May 16, 2019

Bats BYX Exchange, Inc.
Bats BZX Exchange, Inc.
Bats EDGA Exchange, Inc.
Bats EDGX Exchange, Inc.
BOX Options Exchange LLC
C2 Options Exchange, Incorporated
Chicago Board Options Exchange, Incorporated
Chicago Stock Exchange, Inc.
Financial Industry Regulatory Authority, Inc.
Investors' Exchange LLC
Miami International Securities Exchange, LLC
MIAX Emerald, LLC
MIAX Pearl, LLC
NASDAQ BX, Inc.
Nasdaq GEMC, LLC
Nasdaq ISE, LLC
Nasdaq MRX, LLC
NASDAQ PHLX LLC
The NASDAQ Stock Market LLC
NYSE National, Inc.
New York Stock Exchange LLC
NYSE MKT LLC
NYSE Arca, Inc.

Re: Request for Amendment to CAT NMS Plan to Prohibit Collection of Retail Investor Personally Identifiable Information

Dear CAT NMS Plan Participants and Mr. Cook:

The American Securities Association (ASA)[1], representing our nation's Main Street and regional financial services companies, respectfully requests an amendment to the Plan ("Plan") Governing the Consolidated Audit Trail ("CAT") that would remove the collection of retail investor personally identifiable information (PII) by the CAT.

While the ASA fully supports the creation of the CAT to better surveil the markets, we believe there is no benefit to collecting retail investor PII, and absent an amendment to the Plan, the personal and sensitive information of millions of American savers will be vulnerable to cyberattack and misuse by criminals. The potential for identity theft, hacking, and data manipulation outweighs any benefits gained from the collection of retail investor PII. ASA's call to remove the collection of retail investor PII from the CAT is consistent with the American people's views on this matter, supported by two nationwide Morning Consult surveys showing an overwhelming majority of Americans oppose sending their PII to the CAT and are not willing to put their personal information at risk in order to expedite the Securities and Exchange Commission ("SEC" or "Commission") enforcement division's ability to prosecute insider trading cases.

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

Once it is fully functional, the CAT will be one of the largest databases in history, collecting and storing information related to the millions of trades that take place in the U.S. stock market every day. The amount of market-moving as well personal and financial information stored in the CAT will make it a prime target for cybercriminals, who have already demonstrated a willingness and ability to hack into ostensibly 'secure' government and private sector databases. With the realities of today's cyber threats, it will unfortunately not be a question of *if* the CAT is hacked into, but *when*.

The ASA fully supports the creation of a market-wide surveillance system, which will allow the SEC to properly oversee markets. However, without further action by the Plan participants, the CAT will collect and store the PII of millions of America's retail investors, creating a target rich environment for bad actors. An amendment to the Plan that removes the collection of PII will protect investors and their personal information without compromising the ability of regulators to properly surveil the U.S. equity markets and prosecute bad actors. We strongly encourage the Plan participants to submit such an amendment to the SEC as swiftly as possible.

Our specific views on this important issue are discussed in further detail below.

Retail Investor Personally Identifiable Information

The CAT became a major regulatory initiative nearly nine years ago in the wake of the May 2010 "flash crash" of the U.S. stock market. The Commission eventually adopted Rule 613 in July 2012 which required self-regulatory organizations ("SROs") to create and submit a national market system ("NMS") plan to the SEC that would capture order information for NMS stocks.

It is undeniable that in the years since the CAT was conceived and developed, Americans' views towards data security and the safety of their own personal information have shifted decidedly. Massive breaches of government and private databases, the ongoing problem of identity theft, and the increasing aggressiveness of foreign cybercriminals have rightly made Americans skeptical about the ability of the government (or any other entity) to keep their information safe.

Recent nationwide surveys of retail investors conducted by Morning Consult reveal how the American people overwhelmingly oppose sending their PII to the CAT. Nearly nine in ten retail investors opposed the government requiring their broker to send investment information to an unregulated third-party. Additionally, 72% of investors are not willing to put their personal information at risk in order to facilitate more insider trading cases, while 76% favor being allowed to 'opt-out' of having their PII collected under a system such as the CAT. The CAT Plan requirements must reflect the data privacy and security standards expected by the American people.

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 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.

In its current phase, the CAT appropriately collects all data and trading information from the exchanges. The SEC can effectively surveil the market through the consolidation of order message and trading confirmation information alone. Such data provides the SEC with a comprehensive view of order flow and trading activity without exposing sensitive investor information. Neither the SEC, nor any other entity, needs to collect the PII of virtually every American saver and retail investor to make the CAT a useful tool for regulators.

The CAT, SEC Enforcement, and Threats Posed by Foreign Actors

Identifying and taking action against insider trading and market manipulation have been offered by the SEC as reasons for why the collection of retail investor PII through the CAT is necessary. Yet when the SEC's own enforcement program and statistics are considered, this argument is not convincing. From FY2011 through FY2018, the SEC has taken a significant number of enforcement actions related to insider trading (387) and market manipulation (340). 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 and unsecure database of retail investor PII outweighs the costs of a likely cyberattack, which will threaten every aspect of the lives of millions of American investors. To us, this choice is not even close.

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*."[2] The CAT is certainly no exception to this and the SEC would do well to acknowledge that the CAT 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.

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." Foreign actors that hack into the CAT will gain access not just to sensitive personal and financial information, but to proprietary trading

[2] Statement on EDGAR Hacking Enforcement Action January 15, 2019.
[3] https://www.intelligence.senate.gov/sites/default/files/documents/os-dcoats-012919.pdf

information that will allow them to manipulate the U.S. markets, harming the very Main Street investors that CAT is intended to protect.

Legal and Reputational Risk to Brokers

ASA also continues to be concerned about both the legal and reputational risk to our broker-dealer members. If a significant cyberattack takes place and the information of a brokerage firm's customers is compromised, it is not clear under the Plan when brokers will be notified of the breach, what the public response will be, and who will have legal liability for putting customer information at risk.

As you are aware, Regulation S-P, among other things, requires covered financial institutions with retail customers to implement policies and procedures reasonably designed to protect customer information from unauthorized access, protect against any anticipated threats or hazards to the security or integrity of this information, and ensure the security and confidentiality of this information.[4] Brokerage firms are already required to comply with this regulation, however the legal interplay between Regulation S-P and broker submission of customer PII to the CAT seems to be in conflict. As it stands today, the CAT's requirement that brokers send the PII of their customers to the CAT appears to violate Reg S-P on its face as firms cannot assure customer PII sent to the CAT will be protected against any anticipated threats or hazards to the security or integrity of this information, and they cannot ensure the security and confidentiality of this information by the CAT.

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 serious concern. We believe these are just a few of the concerns that have not been considered or fully addressed throughout the development and implementation of the CAT.

Conclusion

Mass collection of retail investor PII under the CAT will put sensitive financial information at risk, leave millions of Americans vulnerable to identity theft and hacking, increase the likelihood for bad actors to engage in manipulative trading, and likely create legal liability for small and mid-size broker-dealers throughout the country. All of this would occur without any corresponding benefit, as access to retail investor PII is unnecessary for the SEC to properly surveil the nation's equity markets. We believe an amendment to the Plan that prohibits the collection of PII is warranted and necessary to protect American investors and instill confidence in our capital markets. We are not the only ones share this belief, as similar concerns about the collection of retail PII were raised in a recent Senate hearing and by senior leaders of the House Committee on Financial Services.[5] This is an investor protection issue plain and simple, and the

---

[4] S*ee* "Privacy of Consumer Financial Information (Regulation S-P)," 65 Fed. Reg. 40334 (June 22, 2000), Rel. Nos. 34-42974, IC-24543, IA- 1883, File No. S7-6-00 (adopting Regulation S-P), available at *https://www.sec.gov/rules/final/34-42974.htm*; 17 C.F.R. § 248.30.

[5] http://americansecurities.org/wp-content/uploads/Letter-to-the-SEC-on-CAT-PII-Collection.pdf

public perception of the SECs ability to uphold that prong of its mission will be severely tested if it does not act to remove the collection of retail investor PII from the CAT.

The ASA looks forward to partnering with the SEC to get the CAT up and running without the collection of retail investor PII, and we stand ready to assist you on this important issue in any way we can.

Sincerely,

Christopher A. Iacovella
Chief Executive Officer
American Securities Association

Cc:
Chair Jay Clayton
Commissioner Hester Peirce
Commissioner Robert Jackson
Commissioner Elad Roisman
Director Brett Redfearn