DIAMANT
INVESTMENT CORPORATION

Comprehensive Portfolio Management

November 21, 2014

Marcia E. Asquith
Office of the Corporate Secretary
FINRA
1735 K Street
Washington D.C. 20006-1506

RE: Comment on CARDS concept proposal – Regulatory Notice 14-37

Dear Ms. Asquith,

As a securities industry veteran with over thirty six years running a self clearing broker/dealer, I am stunned that the FINRA Board of Governors (Board) is still even contemplating moving forward with a Comprehensive Automated Risk Data System (CARDS). The numerous, thoughtful, detailed, written comments opposing CARDS, per Regulatory Notice 13-42, seem to have been dismissed as irrelevant because they go against the wishes of a few overzealous regulators. FINRA seems almost smug in their misguided belief they have completely solved privacy concerns by removing some obvious customer information from the CARDS data collection. I urge the Board to now act as both Statesmen and Leaders of our securities industry, and stop the implementation of CARDS.

First, it is important to recognize that most everyone participating in the securities industry wants customers to be treated fairly. Security industry participants who disagree with this position would typically be deemed troubled brokers. The real issue behind CARDS is whether the existing FINRA organization is able to perform its regulatory mandate, or if there is a need to dramatically reduce the FINRA staff that review the industry and replace them with a database. Regardless of the organizational structure, there always will be some troubled brokers working in our industry.

According to the FINRA 9/30/14 video segment that interviewed Ms. Axelrod of FINRA Regulatory Operations, the only way to identify troubled brokers and associated trades is to create a massive central database of sensitive customer information. The unbridled enthusiasm demonstrated in this video segment illustrates a very narrow focus of pursuing a gigantic regulatory solution, along with a complete lack of perspective or understanding of the larger and more important issues of customer privacy and the costs to the securities industry.

Destroying customer privacy and weakening the financial structure of brokerage firms in the pursuit of "protecting the customer" should not be the objective of the FINRA Board. Seasoned businesspeople in a cross section of industries, and persons in the information technology business quickly conclude that customer privacy will be destroyed under any CARDS system. All that I have

170 MASON STREET ∽ GREENWICH, CONNECTICUT 06830
(203) 661-6410 ∽ (800) 342-4255

spoken to are in disbelief that a system like CARDS has reached the level of a Board discussion. Presumably by now the Board members have had similar discussions with many persons in the real world who are outside the ivory tower of FINRA and its CARDS proponents. The Board must demonstrate a larger understanding of the entire issues when making the decision to terminate CARDS.

CARDS Trial Run

The decision to plow ahead with this concept was based on a sample data test with a couple of very large clearing firms. By avoiding input from the rest of the securities industry, staffers proceeded to design a very complicated system that is only workable for the very large clearing type firms.

Most interesting is just how few potential trade issues were uncovered in this initial sample test of the CARDS system. In the March 3, 2014 Barron's article by Jim McTauge, titled "Big Brother vs. Wall Street", the author describes how FINRA wants to collect details on 70 million brokerage accounts. The article points out that the trial run of CARDS examined 92,000 accounts and identified 13 potential problems that warranted closer inspection.

So we all understand this, FINRA proponents justify the creation of a very large and tremendously costly database because they found 13 possible issues on a sample size of 92,000 accounts. This is just 0.01% of the sample! It is likely that upon further review, many of these 13 issues would be reasonably explained to an examiner. This leaves just a handful of activity that CARDS detected for regulatory review.

This success rate is statistically insignificant. There is no way the securities industry can justify the financial cost of complying with CARDS for so little benefit. Reasonable interpretations of this CARDS sample test is that: (a) further development and implementation of the CARDS system is not needed, (b) the financial burden on the brokerage firms to comply with the CARDS system is unnecessary, and (c) the statistically insignificant measurement of questionable activity suggests the securities industry is doing a credible job in self-regulation from existing processes.

Cost to the Industry

CARDS is a major database undertaking for any size brokerage firm, but will really harm both smaller and mid-size brokerage firms if they are forced to deploy resources to comply with CARDS. Required reading by the Board should be the entire CARDS record layout. It comprises nearly 30 pages of very specific transaction data, along with another 7 pages of codes. When reading the voluminous record layouts, it became clear the designers of this database have no working experience with anything other than a very large computer information system.

However, not all brokerage firms in the securities industry have a need for a very large computer information system. For example, our back office system is a smoothly operating, efficient, and very accurate accounting system that was designed not to run on a large mainframe computer. To maintain customer privacy on the sensitive information we are entrusted with, we purposely do not

maintain confidential customer information on our back office system. The CARDS system would force us to collect and collate this information from several internal sources in order to transmit to a central government type massive database. Because we do not currently maintain all the fields specified in the record layouts, we foresee an extended effort that will include the re-writing of much of our software code, which I place an initial cost of over $2 million to implement.

We have experience implementing many data interfaces over the past decades, but attempting to comply with the CARDS record layouts would be the largest and most expensive coding effort in the 40 year history of our brokerage firm. What is most disturbing is that CARDS would force us to invest in a cost prohibitive regulatory solution that attempts to identify problems that simply do not exist at our firm.

Data Breaches

CARDS proponents recently removed the most sensitive customer information of customer name, address, and social security numbers from the record layouts. But within the remaining 30 pages of coding, the current proposal still has sensitive customer information that will make this large database a terrific target for data breaches of customer information. This means is the current CARDS proposal is still a dangerous system in terms of losing customer confidentiality throughout the entire securities industry.

As I have detailed in my two prior comment letters dated January 17th and March 14th , a very large central database of customer information will have a wealth of data that will be the target of data breaches. Data breaches can occur from inside FINRA by trusted employees, such as what happened with Mr. Snowden at the National Security Agency. They also can occur from external hacking of the data base. There are numerous cases of data breaches at retailers and financial institutions by sophisticated hackers who profit from collecting this information. In a CARDS system designed by FINRA staff who naively included customer names, addresses, and social security numbers in their proposed layouts, rest assured data breaches will happen. FINRA does not have the tools or the expertise to completely prevent data breaches of what may become the largest database of confidential customer information in the world.

To connect the dots, a successful data breach will happen in two stages. The first stage will be to breach the CARDS data base to collect important customer information on specific account numbers at specific brokerage firms. The second breach will occur at specific brokerage firms where the bad guys now only need to identify the customers behind specific account numbers. This will compete their theft of customer information. Thus, removing some customer information from CARDS has not solved any customer privacy concerns, as it is now a two step process to complete a data breach of customer information.

By contrast, in the current environment where CARDS does not exist, customer information resides at numerous brokerage firms, each with different accounting systems and protective systems of confidential information. Customer information is widely dispersed among brokerage firms, and the bad guys do not know which brokerage firm has important customer information that they could profit

from. Yet once all customer information is placed into one central national database, FINRA will unwittingly have made the job of stealing very sensitive customer information much easier.

Destruction of Customer Privacy

The issue of the destruction of customer privacy is much more important than any regulatory compliance benefit. Within the existing CARDS record layouts, the entire securities industry will be forced to include the following information on its customers to a central database.

1) Customer account number and name of brokerage firm.
2) Household accounts: account number or name identifier of a customer's household group of accounts, and which account is the largest parent account when combined with other accounts for margin purposes.
3) Customer net worth: Value of their investment portfolio and the rest of their net worth.
4) Ownership of specific securities: The amount of shares held in each security by the customer account along with the market value of these securities held by the account.
5) Security transactions: A list of what securities the customer account buys and sells, and the amount of money used to buy or sell each position.
6) Customer liquidity: The amount of cash and money market balances held by a customer account.
7) Active traders: identifying whether a customer is a day trader.
8) Customer borrowing needs: Identifying if the account uses margin to borrow money, when margin calls trigger forced sales, and the amount borrowed if on margin.
9) Disbursements of funds: When a customer takes money out of a customer account, the dates and specific amounts of funds taken out of the account. And on a disbursement, whether the money was disbursed by check or money wire, whether the money was sent to the customer or to a third party, to someone either in the U.S. or overseas.
10) Public company: whether the customer account is a senior officer, director, or large shareholder of a public company.
11) Politically exposed person: whether the customer account is politically exposed person (Heads of State or of government, senior politicians, judicial or military officials) either for a U.S. citizen or for a foreign country.

Having this type of information located in a central data base should sent chills through every U.S. citizen that believes they live in a democracy, and any international client or U.S. client who believes the sensitive data they entrusted to their investment firm remains private. Once all this information is in a central database, a customer should be very concerned if they:

(a) are successful in creating wealth,
(b) are part of a family that has accumulated wealth,
(c) become part of senior management of a public company,
(d) are a senior public official in one of our 50 States,
(e) are a member of Congress,
(f) are a senior official in the White House or any federal agency
(g) are a Head of State of any country,

(h) are a senior military official,
(i) are a member of the judiciary system, or
(j) may fit into any of these categories in future years.

Imagine the value of this information to their adversaries, knowing whether these types of citizens have liquidity or debt problems, investment concentrations in a particular industry sector, what their net worth is, the value of their securities holdings, what securities they are buying and selling, and if they make money on trading.

A central database like this brings together all this type of information in one place. To be very clear, once the CARDS system is breached to identify and capture all interesting investment activity from the numerous data fields, the bad guys simply take the specific account number and branch of the brokerage firm to begin the second breach, which is identifying the customer behind the account number. This is the clear and present danger of proceeding with CARDS.

Litigation against the securities industry and FINRA

What is missing in the CARDS proposal is the demonstration that FINRA will have adequate insurance coverage to cover both brokerage firm and customer litigation when data is breached. Once the clients find their trade data and client information have been breached, they will likely first sue their brokerage firm, and the brokerage firm will in turn have to sue FINRA for their data breach. My concern is this type of legal action would fall outside of the typical FINRA Arbitration panels, especially if FINRA is named in the complaints.

Beyond litigation costs, there is a much larger cost that is difficult to quantify. Upon the receipt of each customer complaint or lawsuit, the client relationship is then effectively over. This causes the brokerage firm to (a) lose a revenue source from their client, (b) face legal costs to defend against actions not of their own doing, and (c) face negative publicity that will impact their future. These types of costs cause much more harm than any possible benefit.

FINRA staff issues

Presumably there are many hardworking FINRA staffers who are proponents of CARDS, that do not truly understand the loss of customer privacy issues. Nobody will remember the few trades that were flagged, but everyone will remember the magnitude of the loss of customer data throughout the United States that CARDS presents. Their resumes and career paths will always be linked to CARDS. So when the data breaches occur, they inevitably will take the blame. And their careers will suffer greatly as the architects of this grand disaster.

Similarly, as the Board has been made aware of this issue, it would seem prudent that Board members will want to go down in history as having sided to protect customer privacy. And if the FINRA senior management does not now understand the dangerous implications that CARDS presents, then it simply is time for new leadership at FINRA.

Three other solutions

One solution was described in a front page article in the November 12, 2014 Wall Street Journal by Jean Eaglesham and Rob Barry, titled "In Spotting Troubled Brokers, Geography Matters". It appears the authors applied big data analytics to identify hot spots of troubled brokers. What is interesting is they used existing, publicly available information to identify geographic locations where troubled brokers congregate. If the Wall Street Journal can reach these conclusions without the existence of a CARDS system, then FINRA should be able to protect customers by identifying and closely monitoring troubled brokers by using existing regulatory information at their disposal.

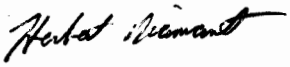
Another solution is to use human intelligence gathering within FINRA. Each regional office has capable staff and examiners who are familiar with brokerage firms in their district. I suspect they already know where the troubled brokers are located and could further focus their reviews on targeted areas. It would seem more beneficial to use the resources of existing FINRA regulatory staff, and encourage work already being done within the brokerage firm community to address such issues.

Yet another solution is to modify CARDS to forever remove the provision that mandates brokerage firms submit all their customer trades and information to one central database. This way the nationwide threat of the beaching of customer data would be mitigated. In this solution, FINRA would make CARDS a voluntary compliance tool for any brokerage firm which may need or simply desire an external data review of their trade activity. Should a FINRA on site audit raise a certain threshold of suspicious trades (perhaps 50 - 100 trades in a branch) then as part of their review, FINRA may require the specific brokerage firm to run their trades through CARDS for a period of time for further regulatory review. After a suitable time period where no trades harmed the customer, then the CARDS requirement on the brokerage firm would be terminated. In essence CARDS would become just another regulatory tool to test patterns of suspicious trades, or the activity of troubled brokers. In this solution, CARDS would be firm specific, not a nationwide system of data collection of customer information.

Conclusion

When reviewing CARDS, the small benefits of identifying some questionable trades pales when one considers the tremendous economic costs to implement, along with the destruction of customer privacy through data breaches. As there are other solutions available that improve the industry without setting up a "big brother" database of customer information, I again strongly urge the Board to act as both Statesmen and Leaders of our securities industry, and stop the implementation of CARDS.

Yours truly,



Herbert Diamant
President