April 16, 2026

The Honorable Scott Bessent
Secretary of the Treasury and Chairman of the Financial Oversight Council
United States Department of the Treasury
1500 Pennsylvania Avenue, N.W.
Washington, DC 20220

Re: Immediate Action Required — Anthropic's Claude Mythos and the Catastrophic Cybersecurity Risk Posed by the Consolidated Audit Trail's Collection of American Investor Personal and Financial Information

Dear Secretary Bessent:

The American Securities Association (ASA)[1] writes to you in your capacity as Chairman of the Financial Stability Oversight Council (FSOC) regarding the emergency meeting convened last week at the U.S. Department of the Treasury. We were pleased that you and Federal Reserve Chair Powell rightly summoned the chief executives of the nation's largest banks to warn them of the existential cybersecurity threat exposed by Anthropic's Claude Mythos Preview.[2]

The subject matter of this meeting confirms what ASA has warned about for years: the U.S. Securities and Exchange Commission's (SEC) Consolidated Audit Trail (CAT) is a significant cybersecurity vulnerability waiting to be exploited.[3] This is no longer a hypothetical. The threat is here, it is identified, and it has a name.

ASA has long and vehemently opposed the CAT's unconstitutional collection of American investor's personally identifiable information (PII).[4] We labeled the CAT as a one-stop shop for

[1] 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. 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. ASA has a geographically diverse membership base that spans the Heartland, Southwest, Southeast, Atlantic, and Pacific Northwest regions of the United States.

[2] Bloomberg, "Bessent, Powell Summon Bank CEOs to Urgent Meeting Over Anthropic's New AI Model," Apr. 10, 2026, available at https://www.bloomberg.com/news/articles/2026-04-10/anthropic-model-scare-sparks-urgent-bessent-powell-warning-to-bank-ceos.

[3] Christopher A. Iacovella, *The National Security Risk No One Is Talking About*, The Hill, July 3, 2019, *available at* https://thehill.com/opinion/cybersecurity/451403-the-national-security-risk-no-one-is-talking-about.

[4] Pensions & Investments, "SEC Sued Over Consolidated Audit Trail," Oct. 18, 2023 (quoting Christopher Iacovella: "ASA also remains vehemently opposed to the CAT's unconstitutional collection of investor's personal and financial information, and we urge every American to question this unprecedented intrusion into their private lives.").

cybercriminals.[5] We have warned that concentrating the names, brokerage account information, and complete trading histories of every retail investor in America into a single government-mandated database was an unconscionable risk.[6] We were told, repeatedly, that our concerns were overstated, but recent events have proven otherwise. Anthropic's Mythos Preview has confirmed the precise risks to American investors ASA identified and the Commission declined to address.

The CAT database's collection and use of investors' personal and financial information poses a systemic risk to the financial system and the hard-earned money of every American investor.

I. What Mythos Is and Why It Changes Everything.

Anthropic's Claude Mythos Preview is, by Anthropic's own admission, the most dangerous AI model ever developed for offensive cybersecurity purposes. In internal testing, the model autonomously identified and developed working exploits for vulnerabilities in every major operating system and every major web browser[7] — including a 27-year-old flaw in OpenBSD, an operating system relied upon to run critical financial infrastructure including firewalls,[8] and a 16-year-old vulnerability in FFmpeg that had survived *millions* of automated security tests.[9] Anthropic reports that Mythos achieved a 72.4 percent success rate in generating working exploits — up from near zero in prior generations of AI models.[10]

In one documented instance, Mythos generated a browser exploit by autonomously chaining four distinct vulnerabilities together, bypassing the protection layers of both the browser and the underlying operating system, without human guidance.[11] What once required a nation-state's

[5]Christopher A. Iacovella, *The SEC's Stock Surveillance Plan Is a One-Stop Shop for Cybercriminals*, Wall St. J., May 17, 2020, *available at* https://www.wsj.com/articles/the-secs-stock-surveillance-plan-is-a-one-stop-shop-for-cybercriminals-11589757740.
[6] Letter from Christopher A. Iacovella, President & CEO, American Securities Association, to Vanessa Countryman, Secretary, U.S. Securities and Exchange Commission, Re: Proposed Amendments to the National Market System Plan Governing the Consolidated Audit Trail to Enhance Data Security, File No. S7-10-20 (Dec. 17, 2020), *available at* https://www.sec.gov/comments/s7-10-20/s71020-8157718-226862.pdf.
[7]Anthropic, "Project Glasswing: Securing Critical Software for the AI Era," Apr. 7, 2026, available at https://www.anthropic.com/glasswing.
[8]Anthropic, Project Glasswing, supra note 5 ("Mythos Preview found a 27-year-old vulnerability in OpenBSD — which has a reputation as one of the most security-hardened operating systems in the world and is used to run firewalls and other critical infrastructure.").
[9]Id. ("Claude Mythos Preview demonstrates a leap in these cyber skills — the vulnerabilities it has spotted have in some cases survived decades of human review and millions of automated security tests.").
[10]Fintech Singapore, "Anthropic's Mythos Forces Cybersecurity's Biological Turn," Apr. 13, 2026 (noting Mythos Preview achieved a 72.4 percent success rate in generating working exploits, "a dramatic leap from near-zero performance in earlier models").
[11]ProtoThema, "Anthropic's Mythos is Changing Everything We Knew About AI," Apr. 10, 2026 (describing Mythos generating "a browser exploit that combined four different vulnerabilities, bypassing protection layers of both the browser and the operating system").

intelligence apparatus or the world's most elite hackers can now be replicated, at scale, by any actor with access to a model of comparable capability — and Anthropic's own lead offensive cyber researcher has warned that comparable capabilities will be broadly available within six to twelve months.[12]

This is the threat environment that now confronts the CAT database and the American investors whose information it holds. The CAT's existing security framework was not designed to withstand this level of sophistication.

II. The CAT Is the Most Dangerous Undefended Target in American Finance.

When the CAT's Customer and Account Information System (CAIS) went live, it became the world's largest database of retail and institutional trading data ever assembled. It contains the name, address, year of birth, account type, account number, and complete transaction history of every retail brokerage customer in America, as well as identifying information for every pension fund, every mutual fund, and every institutional account operating in U.S. equity and options markets.[13] This data is owned and operated by 25 self-regulatory organizations (SROs) — including several owned by for-profit, publicly-traded holding companies — and is accessible to thousands of employees and contractors across those organizations.[14]

While the CAIS may be reformed, the government is contemplating the use of another, more invasive tool to take its place: the CAT customer identifier or CCID.[15] The CCID would be an investor specific identifier that will link investors' intimate personal information to their brokerage accounts and be used to track every American around the financial markets (think of it as an ankle bracelet for investors that monitors their every move just in case they commit a crime). The CCID is PII. So, whether the CAT ultimately uses the CCID or the full data set in CAIS, the type of Mythos breach that you have rightly expressed concern about remains the same.

---

[12]NBC News, "The 'Vulnpocalypse': Why Experts Fear AI Could Tip the Scales Toward Hackers," Apr. 11, 2026 (quoting Logan Graham, Anthropic's head of offensive cyber research: "We should be planning for a world where, within six months to 12 months, capabilities like this could be broadly distributed or made broadly available."), available at https://www.nbcnews.com/tech/security/anthropic-claude-mythos-ai-hackers-cybersecurity-vulnerabilities-rcna273673.

[13]SIFMA, "The Consolidated Audit Trail and Customer PII: Why Take the Risk," Mar. 2, 2021, available at https://www.sifma.org/news/blog/the-consolidated-audit-trail-and-customer-pii-why-take-the-risk.

[14]SIFMA, "The Consolidated Audit Trail: Protect Investor Data, Place Liability Where it Belongs," July 5, 2022, available at https://www.sifma.org/news/blog/the-consolidated-audit-trail-protect-investor-data-place-liability-where-it-belongs.

[15] *Joint Industry Plan; Order Approving an Amendment to the National Market System Plan Governing the Consolidated Audit Trail, as Modified by Amendment Nos. 1 and 2 and by the Commission, Regarding the Customer and Account Information System*, Exchange Act Release No. 34-104586, File No. 4-698, 91 Fed. Reg. 2164 (Jan. 16, 2026) (adopted Jan. 13, 2026), *available at* https://www.catnmsplan.com/sites/default/files/2026-01/SEC_Order-Approving-Proposed-CAIS-Amendment-01.13.26.pdf.

A Mythos-like AI model attacking the CAIS or the CCID used by the CAT does not simply mean a bad actor can steal some data. It means:

1. Mass identity theft at a scale America has never experienced: The PII of every retail investor in the country will be exposed in a single breach;
2. Complete portfolio holdings and trading strategy exposure: This would give adversaries a precise map of every American investor's positions, enabling targeted market manipulation, front-running, predatory trading, and potential liquidation;[16]
3. Nation-state exploitation of financial market intelligence: A foreign adversary, from China[17] or Russia, that gains access to the complete institutional positioning of U.S. equity and options markets would possess an extraordinary weapon for destabilizing the American economy at a moment of its choosing;[18]
4. Exploitation of legacy software vulnerabilities embedded in the CAT's own infrastructure: Mythos excels precisely at finding decades-old, dormant flaws of the kind that permeate the middleware, data feeds, browsers, and operating systems that underpin CAT's vulnerable architecture;[19]
5. Amplified insider threat risk: Twenty-five (25) percent of all cyber incidents involve malicious insiders; with Mythos-class AI, a single compromised employee or contractor with CAT access could enable a breach of incomprehensible scale;[20] and
6. Systemic financial market disruption: Access to CAT data and CCID would allow an adversary to understand and exploit the precise structure of U.S. markets in ways that could lead to mass liquidations and trigger cascading failures across the financial system.[21]

III. The CAT's Security Architecture Is Wholly Inadequate for This Threat.

The CAT was not designed to withstand the threat environment that Anthropic's Mythos has now made real. The Commission itself has never benchmarked the CAT's cybersecurity posture against

[16]Id.
[17] Josh Rogin, Congress Warns the SEC: Don't Expose Americans to Chinese Hacking, Wash. Post (July 26, 2019), https://www.washingtonpost.com/opinions/2019/07/26/congress-warns-sec-dont-expose-americans-chinese-hacking/.
[18]NBC News, Vulnpocalypse, supra note 10 ("[AI] could help hackers crash financial systems or lock up hospitals and manufacturing plants. It could help countries like Iran shut down American critical infrastructure.").
[19]Fortune, "Anthropic's Mythos is a Wake-Up Call, But Experts Say the Era of AI-Driven Hacking is Already Here," Apr. 10, 2026, available at https://fortune.com/2026/04/10/anthropic-mythos-ai-driven-cybersecurity-risks-already-here/.
[20]SIFMA, CAT and Customer PII, supra note 11 (noting "25 percent of all cyber incidents today are caused by malicious insiders or by other employees or contractors").
[21]CNBC, "Powell, Bessent Discussed Anthropic's Mythos AI Cyber Threat with Major U.S. Banks," Apr. 10, 2026, available at https://www.cnbc.com/2026/04/10/powell-bessent-us-bank-ceos-anthropic-mythos-ai-cyber.html.

the same standards it imposes on public companies, broker-dealers, investment advisers, or Regulation Systems Compliance and Integrity (SCI) entities.[22] The SROs that control this data have simultaneously assured regulators that it is secure while repeatedly seeking to limit their own liability in the event of a breach[23] — a contradiction so stark it demands an immediate and comprehensive response.

The single-database architecture of the CAT — the very feature that makes it operationally convenient for the SEC— is precisely what makes it so dangerous in the Mythos era. A model that can autonomously chain multiple zero-day exploits together to breach even the most hardened systems does not need to attack dozens of brokerage databases dispersed throughout the country,[24] it only needs to find one single entry point into one system. The CAT is that system.

IV. ASA's Call for Action

ASA has warned of this risk for years and we have opposed the collection of retail investor PII in the CAT since its creation by the Obama SEC.[25] We have proposed workable alternatives that would preserve the SEC's legitimate regulatory oversight capabilities, including a request/response-based model in which investor PII remains within broker-dealer systems and is transmitted to regulators only upon specific, documented regulatory need.[26] The government rejected those proposals. That rejection must now be revisited with the full recognition that the threat environment has fundamentally and irrevocably changed.

We respectfully call upon you as Chairman of the FSOC to take the following actions:

[22]SEC Commissioner Mark T. Uyeda, Statement on Consolidated Audit Trail Revised Funding Model, Sept. 6, 2023, available at https://www.sec.gov/newsroom/speeches-statements/uyeda-statement-cat-funding-090623 ("[T]he Commission benchmarks its own cybersecurity efforts on CAT to none of those standards or the proposed cybersecurity requirements for brokers, dealers, investment advisers, and Regulation SCI entities.").

[23]SIFMA, Protect Investor Data, supra note 12 ("The SROs have offered repeated assurances that CAT Data will be fully secured, though SIFMA believes the SROs undercut those assurances by repeatedly seeking to limit their own liability for breach or misuse of the data.").

[24] Anthropic Frontier Red Team, *Claude Mythos Preview: Cybersecurity Capabilities Assessment*, Apr. 7, 2026 ("In one case, Mythos Preview wrote a web browser exploit that chained together four vulnerabilities, writing a complex JIT heap spray that escaped both renderer and OS sandboxes. . . . [T]he model autonomously found and chained together several vulnerabilities in the Linux kernel . . . to allow an attacker to escalate from ordinary user access to complete control of the machine."), *available at* https://red.anthropic.com/2026/mythos-preview/.

[25] *Consolidated Audit Trail*, Exchange Act Release No. 34-67457, 77 Fed. Reg. 45722 (Aug. 1, 2012), *available at* https://www.sec.gov/files/rules/final/2012/34-67457.pdf.

[26]Pensions & Investments, "Republicans Float Bill to Bar Personal Data Collection on Audit Trail," July 21, 2023 (describing the Protecting Investors' Personally Identifiable Information Act, introduced by Sen. John Kennedy (R-LA) and Rep. Barry Loudermilk (R-GA)).

First, require the immediate suspension of all collection and retention of retail investor PII in the CAT's Customer and Account Information System and destroy all the data it has collected. The threat posed by Mythos-class AI to this concentrated dataset is not a future risk: it is a present and imminent danger and collection needs to stop now.

Second, immediately end the use of investor PII to create individual customer identifiers that the CAT uses to surveil American investors and Mythos can use to exploit those investors.

Third, order an emergency, independent cybersecurity audit of the CAT's full technology stack, including its legacy software layers, browser-based access points, SRO connections, and contractor access pathways, conducted against the same Mythos-class threat model that the Treasury and Federal Reserve used to brief the bank CEOs last week.[27]

Fourth, direct the SEC to formally adopt, without further delay, its long-pending August 2020 CAT data security proposal prohibiting bulk downloading of CAT data, requiring the use of Secure Analytical Workspaces for all data access, and eliminating any further collection and use of PII by the CAT.[28]

Fifth, work with Congress to enact the Protecting Investors' Personally Identifiable Information Act,[29] which would replace the current bulk-collection model with a request/response-based framework that preserves full regulatory authority while eliminating the single-point-of-failure risk that the CAT currently represents.

Sixth, require the SROs that own and operate the CAT to accept full, explicit, and unwaivable liability for any breach or misuse of CAT data and reject any further attempts by those SROs to disclaim warranties or otherwise shift that liability to anyone else including broker-dealers, pension funds, asset managers, and their customers.

[27]Fortune, "Bessent and Powell Convened Wall Street CEOs to Address Anthropic's Mythos Model," Apr. 10, 2026 (reporting attendees included Citigroup CEO Jane Fraser, Morgan Stanley CEO Ted Pick, Bank of America CEO Brian Moynihan, Wells Fargo CEO Charlie Scharf, and Goldman Sachs CEO David Solomon).
[28]SEC, "Update on the Consolidated Audit Trail: Data Security and Implementation Progress," Aug. 21, 2020, available at https://www.sec.gov/newsroom/speeches-statements/clayton-kimmel-redfearn-nms-cat-2020-08-21.
[29] H.R. 1483/S. 658 *Protecting Investors Personally Identifiable Information Act,* sponsored by Rep. Loudermilk and Senator Kennedy.

The SEC enforcement division's desire to have ready access to every investor's personal information without any evidence of wrongdoing cannot be worth the cost of exposing every American investor to the imminent threat posed by the sophistication of Mythos and AI models like it.

V. Conclusion.

A meeting of the leaders of this nation's largest banks was convened last week because you recognize that a new era of AI-driven cybersecurity risk demands an urgent and coordinated response. The Consolidated Audit Trail — as its currently designed — is the single greatest concentration of investor data in American history, it sits at the intersection of every risk that Mythos has now made operational, and it must be reformed.

ASA urges you to act before investors lose their life savings due to a targeted attack that we now know can be unleashed today.

Respectfully submitted,

Christopher A. Iacovella

Christopher A. Iacovella
President and Chief Executive Officer
American Securities Association

Cc:

U.S. Securities Exchange Commission Chairman, the Honorable Paul Atkins
U.S. House of Representatives Committee on Financial Service Chairman French Hill and Ranking Member Maxine Waters
U.S. Senate Committee on Banking, Housing, and Urban Affairs Chairman Tim Scott and Ranking Member Elizabeth Warren