Filed Electronically

June 22, 2026

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

Re: Concept Release on Consolidated Audit Trail and Other Audit Trails and Data Sources (File No. S7-2026-12)

The American Securities Association ("ASA")[1] writes in response to the Securities and Exchange Commission's ("Commission") April 16, 2026 Concept Release on the Consolidated Audit Trail ("CAT"). The Concept Release invites broad comment on the CAT's purpose, structure, governance, data scope, cybersecurity, and privacy.

I. OVERVIEW

ASA welcomes this review, though it should never have been necessary. The CAT's fundamental design defects were identifiable from the outset and the time to address them is now. ASA strongly urges the Commission to use this Concept Release to eliminate the collection of "Customer and Account Information System" ("CAIS") data and to permanently abandon the "Customer and Account Identifier" ("CCID"). These elements have never been necessary for the CAT to fulfill its core regulatory mission, and the harms they impose — to investor privacy, civil liberties, and data security — are severe. The Commission has an opportunity and responsibility to eliminate this very real threat to investor privacy.

The CCID is not a technical workaround that solves the personally identifiable information ("PII") problem. It *is* the PII problem. It is built using investors' most sensitive personal and

[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.

financial data, and it enables the surveillance of any individual's investment activity over the course of their lifetime. The government has no more right to attach a permanent financial tracking device to every American investor than it does to track their physical movements without cause. The constitutional and statutory defects that plague CAIS data collection apply with equal, if not greater, force to the CCID.

That obligation does not stop at halting future collection. The Commission must also direct that the personal data already amassed under CAIS be permanently destroyed. Retention of that data serves no regulatory purpose and perpetuates the same privacy and security harms that collection created.

II. BACKGROUND

A. Rule 613 and the Creation of the Consolidated Audit Trail.

In July 2012, the Commission adopted Rule 613, requiring national securities exchanges and associations ("SRO"s) to jointly submit a plan to create, implement, and maintain a consolidated audit trail, including a central repository to receive and store CAT data. Rule 613 required each SRO and its members to capture and report trade, quote, and order activity in all NMS securities to the central repository in real time, across all markets, from order inception through routing, cancellation, modification, and execution.

The CAT was designed to replace the existing patchwork of SRO audit trails with a single, unified audit trail. The Commission believed the CAT would improve market surveillance, facilitate reconstruction of broad-based market events, and enhance market analysis. None of those goals require collecting investors' personal data or generating a permanent cross-market tracking identifier, and none requires a permanent identifier capable of tracking every investor across every market for life.

B. The CAT NMS Plan and the Introduction of the CAIS and CCID.

In 2015, the SROs submitted the CAT NMS plan, and on November 15, 2016, the Commission approved it. The CAT NMS Plan required Industry Members to record and report "Customer Identifying Information" and "Customer Account Information." The CAIS was ultimately established as the mechanism for collecting and storing these data elements, including name, address, date of birth, individual taxpayer identification number, social security number, account number, account type, customer type, date account opened, and large trader identifier.

The CCID was developed as a derived identifier — a unique, persistent code generated from an investor's personal and financial information for the purpose of linking that investor's activity across every order, every account, and every broker throughout the market. Unlike a simple

account number, which can be changed, or a Social Security number, which can be at least partially protected, the CCID is a government-generated surveillance tag designed to follow an investor for the entirety of their market participation.

C. Prior Criticism of PII Collection and the Commission's 2020 Proposed Rulemaking.

Following adoption of the CAT NMS Plan, the CAT attracted widespread criticism over cybersecurity and privacy. Major breaches had already occurred: Chinese state-sponsored hackers compromised the Office of Personnel Management in 2015,[2] stealing the records of more than 22 million federal employees; the Commission's own EDGAR filing system was breached in 2016, [3] that same year a CIA employee stole 34 terabytes of the agency's most sensitive classified data; [4] and Equifax was compromised in 2017, exposing the personal data of tens of millions of Americans.[5]

If foreign adversaries could penetrate a federal personnel agency and a domestic credit bureau, and a trusted insider could compromise the CIA's most classified systems undetected, then the CAT promised something worse than any of them: a single registry concentrating the personal, financial, and trading data of every American investor into one high-value target.

Lawmakers saw the danger clearly. Congress held multiple hearings. A bipartisan coalition of senators wrote to the Commission in July 2019 urging it to "prohibit the collection of any retail investor PII by the CAT," citing the threat posed by China's cyber agenda, among other things.[6]

ASA raised these exact concerns with the Commission years ago, repeatedly and on the record, urging it to stop the collection and use of Americans PII. We explained that the use of PII "will do nothing to support the mission of the CAT and will only subject the PII of millions of Americans to theft from cybercriminals"; that there is "no compelling reason for the collection of any PII"; that "the costs associated with collecting PII vastly outweigh any benefit to investors or

---

[2] Majority Staff Report, House Committee on Oversight and Government Reform, *The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation* (Sept. 7, 2016), available at https://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf.

[3] https://www.sec.gov/news/public-statement/statement-clayton-2017-09-20

[4] CIA's WikiLeaks Task Force report, as released by Sen. Ron Wyden's office in June 2020, available through his Senate press release at wyden.senate.gov.

[5] https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement

[6] https://www.kennedy.senate.gov/public/2019/7/sen-john-kennedy-r-la-leads-letter-to-sec-chairman-concerning-data-privacy-and-the-consolidated-audit-trail

the SEC's ability to oversee markets"; and that "[t]he SEC does not need PII to conduct market surveillance and police bad actors."[7]

Every one of those arguments applies with equal force to the CCID, which is generated from that same PII and is specifically designed to maximize its surveillance utility.

In 2020, the Commission proposed replacing "PII" with "Customer and Account Attributes" stored in CAIS, and introduced the CCID as the mechanism by which remaining personal and financial data could be operationalized into a persistent cross-market investor identifier. ASA opposed that proposal then, and opposes it now, because relabeling sensitive data and laundering it through a government sponsored identifier does not reduce the threat; it institutionalizes it.

The threat has only grown. In late 2024, Chinese state-sponsored hackers breached the U.S. Treasury Department, accessing thousands of files including documents from the office responsible for administering financial sanctions. That same year, a Chinese hacking group compromised at least nine U.S. telecommunications companies, accessing the communications of senior government officials. Foreign adversaries target whatever financial and personal data the government collects. The CAT would give them the most valuable trove of all.[8]

D. <u>April 2026 Concept Release</u>.

The Concept Release covers nine major topic areas: the purpose of the CAT, its structure and governance, data scope and design, cybersecurity and data privacy, funding and cost management, the potential for alternative audit trail approaches, and the appropriate balance between civil liberties protections and regulatory need.

This broad review is precisely the kind of fundamental reassessment that ASA has long advocated. The Commission should use it to eliminate CAIS data collection and the CCID — not merely to tinker at the margins of a system that is structurally flawed.

The Commission's remaining questions on governance, structure, alternative audit trail approaches, and cost management are subordinate to this threshold determination. If the CAT's core data collection architecture is unlawful, reforms to its governance or funding model are irrelevant. ASA addresses those secondary questions only to the extent they bear on the legal and privacy defects described below.

---

[7] https://www.sec.gov/comments/s7-13-19/s71319-6381876-197754.pdf

[8] Christopher A. Iacovella, *AI Just Made Every American Investor a National Security Target*, Wash. Times, May 5, 2026, https://www.washingtontimes.com/news/2026/may/5/ai-made-every-american-investor-national-security-target/.

III. COMMENTS ON THE CAT

A. CAIS Data Collection and the CCID Threaten Americans' Privacy and Individual Freedom.

If the Commission does not take further action, the CAT will have at its fingertips a comprehensive record of private financial decisions made by millions of Americans — every equity and option trade and quote, from every account at every broker, by every investor. The CCID stitches that record together permanently, linking every trade, across every account, across every broker, for the entire duration of each investor's market participation.

The CCID makes this surveillance qualitatively worse than mere data collection. A database of personal attributes can, in theory, be restructured, anonymized, or purged. A persistent identifier cannot be unrung. Once generated, the CCID follows the investor everywhere in the market.

Moreover, the Commission has placed few constraints on who may access this data. Because the surveillance function requires eyes to watch and minds to interpret the data, access must extend to thousands of individuals: Commission staff, employees of the two dozen self-regulatory organization participants, the plan processor's personnel, and the contractors, consultants, and vendors who build and maintain the system. The CAT "is required to be able to support a minimum of 3,000 users at one time,"[9] and the actual number of users may be much higher. The insider threat is not theoretical. In 2023, a CFPB employee stole the personal and financial data of more than 256,000 consumers by forwarding it to a personal email account across 65 separate transfers, which went undetected until a colleague noticed the employee had copied a personal address into work correspondence.[10]

These users will have access to every trade, from every account, from every broker, for every retail investor in America. And they will be able to download data from the CAT for any regulatory purpose. The CCID ensures that any such download includes a permanent, linked record of every trade ever made by every investor in the database.

A person's investment decisions are a window into their conscience. An investor's portfolio can reveal politics, religion, and moral convictions: shares bought in a firearms manufacturer or sold from one, a divestment from companies that conflict with faith, a position taken to support or boycott a cause. It can reveal an individual's circumstances too, because people trade when they

[9] "Oversight of the Status of the Consolidated Audit Trail," Senate Banking Committee (Oct. 22, 2019), https://bit.ly/33nifqw.
[10] Letter from Rep. Bill Huizenga, Chairman, House Financial Services Committee Oversight and Investigations Subcommittee, to Rohit Chopra, Director, Consumer Financial Protection Bureau (Apr. 18, 2023), available at https://financialservices.house.gov/uploadedfiles/2023-04-18_huizenga_to_chopra_re_breach.pdf.

marry, divorce, fall ill, lose a job, or prepare to die. The government has no business compiling a permanent record of any of it.

The CAIS and CCID ensure those choices are recorded, linked, and permanently accessible to the government. Investors whose trades reflect moral, ethical, or religious beliefs may be chilled from making those decisions knowing that a permanent government record exists. The danger is not abstract: a leaked or misused record would hand activists, employers, and political opponents a roadmap for pressuring investors over portfolios that fail someone else's ideological test, whatever that test happens to be. The current system makes compelled disclosure complete and permanent.

B. The CCID Is a Cybersecurity Threat Multiplier.

Every trade from every account made by every retail investor in America, all of it concentrated in a single database. The CAT does not merely create that risk, it amplifies it. It is not merely a data point that can be stolen — it is a key that unlocks a complete, linked financial history. A breach of the CAT is not a breach of a moment in time; it is a breach of an investor's entire financial life.

The Commission may contend that retaining only derived identifiers rather than raw PII reduces risk. It does not. That reasoning does not survive scrutiny when applied to the CCID. Dropping a few data fields means nothing when the Commission simultaneously creates a persistent identifier that stitches everything remaining together across every account and every market. A hacker who obtains CCID-linked data obtains not isolated records but a complete, integrated, longitudinal profile of every investor in the system.

A breach could leak highly-confidential information about trading strategies or positions, expose proprietary information about significant business relationships, compromise regulatory efforts, and allow cybercriminals to gain access to individuals' brokerage accounts. Knowing an investor's name, address, birth year, and complete trading history, all linkable through the CCID, gives a cybercriminal everything needed to impersonate that investor, answer security questions, and defeat account authentication measures.

C. Market Oversight Does Not Require CAIS Data or the CCID.

The original impetus for 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.[11] The Commission's stated objectives of improved market surveillance, event reconstruction, and market analysis do not require CAIS data or the CCID. The CAT *can* accomplish all three

[11] Exchange Act Release No. 67457, July 18, 2012.

without them. As the Commission is aware, order-level data tied to broker/account identifiers is sufficient for event reconstruction and market surveillance without using an identifier to link back to American investors.

The Commission has offered no persuasive justification for either. The Concept Release is an opportunity to acknowledge that these elements were never necessary and to remove them. Because this data was never required for the CAT to protect markets, the Commission should not merely cease collection, it should destroy all the personal data already amassed.

The Commission can request customer information when it suspects a regulatory violation may have occurred by requesting it from broker-dealers who are required to respond to such requests within 24 hours. Broker-dealers already maintain the account-level records necessary to respond to a targeted regulatory inquiry, which makes order-level data tied to anonymized, firm-assigned account identifiers sufficient for trade reconstruction, market surveillance, and cross-market analysis.

The Commission does not need a government-generated persistent identifier to connect those records when a specific investigation demands it. A lawful CAT retains order and execution data linked to firm-side identifiers, requires no collection of an individual investor's name, address, date of birth, Social Security number, or any other personal attribute, and creates no mechanism for generating a cross-market tracking identifier. That architecture satisfies Rule 613's original objectives without exposing every American investor to the privacy and security harms this letter describes.

IV. CAT IS LEGALLY AND CONSTITUTIONALLY DEFICIENT

Beyond the policy case for eliminating CAIS and the CCID, the Commission's approach is independently unlawful on multiple constitutional and statutory grounds as set forth below.

A. Collecting CAIS Data and Deploying the CCID Violates the Fourth Amendment.

The Fourth Amendment protects the people from unreasonable searches and seizures. The Commission proposes to sweep in voluminous personal data about investment activities without any suspicion of wrongdoing, and then to compile that data into a permanent, cross-market tracking identifier. Broker-dealers are afforded no opportunity for pre-compliance review: they must surrender this data or face severe penalties.

The Supreme Court has recognized that the aggregation of location data over time constitutes a Fourth Amendment search because it reveals a comprehensive record of a person's past movements.[12] The same logic applies here with even greater force.

The CCID does not merely aggregate location data. It aggregates every investment decision an investor has ever made, across every account and every broker, linked by a government-assigned permanent identifier. If the Fourth Amendment prohibits warrantless access to months of location data, it surely prohibits the government's warrantless compilation of a lifetime of financial activity into a single linked record.

B. The Commission Has No Statutory Authority to Collect CAIS Data or Create the CCID.

Congress never passed legislation ordering the Commission to create the CAT, collect CAIS data, create a CCID, or maintain a system of persistent investor identifiers. Yet the Commission pressed forward anyway, invoking a grab bag of statutory provisions, none of which supplies the authority it claims.

Creating a permanent, government-assigned tracking identifier for every market participant is not reasonably necessary for any purpose that Congress has authorized. It is the kind of consequential policy choice that "one would expect Congress to speak clearly to if it wished to assign" to an agency.[13] Congress has not done so.

C. The Non-Delegation Doctrine Prevents the Commission from Collecting CAIS Data or Deploying the CCID.

Under the non-delegation doctrine, Congress must provide agencies with an "intelligible principle"[14] to guide their actions. Any statutory provision broad enough to authorize the Commission to generate a permanent, cross-market financial tracking identifier for every American investor would be so vague and standardless as to fail this requirement.

CAIS and CCID are not minor administrative tools. They are a comprehensive surveillance architecture. Delegating to the Commission the unilateral authority to impose lifetime financial tracking identifiers on every American market participant raises a non-delegation problem that the Commission has not addressed and cannot overcome.

---

[12] Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018).
[13] *West Virginia v. EPA*, 597 U.S. 697, 721 (2022)
[14] *Whitman v. American Trucking Assns.*, 531 U.S. 457 (2001).

D. Collecting CAIS Data and Deploying the CCID Violates 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 approach would violate these rights by forcing the disclosure of every investor's financial transactions without any evidence of wrongdoing and then compounding the violation by generating a permanent government tracking identifier from that data.

The threat is not limited to breach or misuse by bad actors. Even routine government use of the CAT poses a constitutional danger. Because the CAT captures every buy and every sell, a mild application of artificial intelligence to its information can derive, with precision, what any investor currently holds — what was bought and never sold is owned. That inference transforms the CAT from a market surveillance tool into something Congress never authorized and the Commission has never acknowledged: a real-time government inventory of every American investor's portfolio. A system built to detect insider trading and market manipulation becomes, with minimal additional effort, an instrument for identifying taxable assets, targeting disfavored industries, or suppressing lawful investment activity the government disapproves of.[15] The line between market oversight and financial surveillance is not merely blurry, with AI, it disappears entirely.

The First Amendment separately protects the freedom to make investment decisions reflecting personal, moral, and political beliefs without government monitoring.[16] The CCID ensures that monitoring is not episodic but permanent. Compelled disclosure of investor transactions stitched together by a permanent government identifier and accessible to thousands of users creates a concrete chilling effect. Investors who know that every trade in firearms manufacturers, cannabis companies, or ESG funds is permanently recorded and government-accessible may avoid those securities entirely, suppressing financially-expressive conduct that the First Amendment protects. The CCID does not merely record expression after the fact. It deters it in advance. The Commission's approach is constitutionally untenable.

E. Collecting CAIS Data and Creating the CCID Violates the E-Government Act.

[15] Letter from Christopher A. Iacovella, President and CEO, American Securities Association, to Secretary Scott Bessent, Chairman, Financial Stability Oversight Council (Apr. 16, 2026), available at https://www.americansecurities.org/post/asa-urges-secretary-bessent-to-end-cat-s-use-of-american-investor-personal-information-in-wake-of-an.

[16] See NAACP v. Alabama, 357 U.S. 449, 460-63 (1958).

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.[17] Despite these requirements, the Commission has failed to conduct or publish a privacy impact assessment for CAIS data collection or for the CCID.

The CCID, as a novel government-generated persistent identifier built from personal and financial data, is precisely the kind of new information technology for which the E-Government Act's assessment requirement exists. The Commission's failure to comply with this requirement independently renders any rule, guidance or order implementing the CCID unlawful.

F. The SEC Should First Determine the Legality of the CAT and Conduct a Full Financial Audit Before Approving Proposed Funding Model.

In addition to ASA's fundamental concerns over the collection of PII, ASA continues to be alarmed over the CAT's funding model and its exploding costs. This is especially alarming for a system whose legal foundations are as infirm as those outlined above.

Because the CAT's legal foundation is infirm, the SEC must first:

1. Determine whether the CAT is legal;
2. Perform a full financial audit of CAT costs; and
3. Move the CAT system onto the SEC budget going forward.

We refer the SEC to ASA's February 2026 letter outlining our views on the CAT's funding model.[18]

V. CONCLUSION

The Concept Release is the Commission's best opportunity in years to correct the CAT's fundamental design flaws, and ASA urges the Commission to seize it. ASA has warned of these dangers for years, and every warning has only grown more urgent. CAIS collects the personal and financial information of every American investor without consent and without suspicion of wrongdoing.

The CCID converts that collection into something worse: a permanent, government-assigned identifier that tracks every investor across every trade, every account, and every broker for life.

[17] E-Government Act of 2002, Pub. L. 107-347, § 208.
[18] https://www.americansecurities.org/post/asa-urges-the-sec-to-reject-or-defer-action-on-2025-cat-funding-proposal

No statute authorizes this architecture, no regulatory mission requires it, and no security program can make so attractive a target safe. The Commission should eliminate CAIS and the CCID, and it should do so now.

For the foregoing reasons, ASA respectfully urges the Commission to cease all collection of PII by the CAT and to destroy the personal data already amassed. It's unnecessary, it's harmful, and it's illegal.

Respectfully submitted,

Christopher A. Iacovella

Christopher A. Iacovella
President and CEO
American Securities Association