Cornell University
Law School

Lawyers in the Best Sense

WILLIAM A. JACOBSON
Clinical Professor of Law

154 Myron Taylor Hall
Ithaca, New York 14853-4901
T: 607.255.6293
F: 607.255.3269
E: waj24@cornell.edu

March 20, 2014

Via E-Mail (pubcom@finra.org)

Marcia E. Asquith
Office of the Corporate Secretary
FINRA
1735 K Street, NW
Washington, DC 20006-1506

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

Dear Ms. Asquith:

The Cornell Securities Law Clinic (the "Clinic") welcomes the opportunity to provide feedback on the proposal contained in Regulatory Notice 13-42 ("Regulatory Notice") of the Financial Industry Regulatory Authority ("FINRA") regarding Comprehensive Automated Risk Data System ("CARDS"). The Clinic is a Cornell Law School curricular offering, in which law students provide representation to public investors and public education as to investment fraud in the largely rural "Southern Tier" region of upstate New York. For more information, please see: http://securities.lawschool.cornell.edu.

While the Clinic appreciates FINRA's initiatives to find new ways to better protect investors, the Clinic is against the proposal until FINRA satisfactorily addresses all the concerns stated in this letter.

1. Overall Concern

FINRA has not adequately justified this undertaking.

CARDS is a massive and costly project that involves collection and usage of private information. Consequently, it will introduce privacy, security, cost, and legal issues as discussed below. While technology enables collection and analysis of mass data, the implementation of CARDS requires a strong justification because investors will face these serious issues.

FINRA should describe the impetus for initiating CARDS and detail all the problems that CARDS intends to solve. Investors need to fully understand why the current examination methodology fails to solve those problems and how CARDS will eliminate them. FINRA should

provide a full cost-benefit analysis where costs and benefits for all the stakeholders—including FINRA, clearing firms, introducing firms, and investors—are taken into account. All the alternative solutions considered in place of CARDS and their shortcomings should be explained. Moreover, investors need to understand the complete timeline of the project.

The next three sections describe the Clinic's specific concerns.

2. Privacy and Security Concerns

The risk of a data breach directly correlates to the number of data servers and the amount of data held at each server. Because CARDS will require the FINRA's server to store and use new data, CARDS will necessarily increase this risk.

In its update on March 4, 2014, FINRA stated that "FINRA has concluded that the CARDS proposal will not require the submission of information that would identify to FINRA the individual account owner, particularly, account name, account address or tax identification number." If FINRA follows this conclusion, the risk will be reduced but will not be eliminated.

a. Investors should be assured that their personal information will not be compromised.

As additional functions are implemented to CARDS in the future, more data might be required. FINRA stated that it "expects that as applicable securities laws and FINRA rules evolve and are amended to include additional books and records requirements, it would revise CARDS' data specification elements to include that information." (Regulatory Notice, p. 9.) Investors should have an assurance that their personally-identifying information, such as their names, account numbers, addresses and tax identification numbers, will never be submitted to CARDS. The Clinic suggests two ways to achieve this.

First, FINRA should make and commit to a public statement stating that no personally-identifying information will ever be submitted to CARDS.

Second, FINRA should disclose and describe all the data fields that CARDS intends to use. Such a disclosure should be published at the implementation stage and continuously updated. Even without personally-identifying information, an investor's identity could be compromised from a set of data values related to the investor. The proposed disclosure would give an opportunity to the public to comment on such a problem. If FINRA plans a material change to the data requirement of CARDS, a new regulatory notice should be created.

b. Three implementation methods are suggested to alleviate privacy and security concerns.

First, data with no expected future use should be destroyed permanently. This can be achieved by setting data to expire after a certain period of time or destroying data if a specific time period has passed since the data's last accessed time.

Second, data should be stored in aggregate forms to the extent possible. For example, data could be grouped by type per broker instead of storing each investor's data separately.

Third, CARDS could be executed directly on the system where the data source resides. For example, FINRA could implement CARDS as a black-box program and distribute it to clearing and introducing firms. After these firms execute the program on their systems, the program would automatically send reports to FINRA. Such reports would contain information about only problematic transactions. This distributed execution mechanism will eliminate additional privacy and security issues introduced by CARDS.

c. Strict security measures are required.

CARDS should be physically and remotely accessible only by designated users. Information about interactions with CARDS, including accessed times and users, should be logged. Implementation of firewalls, maintenance of strong password systems, and encryption of data are also critical.

3. Cost Concerns

The Clinic is concerned with costs associated with CARDS because investors will eventually bear the increased costs. CARDS will require a significant amount of financial and human resources to implement and maintain.

Types of costs and parties who will directly bear these costs are summarized in the following table:

	FINRA	Clearing/Introducing Firms
Start-up Costs (One-time)	• Design, development, and implementation of CARDS • Hardware purchase and lease	• Implementation of FINRA's requirements, including standardization of data
Training Costs (Ongoing)	• Education and training for FINRA employees and outside users	• Education and training for employees
Maintenance and Upgrade Costs (Ongoing)	• Defect fixes, system patches, and CARDS upgrades • Overhead in running hardware • Hardware replacement and upgrade	• Regular data submission • System and data maintenance to keep in compliance with the FINRA requirements

Before proceeding with CARDS, FINRA should provide estimates of these costs, budgetary plans, and expected cost allocations between FINRA, clearing firms, and introducing firms. Moreover, FINRA should perform an extensive study on the potential impact on investors. If FINRA expects any savings from CARDS, such as savings from a reduced number of on-site examinations, FINRA should describe them as well.

4. Legal Concerns

The Clinic has three additional legal concerns.

First, the proposal does not state the legal authority that allows FINRA to collect and use investors' financial data in a centralized manner. FINRA should specify the relevant authority.

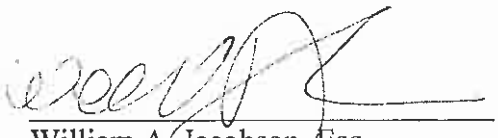
Second, although FINRA stated that "CARDS would not supplant the legal, compliance and supervisory programs firms administer" (Regulatory Notice, p. 7), the existence of CARDS may become an issue in arbitration and other cases. For example, when an investor sues a firm for a loss caused by negligent oversight, the firm might argue that it was not negligent because CARDS did not detect any issue. FINRA should ensure that CARDS does not place such an additional burden on investors to prove firms' wrongdoing.

Third, FINRA should explain legal consequences of a data breach, including but not limited to FINRA's liability and that of firms producing data. Data may be breached both internally and externally. Internal rogue users, who may be employees, contractors, or visitors, at FINRA will pose internal risks. Externally, hackers will attempt to gain access to CARDS. When a data breach occurs, investors will require legal remedies. FINRA should explain how it intends to provide such remedies.

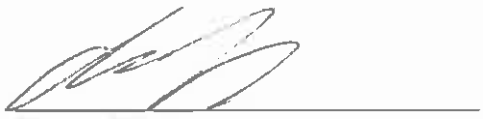
Conclusion

CARDS will introduce serious risks to investors. Because the Clinic is concerned about privacy, security, cost, and legal issues associated with CARDS, the Clinic is opposed to CARDS until FINRA satisfactorily addresses all the foregoing concerns.

Respectfully submitted,



William A. Jacobson, Esq.
Clinical Professor of Law, Cornell Law School
Director, Cornell Securities Law Clinic



Young Wook Lee
Cornell Law School '15