USAA®
9800 Fredericksburg Road
San Antonio, Texas 78288

March 21, 2014

Marcia E. Asquith
Office of Corporate Secretary
FINRA
1735 K Street, NW
Washington, DC 20006-1506
pubcom@finra.org

Re: Comprehensive Automated Risk Data System (Regulatory Notice 13-42)

Ladies and Gentlemen:

In the interest of our members – the men and women of the U.S. military and their families – United Services Automobile Association (USAA) is pleased to provide our comments to the Financial Industry Regulatory Authority (FINRA) with respect to the Request for Comment on a Concept Proposal to Develop the Comprehensive Automated Risk Data System (CARDS)[1] (the Concept Release).

USAA is a membership-based association, which together with its family of companies, serves present and former commissioned and noncommissioned officers, enlisted personnel, retired military, and their families. Since USAA's inception in 1922 by a group of U.S. Army officers, we have pursued a mission of facilitating the financial security of our members and their families by providing a full range of highly competitive financial products and services, including personal lines of insurance, retail banking, and investment products. Our core values of service, honesty, loyalty, and integrity have enabled us to perform consistently and be a source of stability for our members and customers, even in the midst of the financial crisis of recent years.

USAA appreciates FINRA's efforts to become faster, more efficient and more effective in protecting investors and ensuring market integrity. However, USAA has concerns that CARDS may amount to an invasion of privacy and may pose a security risk to our members' data. The risks associated with a potential invasion of privacy or data security breach are high, and the associated costs – both actual and reputational costs – are substantial, yet the Concept Release does not set forth the material benefits of CARDS for member firms or the investing public.

In this letter, we stress the significant burden, liability, and responsibility FINRA is taking on by transferring, storing and eventually destroying the information requested through CARDS. Although we hope FINRA reconsiders the application of CARDS altogether, if it should go forward, FINRA must use the highest industry standard practices to de-identify data and protect information. Finally, FINRA must provide a clear plan in the event of a data breach and address FINRA's (or member firms') liability should a breach occur.

---

[1] FINRA Regulatory Notice 13-42, Comprehensive Automated Risk Data System (Dec. 2013).

1. CARDS could make FINRA a target for information security breaches and jeopardize the private, personal data of our members.

At the heart of USAA's relationship with our members is a privacy promise to safeguard their personal information. We take this promise very seriously. Further, as a financial services provider and a keeper of personal information, especially for members of the U.S. military community, privacy and information security are among our top priorities. We are concerned that CARDS will increase the vulnerability of the data of our members, many of whom, by virtue of their positions within the military, are particularly sensitive to privacy issues.

By consolidating in a single place, the financial life of nearly the entire investing public, CARDS is an obvious target for hacking and raises security concerns at least as great, if not greater, than those faced by individual firms. The risk to investors is magnified considering that a hacker need only defeat one system, FINRA, to gain access to client information from any firm.

Even if FINRA could ensure the CARDS data was secured and protected from external vulnerabilities, USAA still has privacy concerns. CARDS will allow an additional access point for our members' private information. We urge FINRA to limit the individuals who will have access to CARDS information (*e.g.*, FINRA staff, systems administrators, third-party vendors) and to consider whether those individuals will be subject to heightened background checks or other standards and how those individuals will be supervised and re-evaluated.

We appreciate that FINRA has stated it will not seek personally identifiable information (PII) through CARDS and will instead focus on acquiring account identifying information. Although removing PII from the process and from CARDS reduces the risk to member firm information, it does not eliminate it, especially if FINRA requests individual account numbers. CARDS would still act as a gateway to PII at the member firm or clearing firm and jeopardize the privacy of our members' information.

2. CARDS will subject FINRA and member firms to additional liability.

The Concept Release does not address the liability of FINRA or member firms for a CARDS security breach, either during a firm's transmission to FINRA or while FINRA is in possession of the required data. For example, the Concept Release does not contemplate how FINRA would react in response to a breach of information, the timeframe in which FINRA would notify the submitting firm or who would provide notification to affected individuals. Further, data security breaches are expensive to address. On average, it costs U.S. companies approximately $188 per record to address a data security breach.[2] In addition, reputational harm can cause immeasurable damage in the form of loss of existing customers and can negatively impact business growth. The potential for reputational harm is particularly important to USAA, as we a place high value on our members' trust. Would FINRA be responsible for all costs associated with a FINRA breach or provide indemnity to the member firm? In either case, how would FINRA account for, and compensate for, reputational harm? We urge FINRA to develop and publish a clear plan for addressing data security breaches.

---

[2] Ponemon Institute LLC, Ponemon Institute© Research Report, *2013 Cost of Data Breach Study: Global Analysis*, p. 1, May 2013, *available at* http://www.ponemon.org/local/upload/file/2013%20Report%20GLOBAL%20CODB%20FINAL%205-2.pdf.

3. Employ an industry-acceptable information security standard for the protection of information.

The Concept Release does not fully describe the security measures FINRA will take to protect customer information. In the Concept Release, FINRA states it will incorporate current and effective information security methods but does not specify what information security it will employ.

The manner in which FINRA plans to de-identify data is a key element of data security. If a requirement of CARDS is to join records from disparate systems based on identifiable persons (*e.g.*, associated persons or customers), FINRA should mandate a standard algorithm that all introducing firms and clearing firms will use to create a surrogate key from a primary key of the person (*e.g.*, SSN or registered person CRD number). The surrogate key would create a unique value that FINRA can use to join records from the disparate systems, and the surrogate key should not be capable of reverse engineering to obtain the primary key. If FINRA identified a particular concern and needed to re-identify a particular individual, the submitting firm could then provide that individual's identity.

We recommend FINRA employ a standard, such as the National Institute of Standards and Technology (NIST) - Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information or its equivalent (*e.g.*, the international standard ISO 27000 series), for the full de-identification of PII prior to information submission to CARDS by introducing firms and/or clearing firms. These controls should be published well in advance of any rulemaking.

4. Conclusion

We recommend that FINRA reconsider its use of CARDS. However, should FINRA move forward, we request that FINRA:

- Publish its privacy policy and requirements for transmission, storage, retention, and destruction of the data collected through CARDS.
- Address FINRA's liability to member firms for potential security breach.
- Detail the disclosures member firms will be required to provide customers regarding the measures FINRA is taking to protect data maintained by CARDS.
- Clearly articulate the material benefits that collection of such sensitive data will achieve.

Such information will allow member firms to initiate a full information security risk assessment and work to alleviate as many concerns as possible to protect customer data.

* * * * *

We appreciate FINRA's consideration of our comments. Should you have any questions or wish further clarification or discussion of our points, please contact Daniel Mavico, Executive Director at 210-498-0034.

Sincerely,

Steven Alan Bennett
Executive Vice President
General Counsel & Corporate Secretary