



March 14, 2019

The Honorable Michael Crapo
Chairman
Committee on Banking, Housing, and
Urban Affairs
United States Senate
Washington, DC 20510

The Honorable Sherrod Brown
Ranking Member
Committee on Banking, Housing, and
Urban Affairs
United States Senate
Washington, DC 20510

RE: Data Privacy Submission Concerning Collection of Personally Identifiable Information (PII) by the Consolidated Audit Trail (CAT)

Dear Chairman Crapo and Ranking Member Brown:

The American Securities Association (ASA)¹, representing our nation's Main Street and regional financial services companies, welcomes the opportunity to provide feedback to the Senate Banking Committee regarding the collection, use, and protection of sensitive financial information by financial regulators and private companies. We appreciate the Committee's focus on the security of personal data, as this is an issue of growing importance and concern for millions of American households.

As the Committee undertakes its review of how personal data is collected and used by financial regulators, we strongly believe the potential collection of retail investor personally identifiable information (PII) under the Consolidated Audit Trail (CAT) requires your attention. As you are aware, the Securities and Exchange Commission (SEC) adopted a rule in 2012, following the May 2010 "flash crash", creating the CAT in order to capture customer and order event information across the equity markets.

The ASA fully supports the ability of the SEC to properly oversee markets and the creation of a market-wide surveillance system. However, absent further action by the SEC or the CAT plan processor FINRA, the CAT will collect and store the PII of millions of America's retail investors, creating a target-rich environment for bad actors. Neither the SEC, nor any other entity needs to collect the PII of every American saver to achieve the stated goal of the CAT.

As the members of the Senate Banking Committee are well aware, massive breaches of PII at government agencies in recent years have eroded the trust Americans have in the ability of

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 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.



government to safeguard their data. Once it is fully operational, the CAT will be one of the largest repositories of information created in history, and a prime target for hackers who will have ready access to the personal information of every individual that conducts a transaction in the U.S. equity markets. This should alarm all Americans.

The ASA welcomed the recent news that the stock exchanges had terminated the contract with Thesys Technologies – an unregulated third party – to be the CAT plan processor. The ASA also strongly supports the Financial Industry Regulatory Authority (FINRA) taking over as the plan processor for CAT. Since 1998, FINRA and its predecessor organization have operated the Order Audit Trail System (OATS), which allows FINRA to monitor and analyze the full cycle of orders for National Market System (NMS) and over the counter (OTC) stocks. Today, brokerage firms already submit much of the same information that would be collected under the CAT to FINRA, and FINRA has demonstrated over the years that it can effectively oversee the brokerage industry’s daily equity transactions without collecting retail investor PII.

While the transition to a new plan processor presents an opportunity for the SEC and other parties to reject the future collection of retail investor PII by the CAT, Congress, of course, also plays a critical role. The collection of retail investor PII in no way bolsters the ability of the SEC to oversee equity markets more effectively (the agency has had no issue bringing insider trading cases since FY2011 totaling 387), and only presents serious risks to American investors. We believe that this Committee – through its oversight role or through legislation– should prioritize the security of American investors’ PII and ensure the CAT does not become the world’s largest one-stop shop for cybercriminals.

We urge the Committee to stand with the overwhelming majority of Americans who oppose sending their PII to the CAT. A recent ASA survey found that while 75% of American investors trust their broker to keep their information secure, **nine in ten** are opposed to the government requiring their broker to send their information to an unregulated third-party.

The ASA survey results should come as no surprise considering so many Americans have been targeted in data breaches and have suffered the horrible consequences from identity theft. According to a 2018 Harris Poll survey, nearly 60 million Americans have been affected by identity theft. A report released earlier this year from Symantec found 143 million American consumers were victims of cybercrime in 2017 alone. This is especially concerning for America’s seniors and highlights the need to protect all Americans from the CAT’s glaring data security vulnerabilities.

The ASA recently submitted a letter–along with the aforementioned survey–to SEC Chairman Jay Clayton on this important issue, which is attached hereto as Exhibit A.

Conclusion

We believe the continued potential for PII collection under CAT represents one of the largest risks to the personal data security of American investors. We implore members of the Committee



to – if necessary – assert their constitutional prerogative to protect America’s retail investors and retirement savers. The ASA thanks the Committee for its leadership on data privacy and stands ready to work with you on this critical issue.

Sincerely,

Christopher A. Iacovella
Chief Executive Officer
American Securities Association



The Honorable Jay Clayton
Chairman
U.S. Securities and Exchange Commission
100 F Street NE
Washington, DC 20549

February 25, 2019

Re: Collection of Personally Identifiable Information (PII) by the Consolidated Audit Trail (CAT)

Dear Chairman Clayton:

The American Securities Association (ASA)¹, representing our nation's Main Street and regional financial services companies, appreciates your leadership and the work of the Securities and Exchange Commission (SEC) to protect hardworking retail investors, instill confidence in America's capital markets, and promote policies to accelerate economic growth. Nevertheless, we write today to express some concerns regarding the collection of personally identifiable information (PII) through the consolidated audit trail (CAT). While the ASA strongly supports the ability of the SEC to oversee markets and protect investors—including the creation of a market-wide surveillance system—we believe these goals can be accomplished without jeopardizing retail investors' sensitive data and privacy. We stand with the overwhelming majority of retail investors who do not want to send their PII to the CAT and we look forward to working with the SEC to implement well-tailored reforms outlined below.

While ASA welcomes recent reports revealing that the exchanges intend to fire Thesys Technologies as the plan processor and instead have the Financial Industry Regulatory Authority (FINRA) run the CAT, we remain concerned that the question of PII collection remains unresolved. The SEC should take steps to eliminate any PII collection requirements for whichever entity is ultimately selected as the CAT plan processor.

Personally Identifiable Information

In its current phase, the CAT appropriately collects all data and trading information from the exchanges. We believe the SEC can effectively surveil the market through the consolidation of order message and trading confirmation information alone. Neither the SEC, nor any other entity, needs to collect the PII of virtually every American saver and retail investor to achieve this goal.

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 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.



At a time of growing cyber threats targeting government and business, we would reiterate our data security and cyber safety capabilities concerns regardless of who is the plan processor for CAT. Our customers, in communities across the United States, have repeatedly made it clear that they do NOT want their sensitive information sent to a one-stop, target-rich environment for cyber criminals. This concern is real, and we strongly suggest the SEC amend the CAT plan to address it.

The ever-present threat of a cyberattack on large databases is an unfortunate reality that must be dealt with. In the past decade alone, cyberattacks at the Office of Personnel Management (OPM), Federal Deposit Insurance Corporation (FDIC), Department of Defense, and the SEC's own EDGAR database – to name just a few – have compromised sensitive information and undermined the faith Americans have in the ability of government to properly protect their personal information.² These attacks demonstrate that even large federal agencies with significant IT budgets are vulnerable to bad actors, let alone an unregulated third-party with zero experience in this sophisticated level of cybersecurity and which will be charged with storing an unprecedented amount of the PII of “Mr. and Mrs. 401k”.

The CAT and SEC Enforcement

Identifying and taking action against insider trading has been offered by the SEC as a reason for why the collection of PII through the CAT is necessary. This is a remarkable assertion given the agency's own enforcement statistics. Since FY2011, the SEC has taken a significant number of enforcement actions related to insider trading (387). SEC officials have also spoken on several occasions about how the use of “big data” and artificial intelligence are increasingly assisting the agency in its efforts to crack down on bad actors. The continued ability of the SEC to take enforcement actions related to trading activity – and the technological progress that is already bolstering those efforts – calls into question whether the marginal benefits of maintaining a vast, unsecure, and unregulated database of investor PII outweigh the costs of a likely cyberattack, which will threaten every aspect of the lives of millions of Americans.

A recent U.S. Intelligence Community “Worldwide Threat Assessment”³ report warned that “[o]ur adversaries and strategic competitors will increasingly use cyber capabilities—including cyber espionage, attack, and influence—to seek political, economic, and military advantage over the United States and its allies and partners.” The report goes on to explicitly state that certain adversaries will “increasingly use cyber operations to threaten both minds and machines in an expanding number of ways—to steal information, to influence our citizens, or to disrupt critical infrastructure.” If this is not a warning to the SEC about why it should not consolidate the PII of American investors, then we don't know what is.

² <https://www.investmentnews.com/gallery/20190219/FREE/219009999/PH/10-top-scams-targeting-seniors&Params=Itemnr=2>
“Identity thieves use stolen personal information to make unauthorized credit card purchases or steal money from bank accounts; they also use the information to apply for Social Security benefits or get health care covered by Medicare.”

³ <https://www.intelligence.senate.gov/sites/default/files/documents/os-dcoats-012919.pdf>



The recent enforcement actions taken by the SEC and Department of Justice against Ukrainian nationals that hacked into the EDGAR database also demonstrate the threat level posed by foreign actors. We agree with the Commission’s recent statement regarding this episode that “this action illustrates that the SEC faces many of the same cybersecurity threats that confront exchange-listed companies” and that “[t]hese threats to our marketplace are significant and ongoing and often involve threats from actors outside our borders. *No system can be entirely safe from a cyber intrusion.*”⁴ The CAT is certainly no exception to this and will never be immune to intrusions from cybercriminals, particularly those in foreign countries that seek to harm the integrity of the U.S. capital markets and steal the identity of the American people. It is simply irresponsible to put the information of American investors at risk when bad actors from inside and outside of the United States will do everything in their power to obtain it.

The Role of the Financial Industry Regulatory Authority (FINRA)

While we appreciate the reports that Thesys is no longer responsible for the CAT plan, we continue to believe FINRA is in a much better position and has the requisite experience and expertise to be the ultimate operator of the CAT. Since 1998, FINRA and its predecessor organization have operated the Order Audit Trail System (OATS), which allows FINRA to monitor and analyze the full cycle of orders for National Market System (NMS) and over the counter (OTC) stocks. Today, brokerage firms already submit much of the same information that would be collected under the CAT to FINRA.

Importantly, FINRA has also recognized in the past that the collection of PII associated with orders is both unnecessary and presents a serious risk to the security of sensitive information. The OATS system has operated for two decades without collecting the volume of PII envisioned under CAT, and FINRA’s decision in 2015 to abandon the Comprehensive Automated Risk Data System (CARDS) proposal further highlighted the belief that the costs of such PII collection outweigh any benefits. While many believe the CARDS proposal was fundamentally flawed from the very beginning (which ultimately led to the entire proposal being pulled), FINRA to its credit acknowledged early on the concerns surrounding the collection of PII that was being contemplated under CARDS. Even without a large database of PII under CARDS or any other initiative, FINRA continues to effectively oversee and regulate the brokerage industry’s daily equity market transactions.

If the SEC wants the CAT to become operational in the near-term, then FINRA should run it. FINRA has most of the Phase II information today, and with a few enhancements to the current OATS system, it could have a true market-wide surveillance system in place in fairly short order. The SEC and the ASA share a similar goal: to have a functioning CAT. This will promote investor trust and confidence in markets, and we support FINRA running it without PII.

We would also be supportive of FINRA and the SEC being the only entities who have access to any of the CAT data and information.

⁴ Statement on EDGAR Hacking Enforcement Action January 15, 2019.



Legal and Reputational Risk to Brokers

ASA also continues to be concerned about both the legal and reputational risk to our members. If a significant cyberattack takes place and the information of a brokerage firm's customers is compromised, it is not clear to anyone when brokers will learn of the breach and who will have legal liability for putting this information at risk. Brokerage firms are already required to comply with the SEC's Regulation S-P and to have policies and procedures in place to protect customer information, however the legal interplay between Regulation S-P and broker submission of data to the CAT remains unclear and should be addressed. As it stands today, the CAT's requirement that brokers send the PII of their customers to an unregulated third-party appears to violate Reg S-P on its face.

While our members should not be held liable in any way in the event of a CAT data breach, the reputational harm that a firm whose clients have had their information stolen could incur is a significant issue for us. We believe these concerns have not been considered or fully addressed throughout the development and implementation of the CAT.

American Investors Do Not Want Their PII Sent to an Unregulated Third-Party

A recent Morning Consult national survey (attached as exhibit A), and commissioned by the ASA, reveals just how strongly American investors oppose sending their personal information to the CAT. While three in four investors trust their broker to keep their personal and financial information secure, nearly **four in five** would not feel comfortable if their broker were forced to send this information to an unregulated third-party. The survey showed a whopping **nine in ten** investors are opposed to the government requiring their broker to send investment information to an unregulated third-party. Investors with money in the market participated in the nationwide survey. The SEC does not need PII to conduct market surveillance and police bad actors. We implore the Commission to immediately reverse this decision.

Conclusion

While we commend the SEC for its work to prioritize investor protection and for managing the complexities of CAT implementation, we believe the overarching goals of CAT can still be accomplished without collecting investor PII. We are eager to work with the Commission to modernize the next phase of the CAT in 2019 and to remove the PII reporting requirements for retail investors. This is a common sense and well-tailored change to maintain needed investor protections without risking the most sensitive information of every American saver.

We look forward to being a helpful partner to move this initiative forward.



Sincerely,

Christopher A. Iacovella
Chief Executive Officer
American Securities Association

Cc:
Commissioner Peirce
Commissioner Jackson
Commissioner Roisman