sifma® Invested in America

sifma asset management group

MFA Managed Funds Association

SENT VIA EMAIL

February 4, 2022

Mr. Michael Simon
Chair, Operating Committee
Consolidated Audit Trail, LLC

Re: Data Security for the Consolidated Audit Trail

Dear Mr. Simon:

As we approach the July 11, 2022, implementation date of the Consolidated Audit Trail's Customer and Account Information System, the membership of the Securities Industry and Financial Market Association ("SIFMA") SIFMA, SIFMA AMG, and MFA member firms remain extremely concerned with data protection within the CAT system. We share your interests in maintaining the strict confidentiality of data collected through CAT and welcome the opportunity to share with you our member firms' collective expertise with respect to data protection and evolving industry standards and practices regarding data security. To ensure the CAT data set allows for appropriate regulatory use but also is subject to best-in-class data protection standards for the proprietary trading strategies (i.e., Intellectual Property) of our membership, SIFMA, SIFMA AMG, and MFA (together, the Associations) urge you to provide much greater transparency into the specific data security standards deployed by FINRA CAT and the CAT NMS Plan in seven key areas set forth below. We welcome further information regarding these seven key areas that can be made available to all industry members. We also welcome an opportunity to discuss with you in greater detail the security protocols regarding the Intellectual Property of our member firms and their clients.

In summary, the aggregation of trade data in the CAT, complete with Firm Designated IDs (FDID) associated with each trade, creates a highly proprietary database subject to a broad threat profile. We note that there are entities within the federal government accustomed to dealing with very large electronic databases that are meant to be kept secret and secure from external threat. We strongly believe that FINRA CAT should look to this model to fully leverage the best-in-class information security infrastructure employed by the federal government as well as by certain companies in the private sector. We further believe that FINRA CAT should look to adopt the security initiatives from the Commission's August 2020 proposal on CAT data security, even in the absence of the Commission adoption of this proposal, as these initiatives would greatly enhance the security of CAT data.

1. Information Security Classification standards & subsequent controls.

By consolidating trading data across all exchanges and broker-dealers and being able to link this data with the brokers and customers who originated the trades, the CAT database should be viewed as much more sensitive than the constituent data individually, and thus worthy of a higher level of data security. For instance, it is likely that a similar federal data set would be marked SECRET, which then dictates the specific standards for holding, accessing and using the data. With the foregoing in mind, we would appreciate answers to the following questions:

A. Is it the case that the consolidated data is subject to a higher level of security control than is the constituent data & what classification level does SEC/FINRA assign to the consolidated data to be housed in the CAT?

B. The document "High Level CAT Security Requirements" suggests the CISO and COO of the Plan Processor are responsible for enforcing policies, procedures, and controls, for maintaining standards, but the standards themselves are the general security industry standards (SOC-2, NIST, etc.). Why is this level of control viewed as sufficient?

2. Amazon Web Services (AWS)

The Associations note that the IT architecture of the CAT should assume AWS will be compromised from time to time (insider, supply chain, etc.), and the data in the CAT should be secure against this kind of compromise.

The federal government uses AWS as part of its classified IT infrastructure. To make that happen, AWS established the AWS SECRET Region, which was designed and built to meet the regulatory and compliance requirements of the intelligence community. For other agencies of the federal government, AWS GovCloud was established to accommodate their security requirements. Similarly, we think the CAT should consider a similar framework. With the foregoing in mind, we would appreciate answers to the following questions:

A. Where is CAT data stored? AWS SECRET region, AWS GovCloud or alternate location? If AWS SECRET Region was not selected what was the rationale for a lower data security regime?

B. If an alternate location, what are the specific control standards deployed, and are they comparable to AWS Secret or AWS GovCloud?

3. Information Lifecycle

The CAT data is confidential and extremely sensitive to our members and their clients. It therefore should be hosted in a secure facility. Any processing, accessing, sharing or use of the CAT data should occur within an equally secure facility. Additionally, there should be a well-defined schedule for the lifecycle of the CAT data, including how and when to destroy the data, or declassify the data. With the foregoing in mind, we would appreciate you addressing the following areas:

A. Please describe the security specifications of the facilities in which the consolidated data is to be stored and accessed.

B. Please confirm that data cannot be bulk downloaded or transferred or stored outside of one of these secure facilities.

C. Please describe specifically the user access controls and supervision of the data.

D. Please describe the lifecycle of the data, including how and when to destroy or declassify the data.

4. Encryption keys

We recognize that CAT data will be encrypted. However, we note that key management is a critical aspect of safeguarding encrypted data. If the keys are compromised, then the encryption is not effective. We have reviewed the document titled "High Level CAT Security Requirements," but we note that it only states that there must be a plan for the keys, but it does not provide any information regarding this plan. We would appreciate answers to the following questions related to this plan:

A. Where are the encryption keys managed? Are they managed on AWS, or otherwise? Is there the equivalent of two-person integrity (TPI) control of access to information, at least one from outside the AWS environment?

5. Structured Encryption

We believe that the CAT data is most exposed when it is decrypted so it can be used in query and/or computation. We believe that structured encryption could help address this security concern, and would appreciate an answer to the following question:

A. Has FINRA CAT followed the developments in Structured Encryption, which allows query on encrypted structured data without the need for decryption?

6. Non PII data

In the document "High Level CAT Security Requirements" that we have reviewed, the section titled "Architecture-level Controls" in the last bullet of item 6 states that, "Non-PII CAT Data stored in a Plan Processor private environment is not required to be encrypted at rest." This statement raises concerns with us, and we would appreciate answers to the following questions regarding it:

A. What exactly does that mean? Does that mean consolidated trading data identified by FDIDs are not required to be encrypted at rest if they reside within prescribed environments within the AWS system? If so, when where and why? What about at the SROs?

B. Is this the allowance which enables the data to be used in computation? If so, are there requirements about how long the data is unencrypted before being erased? For instance, if an SRO download encrypted data, can they unencrypt the data and store it indefinitely either in their own system or within some environment within AWS?

7. CAT data Security audit

As you are aware, the issues associated with maintaining secure, large electronic databases are complex, very specialized, and technically complicated. We believe that the SEC and FINRA CAT would benefit from external review of CAT data security by an appropriate independent organization, one which has an established track record of working for the federal government on issues of science and technology in support of national security (e.g., JASON, NAS). Among other things, the CAT database will contain the Intellectual Property of our members and their clients, who have spent hundreds of billions of dollars over the years developing and will be highly sought after by both domestic and foreign actors, including potentially nation-states. The benefit of going to organizations such as these is that they can leverage existing federal government experience (e.g., reviews of IC, DOD, DOE, DOJ, NIST, etc.). We note that JASON has the security clearances necessary to engage in detailed conversations with government stakeholders already on the cloud. The output of this type of review would be a report directly addressing security issues associated with the CAT, with a view toward the most serious threats, and suggestions for best practices to minimize these threats. We the foregoing in mind, we would appreciate an answer to the following question:

A. Is FINRA CAT preparing to perform an external review of the CAT security pre-go live and on and ongoing basis?

*****

In sum, we note our concerns and suggested approaches above are consistent with testimony from the numerous Congressional hearings over the last five years regarding CAT data security standards, as well as best practices regarding data breach post-mortems and the overall protection of the intellectual property of our member firms and their clients, which is foundational to the integrity and growth of our markets. We very much look forward to continuing to work with FINRA CAT and the Plan Participants on this critical CAT endeavor of ensuring the security of CAT data.

Sincerely,

Ellen Greene
Managing Director
Equities and Options Market Structure
SIFMA

Jennifer W. Han
Executive Vice President
Chief Counsel & Head of Global Regulatory Affairs
MFA

Lindsey Weber Keljo, Esq.
Acting Head, Asset Management Group and Associate General Counsel
SIFMA

cc: The Honorable Gary Gensler, Chair, Securities and Exchange Commission
The Honorable Hester M. Peirce, Commissioner, Securities and Exchange Commission
The Honorable Allison Herren Lee, Commissioner, Securities and Exchange Commission
The Honorable Caroline A. Crenshaw, Commissioner, Securities and Exchange Commission

Director Haoxiang Zhu, Director, Trading and Markets, Securities and Exchange Commission
David Shillman, Associate Director, Trading and Markets, Securities and Exchange Commission