BDA Bond Dealers of America

21 Dupont Circle, NW • Suite 750
Washington, DC 20036
202.204.7900
www.bdamerica.org

December 1, 2014

VIA ELECTRONIC MAIL

Marcia E. Asquith
Office of the Corporate Secretary
Financial Industry Regulatory Authority
1735 K Street, NW
Washington, DC 20006-1506

RE: **FINRA Regulatory Notice 14-37: FINRA Requests Comment on a Rule Proposal to Implement the Comprehensive Automated Risk Data System ("CARDS")**

Dear Ms. Asquith:

On behalf of the Bond Dealers of America ("BDA"), I am pleased to submit this letter in response to the Financial Industry Regulatory Authority's ("FINRA") Regulatory Notice 14-37 (the "Notice"), requesting comment on a proposed rule to implement the Consolidated Automated Risk Data System ("CARDS"). BDA is the only DC based group representing the interests of middle-market securities dealers and banks focused on the United States fixed-income markets and we welcome this opportunity to present our comments on this Notice.

BDA supports FINRA's goal of making the examination process more efficient and more effective from an investor protection standpoint. However, rather than making the examination process more efficient, FINRA's CARDS proposal would fundamentally alter the examination process, subject firms to unknown costs and risks and expose brokerage customer information to dramatically increased risks, the costs of which have not been recognized or estimated by FINRA to any reasonable extent. BDA does not believe the Notice provides firms, especially small-to-medium sized broker-dealers, with sufficient information to estimate the initial or ongoing cost burden of CARDS. In addition, the proposal raises significant data security, privacy, and cybersecurity risk concerns for the investing public.

BDA is concerned with the proposed rule's lack of detail with respect to cost estimates for the accumulation and disclosure of customer information under CARDS, especially in relation to small and middle-market broker-dealers. The discussion of the proposed rule includes a per-firm estimated cost range of $390,000 to $8.33 million for the implementation of CARDS in addition to an ongoing, annual cost estimate range of

$76,000 to $2.44 million for each FINRA member firm. FINRA's discussion of the anticipated cost burden of CARDS includes a litany of cost categories but does not provide firms with a detailed breakdown of the itemized cost estimates associated with each particular cost category. This gives small-to-medium sized firms little basis to judge if the cost burdens presented in the Notice are reasonable and if they capture all the changes firms will have to make in order to comply with CARDS, including increased cost burdens incurred from the use of third party vendors and hiring additional IT, compliance, and operations personnel and addressing increased security risks arising out of the standardization of data configurations to comply with the data disclosure requirements of the propose rule. Based on what little firms have been told about CARDS, the low end of these cost ranges do not appear feasible. This lack of clarity on costs is alarming for firms, especially in light of the trend towards greater industry consolidation. BDA is concerned that greater consolidation driven by burdensome regulatory costs will harm competition and reduce investor choice.

Therefore, we would ask FINRA to provide clarification, for the benefit of firms, of each specific cost category it anticipates would be associated with the CARDS proposal. It is extremely difficult for firms to anticipate the cost burden of what they will be required to spend on technology, back office, operations, third party vendors, new information delivery requirements, and new data security measures in connection with the new disclosures of customer account data under CARDS without comprehensive details provided by FINRA. Firms need a clear roadmap to better judge how burdensome it will be to implement the sweeping changes contemplated by FINRA.

BDA is concerned that the Notice contains no specific basis for judging the purported cost savings from retiring redundant regulatory requirements. The Notice describes potential cost savings for firms associated with the retirement of certain regulatory reporting obligations. However, it does not provide sufficient detail on what overlapping or redundant reporting obligations CARDS will create, which reporting obligations will be definitively retired, and the timetable on which FINRA plans to retire any redundant or overlapping reporting obligations. Without this crucial information it is impossible for firms to assess what the overall cost burden of CARDS will be on an ongoing basis.

Additionally, in order to interact effectively with FINRA in connection with these proposed new customer data disclosure requirements, FINRA should disclose to firms the data analysis, and data analytic programs, screens and procedures that FINRA intends to conduct utilizing this customer data. This would enable firms to have a meaningful opportunity to conduct similar screenings, analyses, and analytics and be prepared to communicate with FINRA, regarding the results of its screenings, analyses, and analytics of this customer data.

Firms are going to have to engage technology, IT departments, and outside vendors in a manner that will require significant time and costs above and beyond the current systems they have in place, which already require monitoring, maintenance, periodic reviews, and frequent updates in response to constantly changing and

increasingly complex regulatory requirements. Therefore, we ask FINRA to clarify as specifically as possible what firms can anticipate in the way of having to retire or change internal systems in order to meet the upcoming demands of this entirely new system for formatting, maintaining, and disclosing customer account data. Doing so would promote efficiency, improve budgeting, and reduce potentially wasteful spending for firms.

BDA seeks additional information regarding FINRA's ability to protect customer investment and account information. CARDS would create a centralized database containing comprehensive information on individual investment accounts and investor transactions. Under the CARDS proposal, this customer account information would be required to be formatted in a uniform format by all firms and disclosed on a regularly scheduled basis to FINRA. The customer account information would be held by FINRA in a centralized database, pulled from a variety of sources that are currently hosted separately by separate firms. Thus, this newly disclosed customer account data would likely become more vulnerable to targeted cyber attacks. The Notice explains that FINRA has had access to firm-specific confidential information in addition to the investor account and transaction information that it proposes firms submit in CARDS. But, FINRA has never been responsible for holding or protecting, in one centralized location, the amount of investor information it proposes to compile in CARDS. Nor has FINRA, in the scale envisioned by CARDS, elaborated upon how it intends to ensure that investor and account data will be protected during transmission.

As opposed to the non-comprehensive information, tailored by FINRA to particularized review and examination procedures, that FINRA may currently hold, FINRA intends to collect defined, comprehensive, and highly valuable customer account and investor information in CARDS. The publicly defined investor information held in CARDS will be a far more valuable target for intrusion than anything FINRA currently holds. The implementation of CARDS monumentally heightens the risk profile for the customer account data proposed to be gathered and held by FINRA. Yet, the Notice does not outline any enhancements to FINRA's data security capabilities, procedures, or protocols related to keeping customer account data secure under CARDS, in transmission or in storage. The Notice merely states, "FINRA would apply to CARDS the many security controls and protocols it already has in place." The Notice does not include any substantive commitment to enhance FINRA's ability to protect sensitive customer account data for over 110 million U.S. investors. Therefore, the BDA requests a more detailed assessment of FINRA's current data security capabilities, and with more specifics than the three paragraph description offered in the Notice, entitled "B. Data Security."

Data security problems have been widespread throughout the federal government. The CARDS proposal is especially troubling in light of the widespread data security issues that have been identified at federal agencies. A 2012 Government Accountability Office report outlined "material weaknesses" in the data and cyber security capabilities, policies, and protocols at most federal agencies.[1] The report notes

---

[1] *See U.S. Government Accountability Office, "Cybersecurity: Threats Impacting the*

that multiple assessments of "information security controls during fiscal year 2011 revealed that most major federal agencies had weaknesses in most of the five major categories of information system controls,"[2] including "access controls, which ensure that only authorized individuals can read, alter, or delete data."[3] In addition, a separate GAO audit of the Securities and Exchange Commission (SEC) found significant weaknesses with the Commission's access controls and its ability to store and protect confidential financial information.[4]

Recognizing that FINRA was not reviewed in the GAO report, BDA is nonetheless concerned as a result of FINRA's direct connection and information sharing with federal agencies, coupled with the Notice's lack of detail on exactly who beyond FINRA's walls will have access to customer account information to be collected by FINRA under the CARDS proposal. The Notice states that FINRA would limit access to the "raw data" held in CARDS. The proposal does not detail which other FINRA employees, federal regulators, other Self Regulatory Organizations (SROs), or third-party contractor employees could, in the future, have access to customer account information to be collected by FINRA under the CARDS proposal that may not be considered to be in a "raw" format such as analyses of investment accounts or individual transactions based on raw data. BDA requests that FINRA more fully discuss which other federal agencies or SROs it could share access to customer account data to be collected by FINRA under the CARDS proposal or to reports or analytic data derived from such customer account data and to what extent FINRA's contract or consultant employees would have access to CARDS reports or data.

BDA disagrees with FINRA's assessment that the risk of a cyber attack or security breach is "remote." The BDA appreciates FINRA's decision to not collect certain items of Personally Identifiable Information (PII), including customer names and addresses, Social Security and tax identification numbers in CARDS. However, even with exclusion of such items of PII, the customer account data FINRA intends to collect through CARDS is valuable and raises serious cyber security concerns.

Cyber security attacks have become more prevalent in recent years. Hackers have penetrated the networks of the Federal Reserve System, the Department of Defense (DoD), and the National Aeronautics and Space Administration (NASA). As a 2014 (GAO) report about cyber threats notes, "The cyber-threats facing the nation are evolving and growing, with a wide array of potential threat actors having access to increasingly sophisticated techniques for exploiting system vulnerabilities."[5] Furthermore, in recent years, myriad private businesses and government entities have been hacked. The private

---

[2] ibid.

[3] ibid.

[4] *See U.S. Government Accountability Office, "Information Security: SEC Needs to Improve Controls over Financial Systems and Data," April 17, 2014, Available: http://www.gao.gov/products/GAO-14-419*

[5] *See GAO Report, "Cybersecurity: Threats Impacting the Nation,"*

information associated with millions of U.S. consumers was compromised in the cyber attacks on Target, Home Depot, and JPMorgan Chase.

The 2014 Annual Report of the Financial Stability Oversight Council's (FSOC) highlights the potential for a cyber attack to harm the stability of the U.S. financial system. The report states, "Cyber incidents can impact the confidentiality, integrity, and availability of the information and technologies essential to the provision of services, resulting in financial, compliance, and reputation risk. Moreover, cyber incidents that disrupt, degrade or impact the integrity and availability of critical financial infrastructure could have consequences on operations and efficiency. Such incidents can undermine the confidence of consumers and investors, and ultimately, threaten the stability of the financial system." [6]

Therefore, BDA disagrees with FINRA's judgment that the risk of a security breach is "remote." BDA does not believe that FINRA has acknowledged the potential risks for a cyber attack on the CARDS database, a breach during the transmission of data, or outlined its cyber attack detection or defense capabilities in any serious way.

Thank you again for the opportunity to submit these comments.

Sincerely,

Michael Nicholas
Chief Executive Officer

---

[6] *See Financial Stability Oversight Council, 2014 Annual Report, Available: http://www.treasury.gov/initiatives/fsoc/studies-reports/Pages/2014-Annual-Report.aspx.*