "very serious concerns about the security of such extraordinary amounts of personally identifiable information being collected and held by the CAT").

In 2019, the Commission received letters and comments urging the agency to stop collecting PII through the CAT. In July 2019, a coalition of senators sent a letter to the Commission expressing grave national security concerns:

> 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. . . . 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. . . . [W]e 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.

Sen. John Kennedy, et al., Letter to SEC (July 24, 2019), bit.ly/2A1E5oi.

ASA also urged the Commission on multiple occasions to stop collecting PII. *See* ASA, Comment on SEC Proposed Rulemaking (Oct. 28, 2019), bit.ly/2Rg5k2V; ASA, Letter to SEC and CAT NMS Plan Participants (May 16, 2019), bit.ly/3egvJqR; ASA, Letter to SEC (Feb. 25, 2019), bit.ly/3iQ7e7A. ASA explained that (1) PII collection "will do nothing to support the mission of the CAT and will only subject the PII of millions of Americans to theft from cybercriminals"; (2) there is "no compelling reason for the collection of any PII under the CAT"; (3) "the costs associated with collecting PII vastly outweigh any benefit to investors or the SEC's ability to oversee markets"; and (4) "[t]he SEC does not need PII to conduct market surveillance and police bad actors." ASA, Comment on SEC Proposed Rulemaking (Oct. 28, 2019), bit.ly/2Rg5k2V.

Others made similar arguments and requests. The American Civil Liberties Union wrote a letter to Chairman Clayton expressing dismay that "the CAT will collect and store far too much [PII]" and urging the Commission to "consider further measures to limit the personal information maintained by the CAT." ACLU, Letter to SEC (Dec. 16, 2019), bit.ly/2Nk9oh8. And Commissioner Peirce criticized the CAT's enormous collection of customers' personal and financial information, arguing that it would create a database "so vast and so attractive to hackers that it will be hard to protect" from cybercriminals. Comm'r Hester M. Peirce, *This CAT is a Dangerous Dog*, RealClearPolicy (Oct. 9, 2019), bit.ly/3fTxTxE.

These arguments made clear that a broad, diverse coalition of market participants and civil liberty advocates agreed that there was no benefit—and significant potential harm—from personally identifiable information being collected under the CAT.

D. The Commission's Notice of Proposed Rulemaking

On August 21, 2020, the Commission filed a notice of proposed rulemaking that proposed a change in how the CAT collected personally identifiable information. *See Proposed Amendments to the National Market System Plan Governing the Consolidated Audit Trail to Enhance Data Security*, Rel. No. 34-89632; File No. S7-10-20 (Aug. 21, 2020), bit.ly/3hVkVRB ("NPRM"). The Commission proposed to no longer collect "PII" or "Personally Identifiable Information." *Id.* at 99-106, 355-57; *see* CAT NMS Plan, §1.1 (defining "PII"). Instead, Industry Members will be required to record and report "Customer and Account Attributes." *Id.* at 409. The Commission proposed to define "Customer Attributes" as "information of sufficient detail to identify a Customer, including, but not limited to . . . name, address, year of birth, [and] individual's role in the account." *Id.* at 404. The Commission proposed to define "Account Attributes" as "account type, customer type, date account opened, and large trader identifier (if applicable)." *Id.* at 403.

The Commission also asked for comments on whether it should go further and not collect *any* customer and account information. *Id.* at 106. The NPRM stated: "The proposed amendments define 'Customer and Account Attributes' as meaning the data elements in Account Attributes and Customer Attributes. Do commenters believe these definitions should be modified to add or delete data elements? If so, what elements?" *Id.*

COMMENTS

The Commission has proposed to collect "Customer and Account Attributes," which include "name, address, year of birth, individual's role in the account" and "account type, customer type, date account opened, and large trader identifier." NPRM at 403-04 (cleaned up). The Commission also has asked whether its definition of "Customer and Account Attributes" should be "modified to add or delete data elements." *Id.* at 106. As explained below, ASA strongly urges the Commission not to collect *any* of the data elements contained in its proposed definitions.

I. Collecting "Customer and Account Attributes" Will Cause Extraordinary Harms to American Investors and Achieve Minimal Benefits

Under the Administrative Procedure Act ("APA"), "[f]ederal administrative agencies are required to engage in reasoned decisionmaking." *Michigan v. EPA*, 576 U.S. 743, 750 (2015) (citation omitted). An agency rule is "arbitrary and capricious" if, among other things, the agency "fail[s] to consider an important aspect of the problem" or "offer[s] an explanation for its decision that runs counter to the evidence before the agency." *Motor Vehicle Mfrs. Ass'n of U.S., Inc. v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983). As explained below, collecting "Customer and Account Attributes" would be arbitrary and capricious given the enormous harms it will cause and the minimal (if any) benefits it will create.

A. Collecting "Customer and Account Attributes" Threatens Americans' Privacy from Unwarranted Government Surveillance and Cybercriminals

If the Commission collects "Customer and Account Attributes" in the CAT, the CAT will become a "comprehensive surveillance database." Statement of Hester M. Peirce in Response to Release No. 34-88890; File No. S7-13-19 (May 15, 2020), bit.ly/3gUHeqp ("Peirce Statement"). It will not be, as some may believe, "an innocuous repository of dry economic data." *Id.* Rather, the Commission will have at its fingertips a "comprehensive record of decisions made by millions of Americans." *Id.* It will know "every equity and option trade and quote, from every account at every broker, by every investor." *Id.*

Moreover, the Commission has placed few constraints on who may access this extraordinary trove of data. On the contrary, "[b]ecause the surveillance function requires eyes to watch and minds to interpret the data, *thousands* of Commission staff and employees of the participants must have access to the database." *Id.* (emphasis added). The CAT "is required to be able to support a minimum of 3,000 users at one time," and "the actual number of users may be higher." *Id.* at n.15 (citing *Amended CAT NMS Plan for Consolidated Audit Trail, LLC*, FINRA CAT, 106 n.61 (Aug. 29, 2019)). These users—a combination of SRO and Commission employees—will have "access 'to every trade, from every account, from every broker, for every retail investor in America.'" SIFMA, *Senate Banking Committee Hearing on the CAT* (Oct. 22, 2019) (quoting Sen. Tom Cotton), bit.ly/33hrSqM. And these users will be able to download data from the CAT in bulk. *See* CAT NMS Plan §6.10(c).

The Commission also has not placed proper limits on *when* the CAT data may be accessed. The SROs and the Commission can access the CAT's data at any time and for almost any reason—all they need is a "surveillance [or] regulatory purpose[]" for gaining access. 17 C.F.R. §242.613(e)(4)(i)(A); CAT NMS Plan §6.5(g). This is a virtually limitless standard.

Collecting "Customer and Account Attributes" in the CAT database will cause significant harm to investors and create enormous and unnecessary risks to investors. ASA describes some of these harms and risks below.

The Threat to Individual Freedom. Collecting "Customers and Account Attributes" will allow the Commission to create an unprecedented surveillance program that will impose substantial costs on individual freedoms. "The non-financial costs of being surveilled reach to the very core of our humanity." Peirce Statement. Freedom of thought, expression, and action are "the basis of our national strength and of the independence and vigor of Americans." *Tinker v. Des Moines Indep. Cmty. Sch. Dist.*, 393 U.S. 503, 508-09 (1969). But "[u]ntargeted government surveillance programs, even well-intentioned ones, threaten that freedom." Peirce Statement. That is because "[a]wareness that the government may be watching chills" individuals' activities. *United States v. Jones*, 565 U.S. 400, 416 (2012).

Economic transactions, such as the purchases and sales of stocks, can "offer a window into a person's deepest thoughts and core values." Peirce Statement. It is important to human "dignity"

to have "personal privacy" over data related to economic transactions. *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 579-80 (2011); *see also Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018) (the fact that "records are generated for commercial purposes . . . does not negate [an] anticipation of privacy"). Economic activity might "express a view of how markets work, a determination on the efficiency of markets, expectations about the future, or even a moral philosophy." Peirce Statement. For example, "an investor may purchase shares of a clothing company because he likes the political messages of its celebrity spokesperson or shares of a restaurant chain because it donates to his favorite charity." *Id.* Another investor "may choose to avoid or sell companies that are associated with things he opposes," such as carbon emissions, tobacco, and guns. *Id.* Sensitive and valuable economic data that an investor "intend[s] to be kept confidential" is her "property," and should be respected as such. *Carpenter v. United States*, 484 U.S. 19, 28 (1987).

"Investors whose trades are not a direct reflection of granular moral, ethical, or religious beliefs may fear rebukes from other people who view trading decisions as morally motivated." Peirce Statement. Investors could face public pressure for investing in energy companies, cigarette manufacturers, or weapons makers. Or investors could be publicly shamed for *not* investing in companies that some consider to be more beneficent to society, such as those that score high on Environmental, Social, and Governance ("ESG") factors. *See* Comm'r Hester M. Peirce, *Scarlet Letters: Remarks before the American Enterprise Institute*, (June 18, 2019), bit.ly/3pCbaMh. "[I]n our modern corporate ESG world, there is a group of people who take the lead in instigating their fellow citizens into a frenzy of moral rectitude. Once worked up, however, the crowd takes matters into its own brutish hands and finds many ways to exact penalties from the identified wrongdoers." *Id.*

Accordingly, "compelled disclosure" of investors transactions could lead to "fear of exposure of their beliefs . . . and of the consequences of this exposure." *NAACP v. State of Ala. ex rel. Patterson*, 357 U.S. 449, 463-64 (1958). Although the Commission and SROs have no plan to assess investor virtue, "today's good intentions do not protect against tomorrow's bad actors." Peirce Statement. "One 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." *Id.* "[O]ur Constitution was designed to avoid these ends by avoiding [their] beginnings." *W. Virginia State Bd. of Educ. v. Barnette*, 319 U.S. 624, 641 (1943).

Improper Commission Investigations and Enforcement Actions. The collection of "Customer and Account Attributes" also will increase the likelihood of improper enforcement actions. "Staff at the Commission and at the exchanges will wade through the data pool to troll for securities violations." Comm. Hester M. Peirce, *Intellectual Siren Song*, (Sept. 18, 2020), bit.ly/3lT0wyN. Tracking "unsuspected and unsuspecting Americans' every move in the hopes of catching them in some wrongdoing" is not "consistent with the principles undergirding the Constitution." *Id.* As the D.C. Circuit has recognized, "[a]gencies are . . . not afforded 'unfettered authority to cast about for potential wrongdoing." *Consumer Fin. Prot. Bureau v. Accrediting Council for Indep. Colleges & Sch.*, 854 F.3d 683, 689 (D.C. Cir. 2017) (quoting *In re Sealed Case (Admin. Subpoena)*, 42 F.3d 1412, 1418 (D.C. Cir. 1994)).

Even if the Commission stops short of bringing an enforcement action, the Commission will have the ability to force individuals to "explain [their] actions, potentially at great expenses[,] even if [they] know [they] did nothing wrong." Comm'r Hester M. Peirce, *This CAT is a Dangerous Dog*, RealClearPolicy (Oct. 9, 2019), bit.ly/3fTxTxE. Indeed, "[m]erely being made the subject of an SEC investigation may involve high costs to an investigatee." Judith Bellamy Peck, *The Ninth Circuit's Requirement of Notice to Targets of Third Party Subpoenas in SEC Investigations-A Remedy Without A Right*,59 Wash. L. Rev. 617, 619 (1984). An investigatee may "spend large amounts of time and money in defending against the investigation and responding to agency requests for information" and may also face "a less direct but potentially more serious danger—damage to business reputation." *Id*. In short, the process itself becomes punishment.

The Threat of Cybercriminals. Collecting "Customer and Account Attributes" also increases the danger that Americans will fall prey to cybercriminals. "Every trade from every account at every broker for every retail investor in the U.S. recorded in a single place—the risks to the American investor are staggering." Comm'r Hester M. Peirce, This CAT is a Dangerous Dog, RealClearPolicy (Oct. 9, 2019), bit.ly/3fTxTxE.

The Commission believes that its proposal to eliminate the collection of social security numbers, account numbers, and dates of birth from the CAT will "reduce both the attractiveness of the database as a target for hackers and the impact on retail investors in the event of a data breach." NPRM at 105. To be sure, refraining from collecting certain data (like social security numbers) is a good first step. But serious risks remain. The data elements contained in "Customer and Account Attributes" are still highly valuable to cybercriminals.

First, a security breach could "leak highly-confidential information about trading strategies or positions, which could be deleterious for market participants' trading profits and client relationships." *Joint Industry Plan* at 705. For example, knowledge that a respected investor was buying shares of a certain company could cause others to do the same, unfairly driving up the price of the stock. *See, e.g.*, *What is Front Running?*, Corporate Financial Institute, bit.ly/3ku91i1 (describing "front running," the "practice of purchasing a security based on advance non-public information regarding an expected large transaction that will affect the price of a security"); Liz Moyer, *How Traders Use Front-Running to Profit From Client Orders*, The New York Times (July 20, 2016), nyti.ms/2ICJQfY (same). And knowledge of other institutional investors' private trading patterns could expose proprietary trading strategies, undermining investments into sophisticated trading methods. *See* Jane Croft, *Citadel Securities Sues Rival Over Alleged Trading Strategy Leak*, Financial Times (Jan. 10, 2020), on.ft.com/3nkbFZs (describing accusations that GSA Capital Partners stole Citadel Securities' confidential trading algorithms, which Citadel had spent $100 million to develop).

Second, a data breach could "expose proprietary information about the existence of a significant business relationship with either a counterparty or client, which could reduce business profits." *Joint Industry Plan* at 705. For example, a government report was recently leaked that showed that "a number of banks—JPMorgan, HSBC, Standard Chartered Bank, Deutsche Bank

and Bank of New York Mellon among them—have continued to profit from illicit dealings with disreputable people and criminal networks despite previous warnings from regulators." *Bank Shares Slide on Report of Rampant Money Laundering*, The Associated Press (Sep. 21, 2020), bit.ly/3ppBNEk. This news caused these companies' stocks to sharply decline. *Id.* Similar leaks from the CAT could cause the same harms.

Third, a breach that reveals the activities of regulators, such as data on the queries and processes run on query results, could "compromise regulatory efforts or lead to speculation that could falsely harm the reputation of market participants and investors." *Joint Industry Plan* at 706. For example, when government officials leaked a Federal Trade Commission investigation into Facebook the company's stock "briefly fell into bear market territory, more than 20 percent off its 52-week high." Sara Salinas, *Facebook Stock Slides After FTC Launches Probe of Data Scandal*, CNBC (Mar. 26, 2018), cnb.cx/38AOB4y.

Fourth, a data breach could allow cybercriminals to gain access to individuals' brokerage accounts and steal their investments. Knowing certain information about an individual (*e.g.*, name, address, birth year, recent trades) can help a cybercriminal gain access to a brokerage account. *See* Casey Bond, *How Hackers Can Use Your Boarding Pass To Easily Steal Personal Information*, Huffington Post (Dec. 5, 2019), bit.ly/38HkYyy ("Using personal details such as name, phone number, birthday, etc., there's a good chance that the hacker can have [a] password reset."); *Why Your Birth Date is Important to Hackers?*, Hackology (June 24, 2018), bit.ly/3lx2eFR ("Reveal your birth-date . . . your relatives . . . your address . . . and before you know it hackers are able to pull together a huge amount of data point[s] which leads them to their final act 'Hacking the Victim.'"). For example, a cybercriminal with knowledge of a person's name, address, and recent trades could impersonate a broker-dealer and gain access to a customer's account. Indeed, just last month, hackers infiltrated the popular Robinhood Markets' mobile investment platform, which average investors use for trading stocks, ETFs, options, and crytpo-currency. Through this attack, "2,000 Robinhood Markets accounts were compromised," allowing hackers to "siphon[] off customer funds." Sophie Alexander, *Robinhood Internal Probe Finds Hackers Hit Almost 2,000 Accounts*, Bloomberg Wealth (Oct. 15, 2020), bloom.bg/35Gy7oG. "Several victims said they found no sign of criminals compromising their email accounts." *Id.* "And some said their brokerage accounts were accessed even though they had set up two-factor authentication." *Id.* These kinds of sophisticated attacks will only continue in frequency as hackers and their tactics become more sophisticated. *See CrowdStrike Global Threat Report Reveals Big Game Hunting, Telecommunication Targeting Take Center Stage for Cyber Adversaries*, CrowdStrike (Mar. 23, 2020), bit.ly/32QLxhz.

The Commission believes that some of the recent security measures it has implemented will protect the CAT from cybercriminals. *See* NPRM at 9-10. This is wishful thinking. With every year that goes by, cybercrime increases in severity, frequency, and sophistication. During 2019, "financially motivated cybercrime activity occurred on a nearly continuous basis," with hackers "increasingly . . . conducting data exfiltration, enabling the weaponization of sensitive data through threats of leaking embarrassing or proprietary information." *See CrowdStrike Global Threat Report*, bit.ly/32QLxhz. Indeed, the Commission recently issued new warnings about

ransomware, and Chairman Clayton has stressed that "[c]yber risks . . . [are] there, and they're there more than ever." Kevin Stankiewicz & Bob Pisani, *Cybersecurity Threats to Corporate America are Present Now 'More Than Ever,' SEC Chair Says*, CNBC (Nov. 2, 2020), cnb.cx/36w6sqL.

One well-known instance of Chinese cybercrime is the Equifax hack, which was done by four members of the Chinese People's Liberation Army. According to the Department of Justice, Chinese hackers were able to penetrate Equifax's security, and after a period of surveillance, "were able to download and exfiltrate" enormous amounts of data, including personal and financial information. *See* U.S. Dep't of Justice, *Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax* (Feb. 10, 2020), bit.ly/3mInj0I. This attack was an "organized and remarkably brazen criminal heist of sensitive information of nearly half of all Americans . . . by a unit of the Chinese military." *Id.*

Similarly, in August 2019 and August 2020, Chinese hackers victimized "over 100 . . . companies in the United States and abroad, including software development companies, computer hardware manufacturers, telecommunications providers, social media companies, video game companies, non-profit organizations, universities, think tanks, and foreign governments, as well as pro-democracy politicians and activists in Hong Kong," stealing, among other things, "customer account data[] and valuable business information." U.S. Dep't of Justice, *Seven International Cyber Defendants, Including "Apt41" Actors, Charged in Connection with Computer Intrusion Campaigns Against More Than 100 Victims Globally* (Sept. 16, 2020), bit.ly/2HmrhMw.

In 2018, the Chinese government hacked Marriott International, Inc., potentially stealing the personal information of up to 500 million people. *See* Eric Geller, *Pompeo Says China Hacked Marriott*, Politico (Dec. 12, 2018), politi.co/3mF6eow. In 2015, the Chinese government hacked the Office of Personnel Management, stealing "Social Security numbers and other sensitive information on 21.5 million people who [had] undergone background checks for security clearances," and other "data on about 4.2 million current and former federal workers," in total impacting "almost 7 percent of the U.S. population." Patricia Zengerle & Megan Cassella, *Millions More Americans Hit by Government Personnel Data Hack*, Reuters (July 9, 2015), reut.rs/3oLxV0b.

Indeed, the Commission itself has been victimized by foreign hackers in the recent past. In early 2019, the Department of Justice indicted two Ukrainian men for "a large-scale, international conspiracy to hack into the [Commission's] computer systems and profit by trading on critical information they stole." U.S. Dep't of Justice, *Two Ukrainian Nationals Indicted in Computer Hacking and Securities Fraud Scheme Targeting U.S. Securities and Exchange Commission* (Jan. 15, 2019), bit.ly/2J4SEvh. These men "hacked into the [Commission's] Electronic Data Gathering, Analysis and Retrieval (EDGAR) system and stole thousands of files . . . [and] then profited by selling access to the confidential information in these reports and trading on this stolen information prior to its distribution to the investing public." *Id.* "To gain access to the [Commission's] computer networks, the defendants used a series of targeted cyber-attacks, including directory traversal attacks, phishing attacks, and infecting computers with malware." *Id.*

Eliminating the collection of "Customer and Account Attributes" would significantly lessen these risks from cybercriminals. Indeed, as the Commissions has recognized, "the most secure approach to addressing any piece of sensitive retail [data] would be to eliminate its collection altogether." *Order Granting Conditional Exemptive Relief, Pursuant to Section 36 and Rule 608(e) of the Securities Exchange Act of 1934, from Section 6.4(d)(ii)(C) and Appendix D Sections 4.1.6, 6.2, 8.1.1, 8.2, 9.1, 9.2, 9.4, 10.1, and 10.3 of the National Market System Plan Governing the Consolidated Audit Trail*, Rel. No. 34-88393, at 19, (Mar. 17, 2020), bit.ly/31ys450 ("Exemptive Order").

Government Abuses and Leaks. The collection of "Customer and Account Attributes" also increases the risk that government officials or others with access to the CAT will abuse the CAT for personal gain. Just as cybercriminals profit from stealing and selling individuals' private data, officials operating the CAT could acquire and trade investor data for their own gain. Indeed, they would have an even greater opportunity to profit than cybercriminals, since they could obtain the data without hacking into the CAT.

In addition, government officials also could leak an individual's trading data in order to harm that person's reputation. As explained, individuals' purchases and sales of securities can reveal sensitive information about a person's morals, political beliefs, and finances, and there have been numerous examples of government officials leaking sensitive information to the public. *See, e.g.*, Kim Zetter, *Bradley Manning to Face All Charges in Court-Martial*, Wired (Feb. 3, 2012), bit.ly/34Ft8VK (discussing the leak of over 250,000 United States diplomatic cables, more than 400,000 classified army reports from the Iraq War, and about 90,000 army reports from the war in Afghanistan); Tony Capra, *Snowden Leaks Could Cost Military Billions: Pentagon*, NBC News (Mar. 6, 2014), nbcnews.to/2HINvbO (discussing leak of classified documents pertaining to, among other things, the United States' "military capabilities, operations, tactics, techniques and procedures"). One study found that *42 percent* of government officials believe that it is appropriate to leak information to the press. David E. Pozen, *The Leaky Leviathan: Why the Government Condemns and Condones Unlawful Disclosures of Information*, 127 Harv. L. Rev. 512, 528 (2013).

In short, the danger of government officials abusing and misusing investor data is real, and it is too significant to justify the Commission's unnecessary proposal to collect "Customer and Account Attributes."

B. The Commission Can Achieve Its Regulatory Goals Without Collecting "Customer and Account Attributes"

The Commission has failed to articulate a persuasive reason for collecting "Customer and Account Attributes." To begin, the Commission can achieve its regulatory goals without collecting "Customer and Account Attributes." The CAT was originally conceived as a "tool designed to make it easier for the Commission and SROs to analyze" market events like the 2010 "Flash Crash." Peirce Statement. Before the CAT, the Commission had faced challenges reconstructing market events because there was "no single, comprehensive audit trail available to regulators."

Consolidated Audit Trail at 20. Instead, the Commission had to comb through "a variety of data sources," including separate SRO audit trails, and combine this data into a database that would allow it to reconstruct past trading events. *Id*. at 20, 31-32.

The CAT has largely resolved these problems. The Commission has ordered the creation of a "single consolidated audit trail." *Id.* at 54. By placing order and trade data under one umbrella, the CAT provides the Commission with information that is more "accurate, complete, accessible, and timely." *Id.* at 81.

None of the Commission's arguments for collecting "Customer and Account Attributes" are persuasive. The Commission has claimed that "Customer and Account Attributes" are necessary to "allow regulators to identify bad actors who are using retail trading accounts to perform illegal activity." Exemptive Order at 20. But that is not true. The Commission's "enforcement division already is very successful at locating and bringing to justice wrongdoers in our markets," and the Commission "already has sufficient tools to get the information it needs to pursue credible leads about market misconduct and to do so quickly." Comm'r Hester M. Peirce, *This CAT is a Dangerous Dog*, RealClearPolicy (Oct. 9, 2019), bit.ly/3fTxTxE. The 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." *Id.*

The Commission also has suggested that collecting "Customer and Account Attributes" would allow the Commission to "more quickly initiate investigations, and more promptly take appropriate enforcement action." *Consolidated Audit Trail* at 191. But increased speed does not justify collecting personal customer data in bulk *before* having any reason to investigate an individual. *Id.* at 25.

The Commission finally has claimed that collecting "Customer and Account Attributes" will help it to "protect senior investors and identify other types of fraudulent activity that may target certain age demographics." Exemptive Order at 20; *see* NPRM at 105. But there is zero evidence that the Commission cannot combat fraud against senior citizens without collecting this data. Indeed, the Commission regularly brings such actions. *See, e.g.*, U.S. Secs. & Exch. Comm'n, *SEC Shuts Down Fraudulent Investment Adviser Targeting Senior Citizens* (May 22, 2020), bit.ly/3kJ5k9f; U.S. Secs. & Exch. Comm'n, *SEC Halts Penny Stock Scheme Targeting Seniors* (Nov. 27, 2019), bit.ly/3mF357c.

Even if collecting "Customer and Account Attributes" provides *some* surveillance benefits, however, their collection is still unwarranted. The Commission no doubt would like to sweep up as much information as it can on those it investigates. So too would most law enforcement operations. The Federal Bureau of Investigation, for example, would probably find it useful to have a database that contained real-time information on the credit card purchases of every American. Local police units would probably find it useful to have a database that contained the GPS locations and past travels of every car in the country. But this country does not tolerate such surveillance. *See, e.g.*, *Carpenter*, 138 S. Ct. at 2218 (invalidating data collection that "achieves

near perfect surveillance"). "Privacy comes at a cost." *Riley v. California*, 573 U.S. 373, 401 (2014). The mere fact that the Commission's surveillance may make "law enforcement . . . more efficient" does not justify the privacy intrusions. *Arizona v. Gant*, 556 U.S. 332, 349 (2009) (cleaned up)); *see Mincey v. Arizona*, 437 U.S. 385, 393 (1978) ("[T]he privacy of a person's home and property may not be totally sacrificed in the name of maximum simplicity in enforcement of the criminal law.").

* * *

Collecting "Customer and Account Attributes" will impose serious harms on ASA's members. ASA's members will be forced to disclose their customers' personal and financial information to the CAT; they will incur costs to comply with the Commission's requirements; they will lose business from individuals who do not wish to expose their personal and financial information to the CAT; and, when the CAT is inevitably hacked, they will be forced to incur significant costs to repair their relationships with their customers, including purchasing credit monitoring services for those customers whose personal information was exposed and defending themselves in litigation against allegations that they are responsible for customers' injuries.

As Commissioner Peirce recently explained, "it is doubtful whether the CAT's comprehensive surveillance database will significantly advance the Commission's mission." Peirce Statement. That mission is to "protect investors; maintain fair, orderly, and efficient markets; and facilitate capital formation." *Id.* Although the CAT "may make it a bit easier to investigate certain types of market misconduct," it is "unlikely that it will materially change the types or number of enforcement cases the Commission brings." *Id.* Simply put, the questionable benefits from collecting "Customer and Account Attributes" are not worth the extraordinary costs of collecting such information. The Commission should not collect any of these data elements.

II. The Commission's Proposal to Collect "Customer and Account Attributes" Violates the Fourth Amendment

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." The Commission's collection of "Customer and Account Attributes" would violate the Fourth Amendment by unreasonably compelling the production of confidential personal data.

A. The Collection of "Customer and Account Attributes" Is a Search or Seizure within the Fourth Amendment

A search or seizure within the Fourth Amendment occurs "when an expectation of privacy that society is prepared to consider reasonable is infringed." *United States v. Jacobsen*, 466 U.S. 109, 113 (1984). For an expectation of privacy to be reasonable, the individual must "seek[] to preserve something as private," and her expectation that it will remain private must be "one that society is prepared to recognize as reasonable." *Carpenter*, 138 S. Ct. at 2213 (citation omitted).

Courts repeatedly have recognized that the compelled production of data and records implicates the Fourth Amendment. *See, e.g.*, *id.* at 2217 ("[W]e hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through [cell-site location information]."); *City of L.A., Calif. v. Patel*, 576 U.S. 409, 412 (2015) (Los Angeles ordinance requiring hotel operators to make their guest registries available to the police on demand for inspection violates the Fourth Amendment); *Airbnb, Inc. v. City of N.Y.*, 373 F. Supp. 3d 467, 483 (S.D.N.Y. 2019) (New York City ordinance requiring AirBnB to produce its user records "is an event that implicates the Fourth Amendment.").

The "Customer and Account Attributes" that the Commission seeks to collect are data that companies and individuals "seek[] to preserve as private." *Carpenter*, 138 S. Ct. at 2217 (citation omitted). For example, ASA's members work diligently to keep their customers' "Customer and Account Attributes" private from any form of disclosure. Maintaining their customers' privacy is a top priority and an essential part of their commitment to their clients. To uphold this commitment, ASA's members publish privacy statements, put in place physical, electronic, and procedural privacy safeguards, employ state-of-the-art privacy technology, hire dedicated security staff, and advise their clients on taking proactive steps to protect their privacy. These vigorous efforts are necessary for ASA's members and other broker-dealers like them to preserve their relationship with their customers, who are justifiably concerned with sharing their personal and financial information.

Investors' expectation that "Customer and Account Attributes" should remain private is also an expectation that society should "recognize as reasonable." *Carpenter*, 138 S. Ct. at 2213 (citation omitted). As explained above, investors want this personal data kept private for many reasons: to avoid social stigma for their moral and philosophical judgments about economic transactions; to protect their business and trading profits from diminution or theft; to prevent cybercriminals from breaking into their accounts, stealing their money, data, and identity, or targeting them for extortion; and to avoid government snooping into, or misuse of, their valuable and sensitive data. *See supra* Part I.A. Keeping personal data private to prevent any one of these harms is eminently reasonable.

Other Commission regulations reinforce the idea that "Customer and Account Attributes" carry an expectation of privacy. For example, the Commission's regulations require broker-dealers to "adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information" that are "reasonably designed" to "(1) [i]nsure the security and confidentiality of customer records and information; (2) [p]rotect against any anticipated threats or hazards to the security or integrity of customer records and information; and (3) [p]rotect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer." 17 C.F.R. §248.30(a). This reasonable expectation of privacy is also reflected in a host of other laws, not specific to securities, that impose various requirements aimed at maintaining the confidentiality of similar data. *See, e.g.*, 15 U.S.C. §6803(c) (requiring financial institutions to disclose to their customers how they will "protect the confidentiality and security of nonpublic personal

information"); 42 U.S.C. §1320d-6 (prohibiting the "[w]rongful disclosure of individually identifiable health information").

B. The Commission's Collection of "Customer and Account Attributes" Is Not "Reasonable"

The Fourth Amendment's central command is that official searches and seizures must be "reasonable." *Riley*, 573 U.S. at 381-82. The Fourth Amendment imposes this standard "to safeguard the privacy and security of individuals against arbitrary invasions." *Delaware v. Prouse*, 440 U.S. 648, 654 (1979).

The collection of "Customer and Account Attributes" is not "reasonable" because it is not "sufficiently limited in scope, relevant in purpose, and specific in directive." *See v. City of Seattle*, 387 U.S. 541, 544 (1967). Under the Commission's proposal, the CAT will collect the personal data of every single American investor who purchases or sells a security in the United States, allowing the Commission to reconstruct and store the entire financial portfolio of every individual investor in the nation. And the Commission is doing this preemptively, regardless whether it has any particularized or even general suspicion that an investor has violated any securities laws, and regardless whether the Commission has any desire to make use of an investor's data for market analysis or reconstruction or other regulatory efforts. *See* NPRM at 99-106, 408-09. This is not even close to being properly tailored. *See City of Seattle*, 387 U.S. at 544.

For example, in *Airbnb v. City of New York*, a federal court found that a New York City ordinance requiring hotel booking companies to report the personal information of their hosts and the hosts' guests—for every booking made through their platforms—violated the Fourth Amendment. 373 F. Supp. 3d at 481-95. The Court had "little difficulty" finding that the ordinance was a search or seizure within the Fourth Amendment because Airbnb had a "privacy interest in the data" of its users. *Id.* at 482-86. The ordinance was not reasonable because "the scale of the production that the Ordinance compels . . . is breathtaking," making it "the antithesis of a targeted administrative subpoena for business records" and "devoid of any tailoring." *Id.* at 490-91. That the ordinance would "facilitate [the City's] enforcement efforts" was of no moment. *Id.* at 491-95 "[T]he test of reasonableness is not whether an investigative practice maximizes law enforcement efficacy." *Id.* at 492.

Carpenter also is instructive. There, the federal government obtained a conviction by using cell-cite data to track and produce maps of the defendant's movements, which allowed the government to prove that the defendant's phone was "near four of the charged robberies." *Carpenter*, 138 S. Ct. at 2212-13. The Court held that "the ability to chronicle a person's past movements through the record of his cell phone signals" implicates the Fourth Amendment, such that "when the Government accessed [cell-site data] from the wireless carriers, it invaded [the defendant's] reasonable expectation of privacy in the whole of his physical movements." *Id.* at 2216-19. It also rejected the argument that cell-site data were business records that deserved no Fourth Amendment protection. *See id.* at 2220.

The collection of "Customer and Account Attributes" also violates the Fourth Amendment because it fails to allow "precompliance review before a neutral decisionmaker." *Patel*, 576 U.S. at 420. "[A]bsent consent, exigent circumstances, or the like, in order for an administrative search to be constitutional, the subject of the search must be afforded an opportunity to obtain precompliance review." *Id.* For example, in *Patel*, the City of Los Angeles required "hotel operators to record information about their guests," such as their name, address, license plate number, room information, and method of payment, and to make this information "available to any officer of the Los Angeles Police Department for inspection." *Id*. at 412-13 (citation omitted). If a hotel owner "refuse[d] to give an officer access to his or her registry," that owner could be "arrested on the spot," meaning that the owner would have no opportunity for judicial review. *Id.* at 421. The Supreme Court held that this requirement was unconstitutional, since "business owners cannot reasonably be put to this kind of choice." *Id.*

So too here. The Proposed Rule requires broker-dealers to produce *all* "Customer and Account Attributes" without any opportunity for precompliance review. Brokers cannot opt-out of the CAT, and neither can individual investors, unless they stop trading in U.S. markets. The Commission's proposal to collect "Customer and Account Attributes" violates the Fourth Amendment and should not be adopted.

III. The Commission Has No Statutory Authority to Collect "Customer and Account Attributes"

The Commission's proposal to collect "Customer and Account Attributes" also exceeds the Commission's statutory authority under the Exchange Act. The Commission claims the statutory authority to collect "Customer and Account Attributes" under "Sections 2, 3(b), 5, 6, 11A(a)(3)(B), 15, 15A, 17(a) and (b), 19 and 23(a) [of the Exchange Act], 15 U.S.C. 78b, 78c(b), 78e, 78f, 78k-1, 78o, 78o-3, 78q(a) and (b), 78s, 78w(a)." NPRM at 402. But *none* of these sections authorize the Commission to collect "Customer and Account Attributes." *See N.Y. Stock Exch. LLC v. SEC*, 962 F.3d 541, 546 (D.C. Cir. 2020) (agencies cannot "act[] without delegated authority").

Nor can these provisions be read expansively to encompass the Commission's actions. Courts "expect Congress to speak clearly if it wishes to assign to an agency decisions of vast economic and political significance." *Util. Air Regulatory Grp. v. EPA*, 573 U.S. 302, 324 (2014) (citation omitted). In short, there is a "clear statement" rule for major questions—Congress must clearly and expressly declare that the agency has rulemaking authority to address those questions, or the agency does not have that authority. *P.J.E.S. v. Wolf*, No. 20-cv-2245-EGS, 2020 WL 6770508, at *30 (D.D.C. Nov. 18, 2020); *see Whitman v. Am. Trucking Ass'ns*, 531 U.S. 457, 468 (2001) ("[Congress] does not . . . hide elephants in mouseholes."). Here, Congress never would have silently given the Commission the authority to collect "Customer and Account Attributes." Because there is no clear statement in the Exchange Act empowering the Commission to collect "Customer and Account Attributes," the Commission does not have that authority.

Indeed, "[a]gencies are . . . not afforded unfettered authority to cast about for potential wrongdoing." *Accrediting Council for Indep. Colleges & Sch.*, 854 F.3d at 689. Yet that is exactly what the Commission proposes to do. The Commission lacks the statutory authority to collect "Customer and Account Attributes" through the CAT.

IV. The Non-Delegation Doctrine Prevents the Commission from Collecting "Customer and Account Attributes"

Even if the Exchange Act's provisions could be read to grant the Commission the power to collect "Customer and Account Attributes," those provisions would violate the non-delegation doctrine.

Article I, Section 1 of the U.S. Constitution provides that "[a]ll legislative Powers herein granted shall be vested in a Congress of the United States." "Accompanying that assignment of power to Congress is a bar on its further delegation." *Gundy v. United States*, 139 S. Ct. 2116, 2123 (2019). Under the non-delegation doctrine, "Congress … may not transfer to another branch 'powers which are strictly and exclusively legislative.'" *Id.* (quoting *Wayman v. Southard*, 23 U.S. (10 Wheat.) 1, 42-43 (1825)). The constitutional question is "whether Congress has supplied an intelligible principle to guide the delegee's use of discretion." *Id.*

Here, if any statutory provision in the Exchange Act actually gave the agency the authority to collect "Customer Account Attributes," it would be so broad as to lack any "intelligible principle" to guide the Commission's discretion. Additionally, the issue of collecting "Customer and Account Attributes" is an "important subject[]," not a subject of "less interest," and therefore it must be "entirely regulated by the legislature itself." *Wayman*, 23 U.S. (10 Wheat.) at 43. The non-delegation doctrine thus prohibits the Commission from collecting "Customer and Account attributes."

V. The Proposed Rule Is Unlawful Because the Structure of the SEC Violates the Separation of Powers

The proposed rule also would be unlawful because the structure of the SEC is unconstitutional.

Article II of the Constitution "provides that 'the executive Power shall be vested in a President of the United States of America.'" *Free Enter. Fund v. PCAOB*, 561 U.S. 477, 492 (2010) (cleaned up) (quoting U.S. Const. Art. II, §1, cl. 1). "[T]he executive power include[s] a power to oversee executive officers through removal." *Id.* "Since 1789, the Constitution has been understood to empower the President to keep these officers accountable—by removing them from office, if necessary." *Id.* at 483 (citing *Myers v. United States*, 272 U.S. 52 (1926)). The Framers "insist[ed]" upon this "unity in the federal executive" to ensure that the executive has "both vigor and accountability." *Printz v. United States*, 521 U.S. 898, 922-23 (1997). "In our constitutional system, the executive power belongs to the President, and that power generally includes the ability

to supervise and remove the agents who wield executive power in his stead." *Seila Law LLC v. CFPB*, 140 S. Ct. 2183, 2211 (2020).

The structure of the SEC violates these constitutional requirements. The Commission wields vast executive enforcement powers, including initiating investigations, issuing subpoenas, imposing civil monetary penalties, and commencing enforcement actions in federal court. *See, e.g.*, 15 U.S.C. §§78u, 78u-2. SEC Commissioners, however, can only be removed for cause. *See Free Enter. Fund v. PCAOB*, 561 U.S. 477, 487 (2010); *SEC v. Blinder, Robinson & Co.*, 855 F.2d 677, 681 (10th Cir. 1988). This limitation deprives the President of the constitutional power to "supervise and remove the agents who wield executive power." *Seila Law*, 140 S. Ct. at 2211. In addition, because Commissioners are appointed for five-year terms, the President is denied the "opportunity to shape [the Commission's] leadership and thereby influence its activities." *Id*. at 2204. Because the structure of the SEC violates the separation of powers, the Commission lacks the constitutional authority to adopt the proposed rule.

VI. The Commission's Proposal to Collect "Customer and Account Attributes" Violates the Constitutional Right to Privacy and the First Amendment

The Commission's proposal to require the disclosure of "Customer and Account Attributes" violates the Constitutional right to privacy and the First Amendment. The Constitutional right to privacy encompasses "the individual interest in avoiding disclosure of personal matters." *Whalen v. Roe*, 420 U.S. 589, 599 (1977). In particular, there is a "constitutionally protected interest in the confidentiality of personal financial information." *Statharos v. N.Y.C. Taxi & Limo Com'n*, 198 F.3d 317, 322-23 (2d Cir. 1999); *see California Bankers Ass'n v. Shultz*, 416 U.S. 21, 78-79 (1974) (Powell, J., concurring) ("Financial transactions can reveal much about a person's activities, associations, and beliefs. At some point, governmental intrusion upon these areas would implicate legitimate expectations of privacy.").

Similarly, "[t]he First Amendment prohibits the use of compulsion to exact from individuals (or groups) the *wholesale disclosure* of their associational ties where such inquiry is [n]ot germane to the determination of whether a crime has been committed." *Reporters Comm. for Freedom of Press v. Am. Tel. & Tel. Co.*, 593 F.2d 1030, 1054 n.82 (D.C. Cir. 1978) (emphasis added). And, as explained above, investors' securities transactions "offer a window into [investors'] deepest thoughts and core values" and frequently reflect their "moral, ethical, or religious beliefs." Peirce Statement.

Government actions that infringe on these rights require heightened scrutiny. *See Statharos*, 198 F.3d at 324; *John Doe No. 1 v. Reed*, 561 U.S. 186, 196 (2010). The Commission's proposal to require the disclosure of "Customer and Account Attributes" cannot survive this heightened scrutiny. The Commission's proposal preemptively requires the wholesale disclosure of *all* investor data without *any* indication that the investor has done anything wrong. This proposal is not tailored to further any important government interest. The Commission's proposed rule is constitutionally untenable.

VII. The Commission's Proposed Rule Violates the E-Government Act.

Finally, the Commission's proposal to require the collection of "Customer and Account Attributes" would violate the E-Government Act. The E-Government Act exists to "ensure sufficient protections for the privacy of personal information." 44 U.S.C. §3501, notes. To that end, it requires federal agencies to "conduct a privacy impact assessment" ("PIA") to "ensure the review of the privacy impact assessment," and "if practicable" make the PIA "publicly available" *before* doing one of two things: (1) "developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form," or (2) "initiating a new collection of information." *Id.* A "collection of information" is "the obtaining, causing to be obtained, soliciting, or requiring the disclosure to third parties or the public, of facts or opinions . . . regardless of form or format, calling for . . . answers to identical questions posed to . . . ten or more persons." *Id.* §3502(3); *see also* 5 C.F.R. §1320.3(c).

Despite these requirements, however, the Commission has neither conducted, reviewed, nor published a PIA on the development of the CAT or the collection of "Customer and Account Attributes." *See* U.S. Secs. & Exch. Comm'n, *Privacy Impact Assessments*, bit.ly/30hcpGG (last visited Nov. 28, 2020). OMB requires agencies to "conduct and draft a PIA . . . from the earliest stages of the agency activity and throughout the information life cycle." *See* OMB Circular No. A-130: Managing Information as a Strategic Resource (2016), bit.ly/2UlPWnY. Thus, "a PIA is not a time-restricted activity that is limited to a particular milestone or stage of the information system or PII life cycles," but is a "living document that agencies are required to update whenever changes . . . alter the privacy risks." *Id.* Notwithstanding these requirements, the Commission has failed to conduct any PIA. Accordingly, any collection of "Customer and Account Attributes" before the Commission conducts a PIA would violate the E-Government Act.

CONCLUSION

For the foregoing reasons, ASA urges the Commission to not collect any of the data elements identified as "Customer and Account Attributes."

Sincerely,

/s/ Christopher A. Iacovella

Christopher A. Iacovella
Chief Executive Officer
American Securities Association