PRINCIPAL TRADERS GROUP

FIA Principal Traders Group
2001 Pennsylvania Avenue NW
Suite 600 | Washington, DC 20006

T 202 466 5460
F 202 296 3184

ptg.fia.org

October 23, 2017

Brent J. Fields
Secretary
U.S. Securities and Exchange Commission
100 F Street, N.E.
Washington, D.C. 20549-0609

Re: File No. 4-698: Joint Industry Plan; Notice of Filing of the National Market System Plan Governing the Consolidated Audit Trail

Dear Mr. Fields:

The FIA Principal Traders Group ("FIA PTG")[1] requests that the U.S. Securities and Exchange Commission (the "Commission") delay the upcoming self-regulatory organization ("SRO") consolidated audit trail ("CAT") reporting requirement set to start on November 15, 2017. FIA PTG has a long history of supporting data-driven decision-making and strongly supports regulators having access to the data required to ensure well-functioning markets.[2] However, in light of the recent Edgar and Equifax breaches, we have serious concerns about the security of data that will be required to be reported to a central repository under the CAT.

Our members utilize automated methods of trading and have invested substantial time and financial resources in the development of the trading systems and strategies they use. They would likely face tremendous losses and lose their ability to act as liquidity providers should information from the reporting of their trades be compromised. We urge the Commission to pause the CAT initiative until it can conduct a comprehensive analysis of

[1] FIA PTG is an association of more than 20 firms that trade their own capital on exchanges in futures, options and equities markets worldwide. FIA PTG members engage in manual, automated and hybrid methods of trading, and they are active in a wide variety of asset classes, including equities, fixed income, foreign exchange and commodities. FIA PTG member firms serve as a critical source of liquidity, allowing those who use the markets, including individual investors, to manage their risks and invest effectively. The presence of competitive professional traders contributing to price discovery and the provision of liquidity is a hallmark of well-functioning markets. FIA PTG advocates for open access to markets, transparency and data-driven policy and has previously made recommendations about a variety of equity market structure issues, including Regulation NMS (*see* https://ptg.fia.org/keywords/equity-market-structure).

[2] See FIA PTG response to the Treasury Department's Request for Information (RFI) on the evolution of Treasury market structure at 20.

the security of the CAT and can satisfy market participants that effective and robust security measures are in place to protect the CAT trade repository database against cyber breaches. At a minimum, we ask that no trades be reported until the Commission answers the following set of questions related to the CAT, Reg NMS LLC and the Plan Processor to help assuage the concerns of affected market participants.

All references to "the firm" in the following list apply to Reg NMS LLC and/or the Plan Processor as appropriate:

Policy & Framework

1. Does a documented security framework exist?
2. What security frameworks has the firm aligned with and has it achieved certification? Please provide proof of certifications.
3. Describe the firm's BYOD policy.
4. Does a documented incident response plan exist?
5. Does the firm perform table top IR exercises and have playbooks built for its IR?
6. Does the firm have an on call 3rd party IR specialist?
7. Does the firm have a policy or security requirements in place for third party vendor access to the network or data?
8. How often does the firm provide user education around security awareness?
9. How does the firm assess employees' security understanding?
10. What is the firm's disaster recovery plan?
11. What training do the firm's development and testing teams receive specifically as it pertains to application security?
12. Does the firm adhere to an application security development lifecycle framework? If so, which one(s)?
13. Does the firm have a formal change control policy?
14. Does the firm have a formal DLP policy?

Network Security

1. Are there intrusion detection and prevention controls in place to monitor network traffic?
2. Does the firm monitor for unauthorized network connections?
3. Is there network segmentation of sensitive networks? What controls are used to secure these networks?
4. Does the firm provide Wi-Fi access to corporate and non-corporate assets? If so what type of security and rogue AP detection is used?
5. Does the firm capture and correlate events gathered from all endpoints?
6. Does the firm support and implement Multi Factor authentication for network, email and other various access?

Identity & Access Management

1. How will the expected 3000 users of the system log in to the system?
2. What authentication methods will be supported for the CAT? (e.g. local, SAML, 2FA, common password vaults)
3. How will user access be provisioned? How often will this access be audited to make sure it is still appropriate?
4. Will remote access be enabled for the system? If so, are there security requirements that will be enforced? (VPN, RDP, etc.)
5. Will there be functionality implemented to restrict access to specific IP addresses on a per account basis? (JDoe can only log in from x.x.x.x)
6. Who will have access to the authentication and access logs? How will they be secured?
7. How long are authentication and access logs retained?
8. Are access sessions recorded?
9. Are personal assets (laptops, phones, tablets) allowed to access firm resources?
10. What controls are in place for endpoint protection? Are they active or passive controls?
11. Describe the patch management process.
12. Are access controls implemented and using least privilege?
13. Describe the firm's password policy and how it is enforced.
14. Does the firm regularly perform vulnerability assessments, Red Team exercises, and/or penetration tests?

Data Protection/Security

1. Will the CAT data be encrypted at rest? What encryption methods will be used? Who will have access to the private keys and where will they be stored? Is the firm using key escrow?
2. Will the CAT data going out be encrypted in transit? What encryption methods will be used?
3. What types of controls will be in place to ensure the integrity of the data? How often will backups be tested? Are backups encrypted? Which encryption mechanism?
4. How long will data be retained?
5. What is the firm's data destruction process and policy?
6. How often will the data be backed-up and where will it be stored (AWS Glacier, physical tapes?)
7. What does the recovery time look like in a disaster recovery situation?
8. How often will external penetration tests be performed and who will conduct those tests?
9. Who will have access to the CAT data?

Security Operations

1. What if any client data is/will be stored in the cloud? On-premises? Whose jurisdiction will the data reside?
2. Do servers containing client data have access to the Internet?
3. How is/will client data compartmentalized?
4. Is there a difference in security controls that are in place between systems that contain client data and other systems?
5. How is physical security handled for servers that contain client data?
6. How often does the firm audit highly privileged account usage and regular privileged accounts?
7. How are backups of client data handled and are they encrypted?
8. Does the firm allow for the use of usb/removable media (encrypted / monitored)?
9. Describe how the firm monitors for data exfiltration. Have there been any data exfiltration events in the past 12 months?
10. Describe the firm's Employee Lifecycle Management process.
11. Does the firm have an on premise version of your software?
12. Does the firm have a bug bounty program?
13. Does the firm manage the firm's security operations internally or is this outsourced to a third party?
14. Does the firm manage and own the server and network infrastructure or is it outsourced (third-party managed service) or cloud-based?
15. Describe the firm's AI model and approach, as it relates to CAT data.
16. Will the firm provide results of third-party external audits carried out within the past two years?

Compliance

1. Does the firm integrate with any third-party eDiscovery or compliance services?
2. What level of logging does the firm perform on actions within the service? Does the firm log deletes?
3. Does the firm have the ability to create compliance exports of CAT data? If yes, in what format?
4. Does the firm have an open API that can be used to collect compliance data?

Detection/Response

1. How will the CAT database be monitored? And who will monitor it?
2. Have any Thesys products been compromised as part of a breach in the past five years?
3. What DDOS protections will be leveraged (Cloudflare?)

We look forward to reviewing the responses to these questions and in the interim urge the Commission to delay the start of SRO reporting to the CAT until all impacted parties have adequate assurances from the Commission that their trade data will be protected. If you have any questions about these comments, or if we can provide further information, please do not hesitate to contact Joanna Mallers (jmallers@fia.org).

Respectfully,

FIA Principal Traders Group

Joanna Mallers

Joanna Mallers
Secretary

cc: Walter J. Clayton, Chairman
Michael S. Piwowar, Commissioner
Kara M. Stein, Commissioner