



December 1, 2014

By Electronic Mail (pubcom@finra.org)

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

Re: Regulatory Notice 14-37 -- FINRA Requests Comment on a Rule Proposal to Implement the Comprehensive Automated Risk Data System

Dear Ms. Asquith:

The Securities Industry and Financial Markets Association (“SIFMA”)¹ appreciates the opportunity to provide comment on a proposed rule by the Financial Industry Regulatory Authority (“FINRA”) to implement the Comprehensive Automated Risk Data System (“CARDS”). FINRA initially released CARDS as a concept proposal in Regulatory Notice 13-42² and SIFMA filed two comment letters in response.³ SIFMA respectfully refers FINRA to those comment letters as they discuss significant concerns SIFMA believes remain with the proposed rule.

¹ SIFMA brings together the shared interests of hundreds of securities firms, banks and asset managers. SIFMA’s mission is to support a strong financial industry, investor opportunity, capital formation, job creation and economic growth, while building trust and confidence in the financial markets. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association. For more information, please visit www.sifma.org.

² Regulatory Notice 13-42, FINRA Requests Comment on a Concept Proposal to Develop the Comprehensive Automated Data Risk System (Feb. 28, 2014) [available at <http://www.finra.org/Industry/Regulation/Notices/2013/P412658>] (last visited Nov. 7, 2014) (hereinafter referred to as Regulatory Notice 13-42).

³ Comment Letter from Ira D. Hammerman, Exec. Vice President and Gen. Counsel, SIFMA, to Marcia E. Asquith, Office of the Corporate Secretary, FINRA (Mar. 21, 2014) [available at <http://www.sifma.org/issues/item.aspx?id=8589948105>] (last visited Nov. 7, 2014); Comment Letter from Ira D. Hammerman, Exec. Vice President and Gen. Counsel, SIFMA, to Marcia E. Asquith, Office of the Corporate Secretary, FINRA (July 1, 2014) [available at <http://www.sifma.org/issues/item.aspx?id=8589949729>] (last visited Nov. 7, 2014) (hereinafter referred to as the SIFMA March 21st Letter and the SIFMA July 1st Letter, respectively).

I. *Introduction*

SIFMA believes that FINRA's CARDS proposal would impose undue costs and burdens on the member firms, and is an attempt to diagnose a regulatory ill without appropriately accounting for the impact on investor privacy and civil liberties, and should not be filed with the Securities and Exchange Commission (the "Commission" or "SEC"). Most troubling is that CARDS would require the continued and regular disclosure to FINRA of the most intimate financial details for every investor's securities account, would be aggregated and stored on FINRA's computer system, thereby creating a centralized, prime target for computer hackers and nation state sponsored cyber terrorists.

A. *Statutory Authority Concerns*

As further discussed in this comment letter, SIFMA believes that FINRA lacks the statutory authority under Sections 3(f) and 15A of the Securities Exchange Act of 1934 ("Exchange Act") to issue CARDS as CARDS does not "promote efficiency, competition, and capital formation",⁴ and "impose[s] [a] burden on competition not necessary or appropriate in furtherance of the purposes of [the Exchange Act]."⁵

B. *Cost Concerns*

CARDS would require another new, expensive and standardized technology system to be built by the industry while the industry already produces mass quantities of data and reports to FINRA, the SEC and other self-regulatory organizations ("SROs") on a regular basis. SIFMA believes it would be more cost effective and a better way to account for the full range of investor considerations (such as regulatory oversight, cost effective services and protection of privacy and civil liberties) if FINRA worked with the vast amount of data it already receives through other systems.⁶ In addition, FINRA should consider leveraging the Consolidated Audit Trail ("CAT") system. CAT will track trading flows for all trading

⁴ Exchange Act § 3(f) (stating "[w]henever pursuant to this title the Commission is engaged in rulemaking, **or in the review of a rule of a self-regulatory organization**, and is required to consider or determine whether an action is necessary or appropriate in the public interest, the Commission shall also consider, in addition to the protection of investors, whether **the action will promote efficiency, competition, and capital formation.**") [emphasis added]. See generally *FINRA Framework Regarding FINRA's Approach to Economic Impact Assessment for Proposed Rulemaking (Sept. 2013)* at p. 3.

⁵ Exchange Act § 15A(b)(9).

⁶ Recent examples show that third parties are able to mine FINRA data to provide additional insights. For example, the Wall Street Journal recently reviewed CRD data to identify trends. See generally *How Troubled Brokers Cluster, Often Among Elderly Investors*, Wall Street Journal (Nov. 12, 2014). In other contexts, FINRA uses existing data streams to support proposed rules. For example, FINRA used TRACE data to support issuing proposed debt research rules. See, e.g., SR-2014-048 (proposed debt research rules). These examples indicate that FINRA does not need a completely new CARDS system to be an effective regulator.

activities. SIFMA believes it is more efficient and effective to consider what data fields could be added to CAT rather than mandate the development of CARDS. Reasonable alternatives should be fully identified, debated and discussed before moving to mandate the development of yet another new system.

C. *Privacy Concerns*

FINRA has an important mission of investor protection. The securities industry, which funds FINRA's mission, is firmly committed to promoting investor protection and supports the use of technology to further that mission. CARDS, however, would unnecessarily and inappropriately permit government oversight of all securities transactions of millions of American citizens (and non-U.S. nationals who maintain accounts in the U.S.).⁷ FINRA is proposing that a quasi-governmental entity should know the holdings, account balances and money movements of just about every brokerage account in the country. If allowed to be built, CARDS would deliver a dramatic intrusion into one's personal privacy and compromise one's civil liberties.

D. *Security Concerns*

FINRA's plan to collect and store account-level, detailed information places investors' sensitive financial transactional data at risk, even though FINRA does not plan to link that data to the actual investor's name, address or social security number. Recent press articles about hacking incidents indicate that cyber criminals are likely to discern value in the detailed information that FINRA would collect and store pursuant to the CARDS proposal. This risk should not be minimized or readily dismissed. Target, Neiman Marcus, and the U.S. Postal Service are just a few recent examples of this danger. The supposed benefits of the CARDS system are not sufficient to expose investors to this level of risk.

E. *Regulatory Paradigm Shift*

While SIFMA recognizes and supports FINRA's mission to protect investors, particularly from sales practice abuses, for over 75 years the responsibility for that protection was first and foremost on the broker-dealers to supervise and monitor the activities within their own firms, including the behavior and performance of the financial advisors at their respective firms. FINRA, in turn, has been responsible for monitoring the supervisory systems developed by member firms and the behavior of the registered personnel at the firms. CARDS would drastically change that paradigm

⁷ FINRA is a private actor that, by virtue of its registration as a national association under Section 15A of the Exchange Act and statutorily-recognized self-regulatory organization, is charged with performing important governmental functions such as enforcing the rules adopted under the Exchange Act.

and potentially position FINRA as the first level resource for regular supervision of activity at the individual account level.⁸

This approach is not feasible or effective, as FINRA does not have the same on-the-ground relationships with investors or knowledge of investor account-level details as does a firm or advisor. In addition, CARDS would overwhelm FINRA with superfluous data that may not be meaningful without the appropriate context. CARDS would provide FINRA with every trade, every account balance, and every money movement of every customer of a broker-dealer. That account level information and regular monitoring by a quasi-governmental organization such as FINRA might result in a dramatic departure from over 75 years of regulatory approach.

F. *CARDS Raises Too Many Issues*

FINRA has an important investor protection mission and deserves the tools it needs to fully deliver that mission. SIFMA believes that CARDS, as proposed, is not necessary for that mission, would unnecessarily encroach upon the public's rights of liberty and privacy, would be costly to build, implement and maintain, and at the end of the day would produce more "false positives" due to incomplete information that would drain resources, of both the regulators and the regulated, that could be put to better use to protect investors. Because of these reasons and others, as described in greater detail in the sections and appendixes of this comment letter, SIFMA does not support the proposed rule.

II. *EXECUTIVE SUMMARY*

In this section, SIFMA summarizes some of its general comments on the CARDS proposal. A detailed discussion of each of these issues is included in the various sections and appendixes of this comment letter. SIFMA also has included in this comment letter responses to the specific questions that FINRA raises in Regulatory Notice 14-37.

- **FINRA Lacks the Authority to Issue CARDS:** SIFMA believes that FINRA lacks the authority under Sections 3(f) and 15A of the Exchange Act to issue CARDS because CARDS does not "promote efficiency, competition, and

⁸ SIFMA questions whether FINRA needs CARDS in order to fulfill its regulatory mission. In a recent speech, the Director of the SEC's Division of Enforcement noted that the "[Division of Enforcement] sift[s] through non-public clearing firm data for problematic patterns in the sale and trading of certain asset-backed securities and other complex products. Through this process, [the Division of Enforcement is] deploying proprietary data analytics to identify troubling trends in the sale of complex financial instruments to retail investors that might serve as the basis of a suitability or failure-to-supervise case." See Andrew Ceresney, Director, SEC Division of Enforcement, *Remarks to the American Bar Association's Business Law Section Fall Meeting* (Nov. 21, 2014), [available at <http://www.sec.gov/News/Speech/Detail/Speech/1370543515297>] (last visited Dec. 1, 2014). The SEC's use of existing clearing firm data sounds very similar to how FINRA wants to use CARDS data.

capital formation”;⁹ instead, CARDS “impose[s] [a] burden on competition not necessary or appropriate in furtherance of the purposes of [the Exchange Act].”¹⁰

- **FINRA Must Conduct a Formal and Complete Cost-Benefit Analysis and Share it With its Members for Comment Prior to Submission of a Proposed Rule to the SEC:** FINRA has not conducted a formal and complete Cost-Benefit Analysis. It has conducted only an Interim Economic Impact Assessment. While it is difficult to determine actual costs and benefits related to the proposed rule on this information, as currently proposed the costs far outweigh the anticipated benefits. SIFMA retained IBM to prepare a Cost and Benefit Analysis White Paper addressing this issue. *See Appendix A.*
- **FINRA Has Not Addressed the Significant Privacy and Data Security Issues Raised by CARDS:** Although SIFMA has raised significant privacy and data security issues in its prior comment letters, FINRA has not responded to them. FINRA has concluded that the benefits of the rule outweigh the cyber security risks or that it believes there is no re-identification risk. SIFMA retained IBM to prepare a Re-Identification Risk White Paper that analyzes this issue. *See Appendix B.*
- **Scope of Data Collection:** The scope of data required to be produced by CARDS exceeds its stated objectives. At a minimum, information related to institutional accounts and self-directed retail accounts should be excluded since there is no demonstrable rationale stated by FINRA to collect such information (especially since FINRA already receives such transactional information through, among other systems, the Order Audit Trail System (“OATS”) and the Large Options Position Report (“LOPR”).
- **Clearing Firm Concerns:** FINRA should specifically address that a clearing firm is not responsible for oversight or supervision of information maintained and submitted to CARDS from introducing brokers if it uses the data for no other purpose.

⁹ Exchange Act § 3(f) (stating “[w]henever pursuant to this title the Commission is engaged in rulemaking, **or in the review of a rule of a self-regulatory organization**, and is required to consider or determine whether an action is necessary or appropriate in the public interest, the Commission shall also consider, in addition to the protection of investors, whether **the action will promote efficiency, competition, and capital formation.**”) [emphasis added]. *See generally FINRA Framework Regarding FINRA’s Approach to Economic Impact Assessment for Proposed Rulemaking (Sept. 2013) at p. 3.*

¹⁰ Exchange Act § 15A(b)(9).

III. *FINRA LACKS AUTHORITY UNDER THE EXCHANGE ACT TO ISSUE CARDS*

FINRA is authorized to issue rules under Section 15A of the Exchange Act.¹¹ That section of the Exchange Act limits FINRA’s rule making authority in various ways, including by specifying that FINRA’s rules “do not impose any burden on competition not necessary or appropriate in furtherance of the purposes of [the Exchange Act].”¹² FINRA has not met this statutory burden. FINRA has not established the statutory necessity for CARDS or that it otherwise fills a regulatory gap in FINRA’s current and extensive rulebook.

As stated in SIFMA’s current and prior comment letters, CARDS is duplicative of FINRA’s current reporting and regulatory requirements, is overly burdensome and likely to lead to higher and unjustified costs to member firms, and fails to account for current and future reporting regimes (such as CAT). CARDS, therefore, would be an unnecessary new regulatory reporting system that “impose[s] [a] burden on competition not necessary or appropriate in furtherance of the purposes of [the Exchange Act].” Significantly, the costs of the proposed CARDS system place an undue burden on competition with respect to issues that are already covered by other FINRA rules and regulations without providing any additional regulatory benefit.

In addition, Section 3(f) of the Exchange Act requires that FINRA’s rules “promote efficiency, competition, and capital formation.”¹³ As stated in SIFMA’s current and prior comment letters, CARDS does not meet this requirement because, among other things, CARDS is too costly, is duplicative of current reporting and regulatory requirements, would impose undue costs on member firms and investors that may result in a competitive advantage to alternative business models (e.g., Registered Investment Advisors), and would be highly inefficient.

¹¹ See Exchange Act § 15A. See generally *FINRA Framework Regarding FINRA’s Approach to Economic Impact Assessment for Proposed Rulemaking* (Sept. 2013) at p. 3.

¹² *Id.* at § 15A(b)(9).

¹³ See Exchange Act § 3(f). See generally *FINRA Framework Regarding FINRA’s Approach to Economic Impact Assessment for Proposed Rulemaking* (Sept. 2103) at p. 3.

IV. COSTS ASSOCIATED WITH CARDS

A. FINRA Must Conduct A Cost-Benefit Analysis And Share It With Member Firms Before A Proposed Rule Is Filed With The SEC

As stated in SIFMA's previous comment letters, FINRA must perform and publicly share a complete and final cost-benefit analysis of CARDS and provide time for the members to comment prior to any proposal being filed with the SEC. *Regulatory Notice 14-57* contains only a high-level "Interim Economic Impact Assessment." As previously requested, SIFMA believes that FINRA should (i) explain why it needs (as opposed to wants) CARDS, (ii) justify that the costs and burdens associated with CARDS are necessary and (iii) demonstrate that there are no other reasonable alternatives given existing FINRA, SEC and other SRO systems that meet FINRA's regulatory needs.

SIFMA believes an appropriate cost-benefit analysis not only must evaluate the individual project/rule, but also must be considered within the mosaic of the broader set of numerous regulatory initiatives impacting the financial services industry. Not only is CARDS a stand alone costly initiative, but it also unjustifiably adds to the cumulative effect of the numerous regulatory initiatives imposed on the industry over the last five plus years. Ultimately, these initiatives divert important firm resources from improving a firm's own surveillance capabilities and products and services available to customers. The industry has a finite amount of resources to dedicate for technology systems.

In SIFMA's experience, small to mid-size firms in particular will bear heavy costs associated with FINRA imposing additional required technological and personnel resources. SIFMA encourages FINRA to publicly share for comment its cost-benefit analysis, including the analysis and answers to the following issues:

1. Identifying and qualifying the problems, issues or practices that necessitate regulatory action;
2. The baseline against which to measure the likely economic consequences of the proposed regulatory action;
3. The reasonable alternative options available; and
4. The anticipated economic impacts associated with the options, including the costs and benefits and distributional impacts, in particular as to efficiency, competition and capital formation.

B. *Benefits Should Be Specifically Defined and CARDS Compliance Should Not Become Its Own Regulatory Program Similar to OATS*

There is no doubt that the development and maintenance of CARDS will involve substantial economic, technology and compliance resources. The anticipated benefits described by FINRA, however, are vague and more hopeful than expected. Moreover, CARDS could never achieve the ultimate benefits that FINRA is seeking as no system will ever be able to catch every violation of law or rule or even recognize every emerging trend.

Furthermore, SIFMA reasonably expects that the increased data provided to FINRA will likely lead to more requests from FINRA to member firms because of the number of “false positives” that will be generated due to incomplete information stored in the CARDS database. Thus, member firms will spend significant time and monies responding to requests that serve no regulatory purpose. Member firms will have to increase the number of personnel responsible to respond to FINRA for these unwarranted requests, and thus divert these same resources from its operations, surveillance and supervision systems. That would likely result in an increasing level of FINRA information and examination requests of its members.

CARDS is a very costly vehicle¹⁴ for collecting more information particularly when it appears that the information, as described by FINRA in its concept and proposed rule, would be used only to track transaction activity in specific investment products and assist FINRA’s suitability inquiries. FINRA needs to address with specificity that it is necessary to build a completely new system to gather information regarding product transaction activity. Wouldn’t it be less costly and more efficient to add a limited number of data input to CAT? Second, will the Risk Discovery and Analytics Tool (“RDAT”)¹⁵ be capable of using this newly acquired information immediately for regulatory purposes or does that technology and capability still need to be developed? It would be a substantial waste of resources to develop a system to collect information if FINRA is unprepared to immediately put it to regulatory use by incorporating it in existing surveillance and examination tools.

The only certain regulatory output of CARDS would be a new area of FINRA regulatory review involving industry-wide scrutiny and member firm examinations regarding the accuracy and timeliness of CARDS reporting. Based on our member firms’

¹⁴ SIFMA believes that CARDS related costs also should be considered in light of the extensive costs in time and money incurred by the industry in connection with Dodd-Frank related initiatives and other technology build outs. *See, e.g.*, Volcker Rule related systems, OATS, ACT, INSITE, TRACE, Large Trader Identification, Enhanced Blue Sheets, shortened settlement cycle, and the anticipated CAT system.

¹⁵ RDAT is a FINRA program that employs analytics against a large amount of customer account information collected for a limited number of firms in an examination context. *See generally* FINRA Regulatory Notice 14-37 at p. 16.

experience with OATS and LOPR, this would be an expensive and resource-draining program and likely result in FINRA sending “bills” in the form of monetary sanctions for minor violations of the CARDS rules. Moreover, these added costs far outweigh any potential savings anticipated by FINRA, which are supposed to come from eliminating intermittent and sometimes frequent and extensive information requests for the same information CARDS covers.

C. *Cost-Benefit White Paper*

SIFMA retained IBM to perform a detailed cost-benefit analysis of the CARDS proposal. The Cost-Benefit White Paper highlights, among other things, that IBM estimates that Phase 1 of CARDS will cost the industry \$680 million to build and \$360 million annually for ongoing maintenance. See *Appendix A* for a copy of the IBM Cost-Benefit White Paper.

V. *PRIVACY*

A. *The Public Views Privacy as a Broad Constellation of Rights*

A recent Pew Research Center survey reveals that most Americans feel they've lost control over how their personal information is collected and used.¹⁶ The Pew survey found, among other things:

Privacy evokes a constellation of concepts for Americans—some of them tied to traditional notions of civil liberties and some of them driven by concerns about the surveillance of digital communications and the coming era of “big data.” While Americans’ associations with the topic of privacy are varied, the majority of adults in a new survey by the Pew Research Center feel that their *privacy is being challenged along such core dimensions as the security of their personal information and their ability to retain confidentiality.*

When Americans are asked what comes to mind when they hear the word “privacy,” there are patterns to their answers. ***[T]hey give important weight to the idea that privacy applies to personal material—their space, their “stuff,” their solitude, and, importantly, their “rights.”*** [W]hen responses are grouped into themes, the largest block of answers ties to concepts of security, safety, and protection.

¹⁶ *Public Perceptions of Privacy and Security in the Post-Snowden Era*, Pew Research Report (Nov. 12, 2014) [available at <http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/>] (last visited Nov. 13, 2014).

For many others, notions of secrecy and keeping things “hidden” are top of mind when thinking about privacy.¹⁷ [emphasis added]

In both of the comment letters that SIFMA submitted in response to Regulatory Notice 13-42, SIFMA addressed the significant privacy concerns raised by the concept proposal. In its rule proposal, FINRA dismisses these concerns because (i) CARDS no longer requires the reporting of personally identifiable information (“PII”), and (ii) FINRA has adequate data security protections. As the above quote from the recent Pew survey on public perceptions of privacy indicates, Americans view privacy as a “constellation of concepts” that transcends PII.

B. Regulatory Convenience Cannot Outweigh Individual Privacy Rights

FINRA seems to argue that it is more convenient for FINRA to have access to a CARDS-type system.¹⁸ Convenience, however, is not a sufficient justification for impinging on individual privacy rights. In a recent decision, the U.S. Supreme Court firmly held that individual rights sometimes outweigh the convenience of government.

In *Riley v. California*, the U.S. Supreme Court extended federal constitutional privacy protections to the vast amounts of data that individuals store on hand-held devices. The justices rejected law-enforcement arguments that warrantless device searches were constitutional and crucial to combating crime. Chief Justice Roberts stated that the Supreme Court is aware of the trade-offs between privacy and security: “We cannot deny that our decision today will have an impact on the ability of law enforcement to combat crime. Cell phones have become important tools in facilitating coordination and communication among members of criminal enterprises, and can provide valuable incriminating information about dangerous criminals. Privacy comes at a cost.”¹⁹

The same analysis must be considered when a quasi-governmental organization, such as FINRA, collects, stores, and searches vast amounts of investor financial transactional information. Regulatory convenience should not out-weigh investor privacy rights. As the Supreme Court stated: “Privacy comes at a cost.”

¹⁷ *Id.* at p. 1 (Summary of Findings).

¹⁸ *See generally* FINRA Regulatory Notice 14-37.

¹⁹ *Riley v. California*, U.S. Supreme Court Slip Opinion 13-132, p. 25 (June 25, 2014) [available at http://www.supremecourt.gov/opinions/13pdf/13-132_819c.pdf] (last visited June 26, 2014).

C. *Data-Security*

As discussed in SIFMA's previous comment letters, CARDS, as currently proposed, would require firms to standardize, integrate and pool a number of different sensitive data types together into one master set, and then to transmit this data to a clearing firm, which will in turn transmit the data to FINRA. This creates no fewer than five opportunities for data breach (if one assumes the unlikely scenario that only one server is used for each transmission): data could be compromised at an introducing broker; in transmission from introducing to clearing; at the clearing firm; in transmission from clearing to FINRA; or, at FINRA itself. As such, further consideration must be given to the heightened measures necessary to safeguard this data given the tremendous value that master trading/customer files could present to a successful hacker.

FINRA also states that any risk of a security breach is outweighed by FINRA's ability to reduce fraudulent and abusive behavior. SIFMA, respectfully, disagrees. A data security breach is more than a remote possibility and that possibility is not outweighed by the vaguely described anticipated benefits of CARDS. Some cybersecurity experts believe that computer hackers pose a greater threat to national security than terrorists.²⁰

1. *SIFMA Has Expressed Significant Privacy Concerns and Asked FINRA to Respond to Important Questions Related to Data Security and Privacy.*

It is unclear to SIFMA how FINRA would guarantee the safeguarding of such sensitive information or which parties will be liable in the event of a breach, and whether FINRA will indemnify firms if the breach occurs at FINRA. In the SIFMA March 21st Letter, SIFMA asked FINRA to specifically address:

1. How the data would be protected, both in the various stages of transmission, as well as while maintained at FINRA;
2. Who would be responsible to customers and/or the markets when a breach occurs;
3. Whether FINRA is prepared to indemnify introducing brokers and clearing firms for the release of customer data by FINRA;
4. Whether customers would be permitted to opt out (*i.e.*, refuse to allow their information to be provided to FINRA via CARDS) and, if so, what logistics are required to facilitate an opt-out process;

²⁰ See generally *Feds Hacked: Is Cybersecurity a Bigger Threat than Terrorism?*, The Christian Science Monitor (Nov. 10, 2014) and *US Agencies Struggle vs. Cyberattacks*, Associated Press (Nov. 10, 2014).

5. What disclosures and/or protections would be offered to customers whose data is maintained by CARDS;
6. Who would have access to the information and how would such access be granted in the first instances, and how would access be supervised/re-evaluated on a going forward basis;
7. How long the information would be maintained;
8. Who else, apart from FINRA staff with a “need to know,” would have access to the data;
9. The identity of its systems’ administrators; its policies and procedures for the protection and use of the data; if it plans to use third-party vendors; and, the risk controls that would be used by the administrator;
10. How the costs of remediation of a data breach would be allocated if a breach occurs;
11. The applicability of state and federal data privacy laws to the data collected via CARDS, including an explanation as to whether FINRA, as a Delaware incorporated entity, is subject to state privacy laws directed at corporations;
12. How FINRA would respond to requests for information from private and/or public litigants, as FINRA would become a known repository of an inordinate amount of detailed, personal, financial information; and
13. Which entity (introducing broker, clearing firm, or FINRA) bears responsibility to notify individuals of a data breach, when one occurs?

2. *FINRA’s Rule Proposal Does Not Address These Concerns*

In response to SIFMA’s requests, FINRA stated only that:

1. The information will be encrypted in transmission and after receipt;
2. FINRA would limit access to the raw data to a few fulltime technical employees;
3. FINRA would apply the security controls and protocols it already has in place; and

4. Those controls and protocols are based on industry best practices, guided by federal and international standards and are compliant with data security and privacy laws and regulations.

FINRA's response to SIFMA's list of questions can be summarized as follows: it will continue to do what is already required by law of all organizations to ensure data security. As FINRA is aware, data breaches occur even when current data security standards are met.²¹ With that in mind, SIFMA finds it surprising that FINRA stated that "it believes that the investor protection benefits that would come from CARDS, and FINRA's increased ability to reduce fraudulent and abusive behavior, significantly outweigh the remote risk of a security breach."²²

In the SIFMA March 21st Letter SIFMA quoted Robert Mueller, then Director of the FBI, who stated, "I am convinced that there are only two types of companies: those that have been hacked and those that will be."²³ In fact in 2013 and 2014 alone, there has been public notice of cyber attacks on, among others, the White House, Nasdaq, the National Oceanic and Atmospheric Administration ("NOAA"), the United States Postal Service, Visa, Target, Neiman Marcus, 7-Eleven, Michaels, Yahoo! Mail, Aaron Brothers, AT&T, eBay, P.F. Chang's China Bistro, U.S. Investigations Services, Community Health Services, UPS, Home Depot, Google, Goodwill Industries International, SuperValu, and

²¹ Data breaches have become so common that Forbes magazine publishes a weekly article that catalogs that week's data breaches. See <http://www.forbes.com/sites/katevinton/2014/09/16/data-breach-bulletin-gmail-central-utah-clinic-jp-morgan-george-mason-university/?ss=Security> (last visited Nov. 13, 2014).

²² Regulatory Notice 14-37 at p. 6.

²³ Robert S. Muller, III, Director, Federal Bureau of Investigation, Speech at RSA Cyber Security Conference (Mar. 1, 2012).

Dairy Queen International.²⁴ Additionally, there were threats of cyber terrorism and corporate espionage from nation states such as China, Iran, and Russia.²⁵

SIFMA respectfully disagrees with FINRA's conclusions. SIFMA believes they distort reality and endanger the security of investors' most sensitive financial information for the hope of a more efficient regulatory protocol. Common sense demands that a security breach is not remote, but rather a breach is to be expected. Housing the entire investment community's securities transactional information in a single warehouse would create one of the most attractive targets for cyber criminals. One would anticipate efforts to breach FINRA's ordinary security protocols would be relentless. SIFMA believes that the likelihood of a security breach outweighs the vague, anticipated regulatory benefits FINRA expects to obtain or has yet to identify. Additionally, CARDS should not be considered for approval until FINRA responds to the important questions and concerns about data security in SIFMA's previous comment letters.

D. *Re-Identification Risk Associated with CARDS*

In its previous comment letters, SIFMA discussed its belief that there was a material risk of the re-identification of PII raised by CARDS. The ability, for example, to re-identify individual investors through the use of algorithms and/or linking of the CARDS database to other databases (such as CAT) raises significant privacy concerns even if

²⁴ See, e.g., *Post office breach: The new Cold War?*, USA Today (Nov. 11, 2014); *U.S. Weather System Hacked, Affecting Satellites*, CNN (Nov. 12, 2014); *More Well-Known U.S. Retailers Victims of Cyber Attacks*, Reuters (Jan. 12, 2014); *eBay Hack 'One of the Biggest Data Breaches in History'*, The Week (May 22, 2014); *Cyber Breaches Put 18.5 Million Californian's Data at Risk in 2013*, Yahoo! News (Oct. 28, 2014) (stating "[c]yber intrusions and other data breaches put the personal records of 18.5 million Californians, nearly half the state's population, at risk in 2013, a seven-fold increase over the year before, the state attorney general reported on Tuesday"); *IT Security Stories to Watch: Gmail and Home Depot Data Breaches*, MSPmentor (Sept. 15, 2014) (stating "[d]ata for 4.93 million Google accounts was leaked and published on a Russian-language Bitcoin security online forum"); *Nearly 5 Million Google Passwords Leaked on Russian Site*, Time (Sept. 10, 2014); *U.S. Postal Service Data Breach May Compromise Staff, Customer Details*, Reuters (Nov. 10, 2014). See also *Data Breach Statistics*, IBM Security Services 2014 Cyber Security Intelligence Index (April 2014) (stating there were 1.5 million monitored cyber attacks in the U.S. in 2013 and that "[d]ata breaches are among the most common and costly security failures in organizations of any size. In fact, studies show that companies are attacked an average of 16,856 times a year, and that many of those attacks result in a quantifiable data breach") [available at <http://www-935.ibm.com/services/us/en/it-services/security-services/data-breach/>] (last visited Nov. 12, 2014).

²⁵ See, e.g., *Chinese hackers suspected in major U.S. Postal Service breach*, Mashable (Nov. 11, 2014); *Cyber Experts Warn Iranian Hackers Becoming More Aggressive*, Reuters (May 13, 2014); and *Hackers Breach Some White House Computers*, Washington Post (Oct. 28, 2014) (stating "[h]ackers thought to be working for the Russian government breached the unclassified White House computer networks in recent weeks. . .). See also *Feds Hacked: Is Cybersecurity a Bigger Threat than Terrorism?*, The Christian Science Monitor (Nov. 10, 2014) (stating "[t]his year, hundreds of millions of private records have been exposed in an unprecedented number of cyberattacks on both US businesses and the federal government").

CARDS does not directly collect or store PII. Indeed, the linkage of personal information and the potential for collateral, downstream intrusions are legitimate threats.²⁶

FINRA would be a repository of vast amounts of sensitive data for which it has not and cannot guarantee absolute safeguarding. As noted by IBM in its Re-Identification Risk Study, “As one of the biggest consolidated repositories of nonpublic financial information, CARDS will continue to represent a high-value target for various classes of attackers. Even though CARDS itself cannot be used to effect financial transactions, it could still be used to facilitate fraud, cause serious damage to investors, and to undermine confidence in our financial markets.”²⁷

In its rule proposal, FINRA’s only response to SIFMA’s concern of the risk of re-identification is that it does not believe it could happen. We respectfully believe that before the largest single warehouse of personal financial information is created, FINRA be required to present more assurance against re-identification risk than only its belief it will not happen.

E. *Re-Identification Risk White Paper*

Attached as *Appendix B* is a Re-Identification Risk White Paper prepared by IBM that outlines the re-identification /reverse engineering risk associated with CARDS.

F. *Continued Concerns Regarding Civil Liberties*

As previously stated, CARDS raises significant civil liberties and related concerns.²⁸ Regardless if CARDS would directly collect or store PII, CARDS would be an NSA-like system for the mass surveillance of individual customer accounts.²⁹ One FINRA

²⁶ See, e.g., Comment Letter from the American Civil Liberties Union to Marcia E. Asquith, FINRA, *Regulatory Notice 13-42 - FINRA Requests Comment on a Concept Proposal to Develop the Comprehensive Automated Risk Data System* (Mar. 21, 2014) (stating “[R]esearch has demonstrated that even nominally de-identified information can frequently be re-identified when crossed [sic] referenced with other public databases. The danger seems particularly acute in the case of detailed financial information.”). See also Pew Research Report, *supra* note 12.

²⁷ See IBM Comprehensive Automated Risk Data System (CARDS) Re-Identification Risk Study (RRS) (Dec. 1, 2014) attached hereto as *Appendix B*.

²⁸ See generally SIFMA July 1st Letter at p. 6.

²⁹ CARDS is similar to reported NSA and DOJ programs that collect information on millions of Americans in order to find a single person or a handful of people. See, e.g., *Americans’ Cellphones Targeted in Secret U.S. Spy Program*, Wall Street Journal (Nov. 13, 2014) (stating that a new DOJ surveillance program “is the latest example of the extent to which the U.S. is training its surveillance lens inside the U.S. It is similar in approach to the [NSA]’s program to collect millions of Americans phone records, in that it scoops up large volumes of data in order to find a single person or a handful of people. . . . Christopher Soghoian, chief

official has orally described CARDS as a bird's eye, satellite view of financial activities/accounts that will complement the activities of the FINRA boots on the ground.³⁰ CARDS would enable FINRA to look into every investor's securities transactions through an extensive data collection, manipulation and storage system. This raises questions, in our view, about where to draw the line between the legitimate exercise of regulatory functions from the inappropriate intrusion on personal privacy/civil liberties. FINRA has not addressed these concerns.

VI. PROCESS CONCERNS

As stated above, we believe that prior to filing the proposed rule with the SEC, FINRA should respond to member firm comments and provide an opportunity for members to comment on a final cost/benefit analysis. That being said, SIFMA appreciates that FINRA is committed to review and comment and filing a proposed rule and any future changes to such rule, if adopted, with the SEC under Section 19(b)(4) of the Exchange Act.

SIFMA also reiterates that because Section 19 of the Exchange Act requires the SEC to act on SRO rule filings within very narrow timeframes, the SEC provides a relatively short 21-day comment period on SRO rule filings. SIFMA believes that FINRA should include in its initial Rule 19b-4 filing with the SEC a grant of additional time for the SEC to review the CARDS proposal. In addition, FINRA should indicate in its 19b-4 filing that FINRA believes the SEC should consider providing at least a 60-day comment period for the proposal. The significant and complex issues raised by the CARDS concept, including potential significant cost implications, privacy and civil liberties issues require more than a 21-day comment period so that interested parties can fully consider and comment on the proposal.

VII. SCOPE OF DATA COLLECTION

FINRA's discussion of the anticipated benefits of CARDS appears to focus on retail sales practice concerns. FINRA should address whether the reporting to CARDS of information regarding institutional account sales activity is necessary. If the anticipated use of information is to make suitability inquiries more efficient, SIFMA believes the reporting of institutional sales information would not be additive in any material way. SIFMA does not expect that institutional suitability concerns will be a likely outcome based on the transmission of institutional transactional account information via CARDS (information which already may be available through OATS, LOPR, and later CAT).

technologist at the [ACLU], called it "a dragnet surveillance program. It's inexcusable and it's likely—to the extent judges are authorizing it—[that] they have no idea of the scale of it.").

³⁰ Rick Ketchum, Chairman and Chief Executive Officer, Restoring Investor Trust in the Markets, FINRA Annual Conference Welcome Remarks (May 19, 2014).

SIFMA also believes that FINRA should specifically and more fully explain the need for each data category of information required by the rule.³¹ Tracking and identifying transaction activity to identify trends by investment product, firm and office would not require the extensive amount of information and data required by the rule as currently proposed. SIFMA believes that FINRA could obtain the same results by adding a small number of data categories to CAT. That would be a less costly and more efficient solution.

The proposal, for example, asks for information for all securities accounts. This includes clearance, depository, transfer and other non-customer accounts. This could nearly double the amount of information collected through CARDS. As stated above, SIFMA does not understand how such a broad net will help FINRA achieve its objective of identifying sales practice abuses. This is particularly a concern when one considers the overall costs associated with implementing and maintaining a CARDS reporting and response regime. At a minimum, SIFMA believes that FINRA should drop this aspect from the CARDS proposal or provide a justification as to how this information is core to its regulatory objective.

VIII. *CLEARING FIRM ISSUES*

SIFMA previously expressed its concern that it must be made clear, and not merely suggested, that clearing firms are simply conduits for passing required information from introducing brokers to CARDS and have absolutely no responsibility to review the information or to detect potential sales practice, suitability issues, and/or rule violations.

In *Regulatory Notice 14-37*, FINRA states that the allocation of responsibilities between an introducing firm and its clearing firm is governed by FINRA Rule 4311 and that rule is not changing. Firms can renegotiate their agreements but the introducing firm retains the obligation and responsibility for the timeliness and accuracy of CARDS reporting. FINRA also states if a third party is reporting to CARDS on behalf of an introducing firm, it will be required to maintain the information for three months but if it was simply passing the information on to CARDS and not otherwise using the information for customer review, the third party will not be held to any new supervisory or compliance obligations related to the information.

³¹ SIFMA also notes that various data elements required by CARDS might go beyond current legal/regulatory requirements. For example, CARDS requires the reporting of certain information on Politically Exposed Persons (PEPs) that goes beyond the current regulatory requirements issued by FinCEN. See *Regulatory Notice 14-37* at p. 9 and fnt 8. The only regulation requiring a determination of political status is the regulation requiring [Due diligence programs for private banking accounts \(31 CFR §1010.620\)](#), and that regulation requires firms to ascertain whether any of the identified persons thereunder is a “senior foreign political figure,” a term that differs from the PEP definition referenced by FINRA in the CARDS proposal. If the Bank Secrecy Act and related regulations do not require ascertaining individuals’ status as PEPs (as defined in the CARDS proposal), FINRA should not require the reporting of this information under the proposal. In addition, in the CARDS suitability data fields, FINRA has proposed fields that do not appear to be required under the requirements of SEC Rule 17a-3. See 17 C.F.R. § 240.17a-3(a)(17)(i)(A) (2014) (investment time horizon and risk tolerance).

While these statements are helpful, FINRA also states that “a firm’s compliance and supervisory programs would remain responsible for oversight to prevent and detect problems based on the full information the firm holds.” FINRA should clarify that despite having to hold CARDS data for three months, a clearing firm would not be held to any new supervisory or compliance obligations related to the information contained in the transmission to CARDS.

IX. RESPONSES TO SPECIFIC QUESTIONS

In this section of SIFMA’s comment letter, SIFMA provides responses to the individual questions that FINRA raised in Regulatory Notice 14-37. The below responses should be read in conjunction with the overall comments provided in the other sections of this comment letter and the SIFMA March 21st Letter and SIFMA July 1st Letter.

1. *In proposing the rule to implement CARDS, FINRA has sought to incorporate the feedback received since issuing the concept proposal, discuss the details of its examination and surveillance objectives, and explain how the CARDS initiative and rule proposal strive to obtain data to achieve those objectives in a direct and efficient manner. FINRA welcomes comments on other approaches to achieve the CARDS objectives that would be similarly or more effective.*

As discussed above, FINRA has not yet completed a formal cost/benefit analysis and has not demonstrated an absolute need for CARDS. FINRA’s stated uses for the information once received do not justify the creation of a complicated and expensive system in addition to its existing systems and the future CAT system. FINRA instead should thoroughly explore adding data elements to CAT and accessing other data sources such as MIDAS, OATS and INSITE before committing to CARDS.

Another alternative for FINRA would be to combine existing near real-time data analysis of NSCC to identify potential market integrity issues with FINRA data from existing SSOI reporting that identifies areas of higher risk firm activity. After identifying matters that would require further review, FINRA could request precise information from specific firms in a standardized format.

2. *In addition to the economic impacts identified in the Interim Economic Impact Assessment, are there other significant sources of economic impacts associated with CARDS, including anticipated costs and benefits, to carrying or clearing firms, or introducing firms? What are these economic impacts and what factors or firm characteristics contribute to these impacts? What would be the magnitude of costs associated with developing, implementing and maintaining the systems and procedures to submit CARDS information under the proposed*

rule? What factors or business attributes contribute to the costs associated with the proposal, such as size of the firm or differences in business model?

SIFMA respectfully directs FINRA to the Cost and Benefit Analysis Report attached as Appendix A to this letter. The Report concludes that the costs of CARDS, as currently proposed, far outweigh its anticipated benefits. *See Appendix A.*

3. To what extent do fully-disclosed introducing firms anticipate using a third party to report the Select Account Profile Data Elements under phase 2? What would be the sources and magnitude of costs to introducing firms associated with providing these data elements to FINRA through a third party? What would be the costs associated with providing these data elements directly to FINRA? Do introducing firms currently store these data elements in standardized electronic form in their systems? If not, how costly would it be for introducing firms to standardize the required data in order to transmit it to FINRA directly or through a third party?

Service providers are exploring CARDS reporting solutions, but have not formalized or committed to building such solutions so it is not yet possible to determine the magnitude of costs to introducing firms. However, in light of the fact that introducing firms will have to develop technical capabilities to comply with the proposed rule, as they are currently not required to maintain data in the form required to report pursuant to CARDS, there is no doubt that Phase 2 of CARDS will significantly impact and challenge many introducing brokers.

4. To what extent do carrying or clearing firms anticipate using a third party to report CARDS information under phase 1? What would be the sources and magnitude of costs to these carrying or clearing firms associated with providing the required information to FINRA through a third party? To what extent do clearing firms anticipate transmitting the Select Account Profile Data Elements on behalf of their introducing firms in phase 2? What would be the sources and magnitude of costs to clearing firms associated with transmitting these data elements on behalf of introducing firms?

See the Cost and Benefit Analysis attached hereto as *Appendix A.*

5. What are the costs incurred by firms today in responding to FINRA sweeps and other initiatives designed to address emerging risks to investors? What are the sources of these costs? What factors or business attributes contribute to the costs?

See the Cost and Benefit Analysis attached hereto as *Appendix A.*

6. What economic impact, including costs and benefits would accrue to the investing public by this proposal? How do investors evaluate enhanced investor protection? What would be the magnitude and primary sources of costs associated with the proposed rule to investors? What factors or attributes would contribute to the costs borne by different segments of the public associated with the proposal?

See the Cost and Benefit Analysis attached hereto as *Appendix A*.

7. The rule proposal would require the submission to FINRA of customer and noncustomer account numbers. Should FINRA allow firms to submit unique identifiers rather than account numbers? What would be the costs and benefits of allowing firms to submit unique identifiers rather than account numbers?

This question ignores the fundamental privacy and data security concerns SIFMA has raised regarding CARDS as currently proposed. Reporting an account number or a separate unique identifier (a more expensive proposition) both include intelligence that would be useful in re-identifying an account to cybercriminals.

8. Should FINRA consider an exception to the reporting requirements for firms that do not engage in any retail activity? Should FINRA consider an exception to the reporting requirements for firms that engage in limited retail activity? If so, what threshold should FINRA consider for limited retail activity and what is the basis for such threshold? What are the costs and benefits for any proposed threshold associated with limited retail activity?

As discussed above, should the proposed rule be submitted to the SEC, firms that engage in limited retail activity should be excepted from the CARDS requirements. Similarly, other reporting firms should be excepted from reporting required data regarding institutional sales activity. The rule appears to be focused on retail sales activity and suitability issues. Since institutional accounts are excepted from providing certain suitability related information, data production should be limited to retail account activity only and exclude self-directed retail account activity.

9. The rule proposal would require the transmission of information regarding money movements. What would be the costs and benefits of requiring firms to regularly transmit information relating to money movements?

We are uncertain why such information would be necessary for the stated purposes of CARDS. More importantly, this is another data feed that significantly increases the re-identification and reverse engineering risk resulting from CARDS. See *Appendix B*.

10. *FINRA intends to retire INSITE and AEP as firms start submitting the information as part of CARDS. What would be the costs to firms associated with retiring their existing AEP and INSITE systems? What would be the magnitude of annual cost savings and the factors that contribute to these cost savings? Are there other collections of data that FINRA should consider retiring upon successful implementation of CARDS? What are those systems, and what would be the anticipated costs savings associated with retiring those systems?*

The retirement of INSITE and AEP will save minimal costs. While we support the retirement of redundant and outdated systems, we believe the focus should be on whether necessary data resides within or can be added to existing or already proposed systems like CAT. Adding specific data elements to CAT would result in significant cost savings.

11. *FINRA plans to provide feedback to firms based on FINRA's analyses of CARDS information. Further, FINRA plans to provide firms with access to their own data in a way that would facilitate their use as part of their compliance efforts. What information would be most beneficial to firms in meeting their compliance and supervisory obligations? What benefits might arise from sharing relevant data and analyses with firms?*

It is a difficult question to determine the benefits of sharing relevant data with firms without knowing the specific data that will be shared. It would be more useful for firms to have access to the analytics tools so that firms could conduct their own surveillance and analysis and craft their own oversight. In fact, FINRA's analysis of anticipated benefits of CARDS is more of a discussion of its first productive experience with its RDAT, not CARDS.

A concern is that FINRA has used the provision of data to members as a weapon instead of a tool. FINRA now investigates a member firm's use of the provided data and determines whether they properly use and react to the data provided. FINRA questions whether firms have analyzed the data and come to the same conclusions as FINRA and acted accordingly. It is difficult to meet these exacting standards without the same data and analytics used by FINRA.

12. *Some commenters have asserted that carrying or clearing firms would pass all costs associated with the proposal onto introducing firms. Other commenters have asserted that all the costs would ultimately be borne by investors. Is there sufficient competition among carrying or clearing firms to limit their ability to pass on costs? Is there sufficient competition among introducing firms to limit their ability to pass on costs? What evidence supports these comments?*

See Cost and Benefit Analysis attached hereto as *Appendix A*.

13. *FINRA contemplates that the collection of information to be required by this proposal would enhance efficiency in other programs. In what other ways could FINRA use the information contemplated in this proposal to better protect investors and enhance market integrity? What would be the value of using the information collected in those ways?*

SIFMA believes that FINRA should initially focus on the important core issues raised in this and other comment letters before considering tertiary issues such as those raised by Question 13. SIFMA encourages FINRA to focus on the fundamental principles underlying the CARDS proposal and the legal and operational issues raised by the proposal described in Regulatory Notice 14-37.

14. *Do carrying or clearing firms believe that nine months following SEC approval of CARDS requirements would be a reasonable time period within which to start submitting CARDS information to FINRA under phase 1? Do fully-disclosed introducing firms believe that within 15 months of SEC approval of CARDS requirements would be a reasonable time period within which to start submitting CARDS information to FINRA under phase 2?*

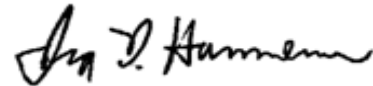
A more realistic time frame would be at least 24 months after SEC approval of the CARDS proposal for Phase 1. This would allow firms to define all the sources, create the necessary feeds and build operational controls to implement CARDS. An appropriate time for the implementation of Phase 2 is difficult to determine without greater granularity on what FINRA anticipates during Phase 2 (or shortly after Phase 2). At this point, SIFMA believes the industry needs more information on Phase 2 before SIFMA can determine an appropriate implementation timeframe.

X. CONCLUSION

SIFMA thanks FINRA for the opportunity to comment on the CARDS rule proposal. We look forward to a continuing dialogue and working together to an appropriate resolution.

If you have any questions or require further information, please contact Kevin Zambrowicz, Associate General Counsel & Managing Director, SIFMA at (202) 962-7386 (kzambrowicz@sifma.org) or our outside counsel, from Sidley Austin, Michael Wolk at (202) 736-8807 (mwolk@sidley.com) or Timothy Nagy at (202) 736-8054 (tnagy@sidley.com).

Very truly yours,



Ira D. Hammerman
Executive Vice President and
General Counsel

Cc: Richard Ketchum, Chairman & Chief Executive Office, FINRA
Susan Axelrod, Executive Vice President, Regulatory Operations, FINRA
Robert Colby, Chief Legal Officer, FINRA
Steven Joachim, Executive Vice President, Transparency Services, FINRA
Jonathan Sokobin, Senior Vice President, Office of the Chief Economist, FINRA

Stephen Luparello, Director, Division of Trading and Markets, SEC
David Shillman, Associate Director, Division of Trading and Markets, SEC

Michael Wolk, Sidley Austin LLP
Timothy Nagy, Sidley Austin LLP

Appendix A

COMPREHENSIVE AUTOMATED RISK DATA SYSTEM (CARDS) Cost Analysis (CA)

December 1, 2014



This white paper analyzes the costs to the Industry and FINRA of Phase 1 of its currently proposed Comprehensive Automated Risk Data System (CARDS) program. It examines the CARDS build and ongoing technology, staff, and outsourcing costs to impacted broker dealer communities. We estimate that total cost to Industry for the some 200 Clearing and Carrying Brokers that fall within Phase 1 of this regime will be approximately \$680M to build, with \$360M required for labor, infrastructure, and storage to maintain the reporting regime annually. FINRA has previously estimated its own costs to develop CARDS to be between \$8M and \$12M over a three year period. We further note that given the average record volumes captured in our survey, costs to store this data alone could approach \$50M annually.

Table of Contents

Contributors	3
Introduction.....	3
Methodology	5
Scope of Model	5
Approach.....	5
Descriptive Statistics.....	6
Survey Results	10
Build cost	10
Run cost	10
Average, Small, and Large Firm Estimates	11
Total Industry Cost	15
Additional technology costs to FINRA.....	16
Other costs	16
Duplication with CAT.....	16
Duplication with AEP and INSITE.....	17
Increase in regulatory inquiry	17
Additional obligations for clearing firms.....	18
Conclusion	18

Contributors

Robert W Johnston, Business Intelligence, IBM Global Business Services

Robert James Stanich, Financial Markets Strategy, IBM Global Business Services

Geoff Burkholder, Business Analytics & Optimization, IBM Global Technology Services

Mary Cosgrove, Business Transformation, IBM Global Business Services

IBM was engaged as a consultant by SIFMA to complete this analysis. All estimates are for planning purposes and are not an offer of services by IBM.

Introduction

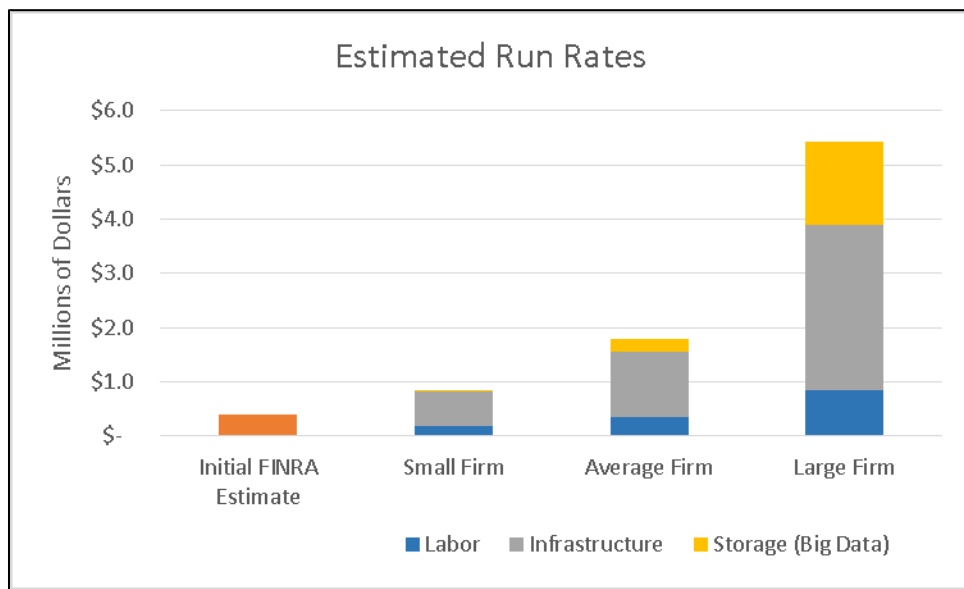
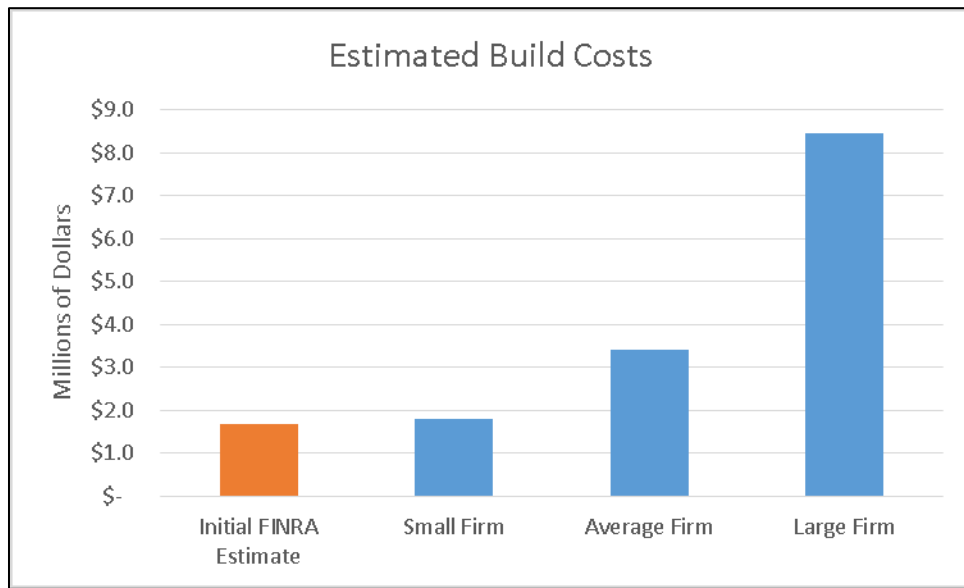
This whitepaper is aimed both at the general reader in the investing public as well as financial market participants and their regulators. Our goal is to help all parties understand the costs to build and operate FINRA's proposed CARDS system. As such, we will not assume the reader is familiar with all of the terminology used here, and will attempt to introduce concepts as we proceed.

FINRA describes its proposed Comprehensive Automated Risk Data System (CARDS) as "a rule-based program that would allow FINRA to collect on a standardized, automated and regular basis, account information, as well as account activity and security identification information that a firm maintains as part of its books and records."¹ Essentially, it moves FINRA from more of an exam-based means of gathering information from financial firms towards a model where every investor's data automatically flows to FINRA for surveillance.

A prior estimate, provided by a pilot group of firms at FINRA's request, estimated a median cost to build CARDS to be approximately \$1.68 M, with an additional \$400k required to operate the CARDS regulatory reporting system on an annual basis.² Our survey and analysis, based on data provided by 16 firms, large and small, administered by IBM through an anonymous survey using its proprietary Business Intelligence Estimating Model, concluded that the mean cost for firms to implement CARDS is \$3.4M, and an annual cost of \$1.8M to run and maintain their CARDS regulatory reporting system. The run rate cost of \$1.8M is comprised of \$340k for labor costs, \$1.2M for infrastructure costs, and \$230k for storage costs under a "big data" model. Using traditional disk storage methods, the run rate would be substantially higher.

¹ <http://www.finra.org/Industry/Regulation/Notices/2013/P412658>.

² *Ibid*



FINRA has previously estimated its own costs to develop CARDS to be between \$8M and \$12M over a three year period. We calculated a separate annual data storage cost based on the average record volumes of firms in our survey and determined that the cost for FINRA to store this data alone could approach \$50M annually, depending on the level of service required.

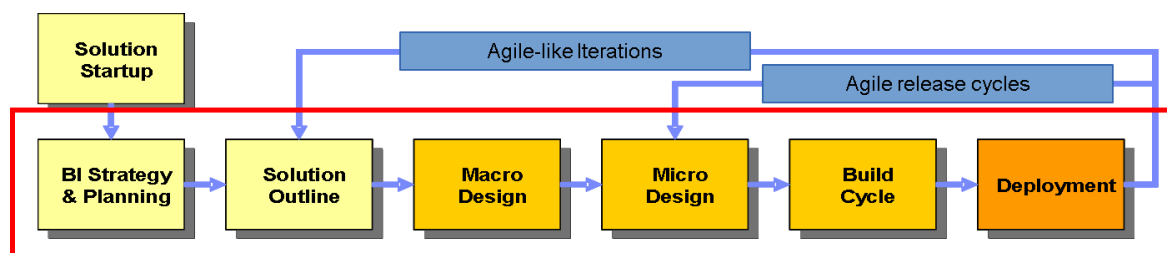
We estimate that total cost to the firms in the industry to build CARDS Phase 1, holding up the median firm and FINRA's estimate that 200 Clearing and Carrying Brokers that fall within this regime, will be approximately \$680M, with an additional \$360M required to operate these systems on an annual basis. The costs of Phase 2, would extend CARDS reporting to thousands of introducing brokers and has not been estimated as part of this exercise. Phase 2 would represent significant additional costs over and above what is estimated in this paper. Phase 2 also

adds the complexity of standardizing and capturing suitability data not currently held in easily normalized data formats (account information held in paper form).

Methodology

Our estimating approach utilizes IBM's proprietary *Business Intelligence Estimating Model 5.0* (BI Estimating Model), part of its *Business Intelligence Method* (BI Method), to derive estimates for participating firms and extrapolate total cost for clearing and carrying brokers. The model is an accepted and broadly utilized IBM standard model for estimating data acquisition and integration projects. IBM has tested and refined the model over hundreds of financial services projects, and the model serves as the basis of IBM's commercial commitments in this line of service.

The BI Method Estimating Model is supported with continuous improvement through calibration with real-world empirical project metrics providing feedback into the model. The model is used by IBM to estimate the level of effort in a time dimension for every phase of the BI Method from *Solution Outline* through *Deployment*.



Scope of Model

The scope of the BI Estimating Model is inclusive of project management, architecture and business analysis, creation of data repositories, data integration, testing, and reporting and analytics.

The estimate generated by the model includes the costs to build, deploy, and operate clearing and carrying firms' CARDS program, an analysis of firms by size, and an overall cost to the financial industry to implement and maintain CARDS from a technology perspective.

Key features of the model include engagement data inputs to over 100+ questions, determination of the complexity by discipline of the reference architecture, calculation of estimates by discipline and by phase of the reference architecture (e.g., Data Integration estimation in hours during Solution Outline, Macro Design, Micro Design, Build, Test, Deploy), and auto-generation of assumptions based on data inputs.

Approach

To gather the necessary inputs to our model from participating firms, IBM created a survey for SIFMA members, which SIFMA distributed. Firms completed the surveys and returned them to

SIFMA, where staff anonymized SIFMA member responses before submitting the results to IBM for input into its BI Estimating Model.

For each of the 21 record types being requested by FINRA under CARDS as specified in their Draft Data Dictionary and Record Layout, we requested certain data points from each firm on how they would fulfill each requirement. The survey included questions, such as the following:

- the number of source systems in which data required to fulfill the record type is stored, across lines of business or by product, as well the underlying technology platform of the systems where the data resides;
- the number of tables in which the data resides;
- the number of transformations necessary to provide each data point in the records; and
- the total volume of transactions anticipated for each record type by that firm.

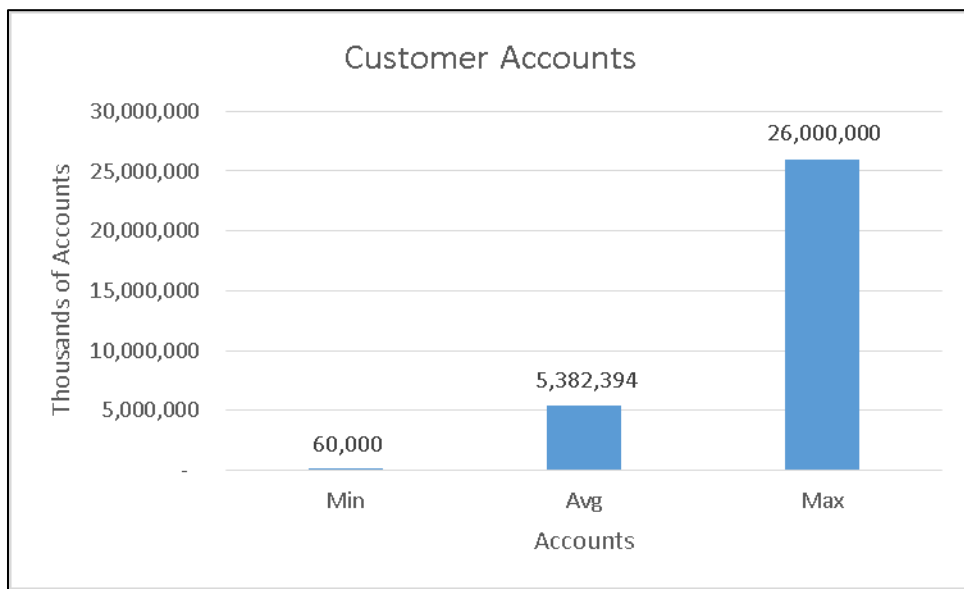
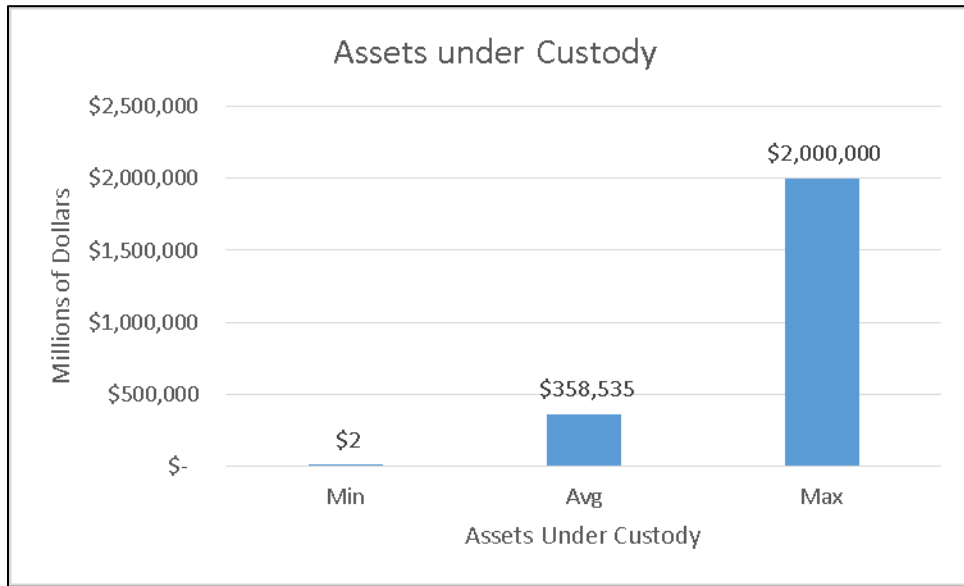
Firms were then asked to provide some basic data about the nature of their lines of business, number of accounts, product volumes, assets under custody (AUC), and expenditures. Finally, firms were polled on a series of other questions around the costs and benefits they anticipate from CARDS, the results of which are outlined in this paper.

The BI Estimating Model was then used to generate a cost for each of the data attributes to be reported and transmitted to FINRA.

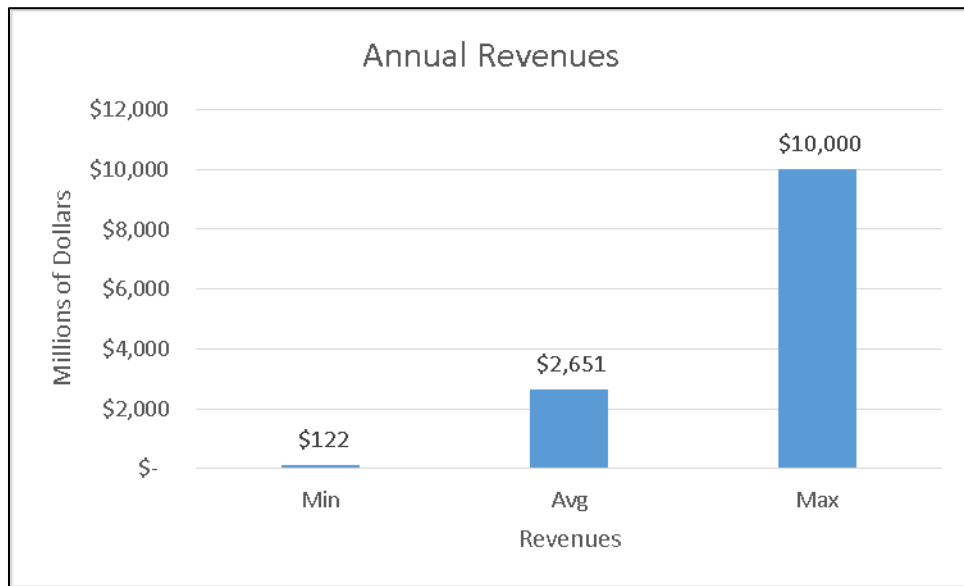
Descriptive Statistics

Sixteen firms participated directly in the survey and the BI estimating model generated results for each firm. A seventeenth firm provided its own estimate outside the survey. This firm's estimate is incorporated into the average cost calculation but is not reflected in the following descriptive statistics.

Our survey includes both large and small firms. Firms in our survey range from \$2M to \$2T AUC with a mean of \$360B AUC, and with accounts on their books between 60k and 25M.



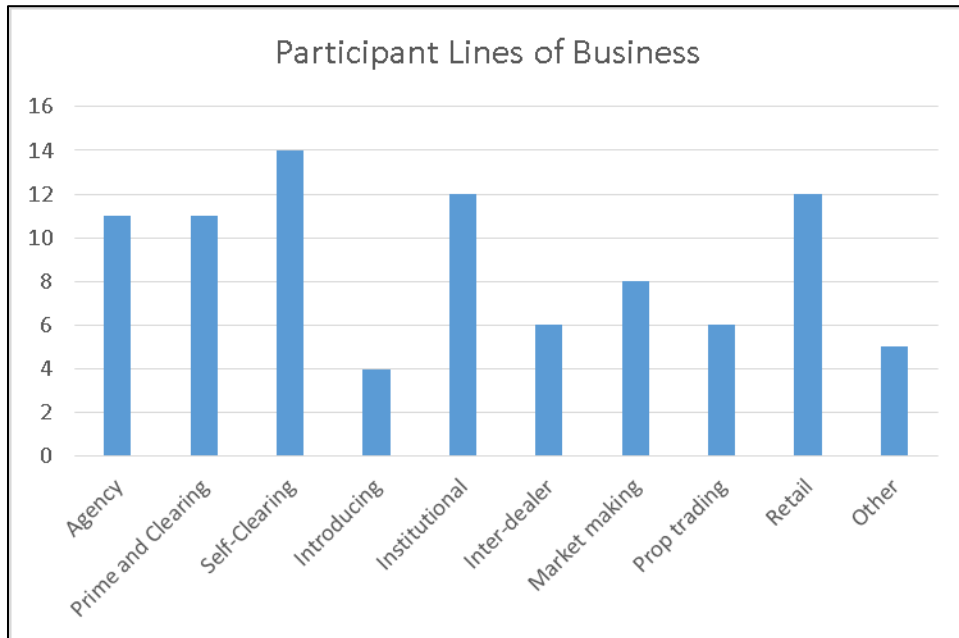
The range of Security Master Records for firms surveyed is between 21k and approximately 5M with an average of 1.5M records. Annual revenues for firms in the sample are between \$120M and \$10B+ annually.



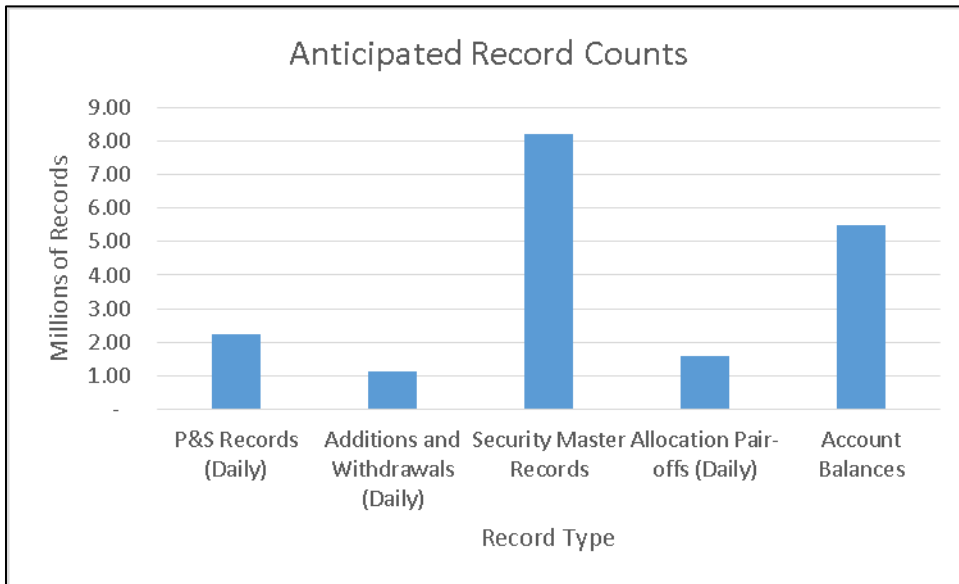
The range of expenditures for securities operations of surveyed firms is between \$240k and \$70M with an average expenditure of \$26M. We also found that Information technology expenditures supporting these businesses range between \$230k and \$200M annually with a mean estimate of \$35M.³

Participants in the survey represent a broad spectrum of financial markets participants. The respondents collectively are engaged in the following businesses agency brokerage, prime brokerage and correspondent clearing, self-clearing, introducing brokerage, institutional trading, inter-dealer market participants, market makers in one or more securities, proprietary trading, retail brokerage, firms with other lines of business would fall under the CARDS requirements. Many of the respondents engage in multiple lines of business.

³ All numbers are approximate.



Looking at just a few of the twenty one record types, together these sixteen firms would expect to create on any given day 31M Purchase and Sales records (2M average), 15.5M Account Addition and Withdrawal records (1M average), 17.5M Allocation Pair-off Detail records (1.5M average), and 71M Securities Account Balances (5.5M average).



Survey Results

Build cost

As noted in FINRA's Regulatory Notice 14-37, estimated build costs for a group of firms participating in an early pilot of CARDS ranged from \$390K to \$8.33M with a median build cost of \$1.68M. Our estimate for the mean build cost for firms to implement CARDS is \$3.4M.

The difference in FINRA's estimate may be due to the scope of the survey and may not have included everything IBM typically estimates when undertaking projects of this nature. Anecdotally, we've received feedback that FINRA's survey was conducted at a time prior to the publication of a standard record layout, that participants in the pilot were providing their files in their own internal formats and may have assumed they would continue to, and that non-retail business was thought by some to be excluded. According to one participant, estimates were provided on a "best guess" basis, without much clarity as to what was in or out of the estimate.

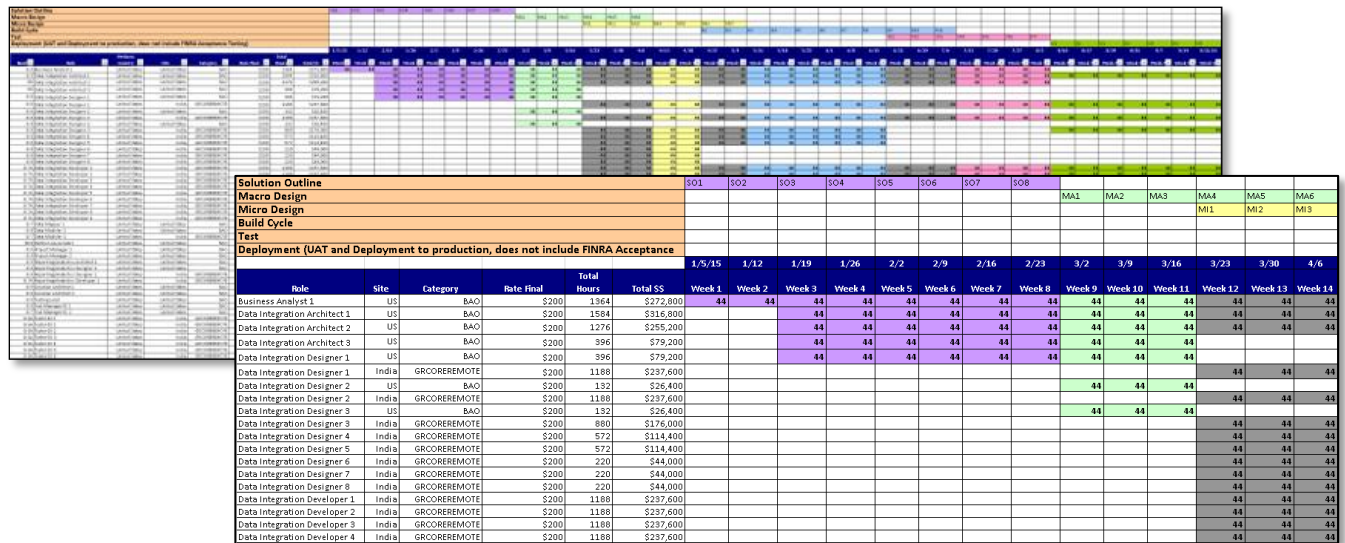
Particularly for small firms, implementation of such programs will typically fall to a small number of employees, and accounting for their efforts on CARDS may not adequately capture the opportunity cost of other projects they will not be undertaking while they focus on CARDS. An advantage of using a third-party estimating model is that it will naturally reflect a program's total cost.

Run cost

As noted in FINRA's Regulatory Notice 14-37, FINRA estimated that participant's ongoing operating costs to comply with CARDS requirements are \$400k with different firms predicting annual costs between \$76k and \$2.44M.⁴ Our own ongoing operating cost estimate is driven directly out of our BI Estimating Model, which showed a mean ongoing operating cost value of \$1.8M. The \$1.8M ongoing operating cost includes the following costs: \$340k for labor to run and maintain the system, error repair and retransmission, and participation in mandatory testing; \$1.2M in hardware and software costs; and \$230K in storage costs under a "big data" model. When using traditional disk storage methods, the data storage estimated cost could be as high as \$2.4M per year.

⁴ <http://www.finra.org/Industry/Regulation/Notices/2013/P412658>.

Sample Medium-firm Project Plan for CARDS under the IBM's BI Method



Average, Small, and Large Firm Estimates

In this section we will examine the cost impact of CARDS upon an average firm, a small firm, and a large firm.

The midpoint of hours required by the average firm to design, build, and deploy CARDS is 16,997 hours. Using an average labor rate of \$200 per hour, the cost of this effort is \$3.4M. The midpoint of hours required by the average firm to run and maintain CARDS is 3,399 hours and at an average rate of \$100 per hour, the run and maintenance costs are \$340k. When factoring in \$1.2M in infrastructure costs and approximately \$230k for storage of CARDS data in a “big data” repository, the total annual expense for an average firm is \$1.8M.

Hourly rates reflect a mix of fully-costed labor, which includes senior and junior staff, and on and off-shore personnel. We assumed a mix of 45% local (US-based) and 55% offshore labor in these models.

One may adjust the rates and mix of labor to arrive at different estimates, however we provide our assumptions for transparency and our estimates are aligned with rates used by the US Securities and Exchange Commission in cost estimates for the Consolidated Audit Trail with hourly labor costs ranging anywhere from \$198 to \$400/hour for local resources.⁵

The estimate includes the design, building, testing, and deployment of this firm’s CARDS technology platform, which will include 1,500 rationalized source system attributes to account for 196 unique target attributes (redundancy has been accounted for) in the 21 required FINRA Record Types. Our BI Estimating Model shows a cost distribution for this effort of roughly 23%

⁵ <http://www.sec.gov/rules/proposed/2010/34-62174fr.pdf> (32596).

for design, 45% for build, and 32% for testing, absent any separate testing that FINRA may mandate.

Average Firm Cost Estimate assuming medium complexity environment				
Design/Build Deploy	Estimator	Low (-25%)	High (+10%)	Mid-Point
Hours	18,375	13,781	20,213	16,997
Average Rate	\$200	\$200	\$200	\$200
Total Cost	\$3,675,000	\$2,756,250	\$4,042,500	\$3,399,375
Run/Maintain				
Hours	3,675	2,756	4,043	3,399
Average Rate	\$100	\$100	\$100	\$100
Labor	\$367,500	\$275,625	\$404,250	\$339,938
Infrastructure				
Less Disk Storage	\$1,286,250	\$964,688	\$1,414,875	\$1,221,938
Traditional Disk	\$2,496,000	\$1,872,000	\$2,745,600	\$2,371,200
<i>Big Data</i>	<i>\$249,600</i>	<i>\$187,200</i>	<i>\$274,560</i>	<i>\$230,880</i>

Average Firm Estimate Drivers - Design/Build/Deploy (DBD)		
Rationalized Source Attributes	1,313	<i>Number of Source Attributes to populate the Target Attributes X the Target Attributes</i>
Unique Target Attributes	196	<i>Unique attributes out of the 399 listed in the Record Type definitions</i>
FINRA Record Types	21	<i>Per FINRA data definition document</i>
Effort hours per Source Attribute	20	<i>Based on detailed bottom-up estimate using IBM estimating techniques</i>
Source Data Redundancy Factor	30%	
Calculated Source Data Attribute Count	1,875	
DBD Cost Distribution		
Design	23%	
Build	45%	
Test	24%	<i>Note testing does not include FINRA mandated testing</i>
By Role		
Business Requirements	4%	
Architecture	18%	
Data Modeling	3%	
Data Mapping	3%	
Data Integration	36%	
Reporting and Analytics	7%	
Testing	24%	<i>Note total testing hours are allocated across testing roles and design/development roles</i>
Project Management	5%	
DBD Resource Distribution		
Local	45%	
Off shore	55%	

Average Firm Estimate Drivers - Run/Maintain		
Effort Basis	20%	
Infrastructure Factor	30%	

Small Firms Estimate

The midpoint of hours required by small firms to design, build, and deploy CARDS is estimated at 9,038 hours, or \$1.8M. The midpoint of hours required by this firm to run and maintain CARDS is 1,808 hours, or \$181k. Total annual expenses for this small firm will run an average \$841k, factoring in \$650k in infrastructure costs (ex-storage) and approximately \$11k for storage of its CARDS data in a “big data” repository. Small firms, however, are much more likely to utilize traditional disk storage, so data storage costs could be as high as \$114k.

Small Firm Cost Estimate assuming low complexity environment				
Design/Build Deploy (DBD)	Estimator	Low (-25%)	High (+10%)	Mid-Point
Hours	9,771	7,328	10,748	9,038
Average Rate	\$200	\$200	\$200	\$200
Total Cost	\$1,954,260	\$1,465,695	\$2,149,686	\$1,807,691
Run/Maintain				
Hours	1,954	1,466	2,150	1,808
Average Rate	\$100	\$100	\$100	\$100
Labor	\$195,426	\$146,570	\$214,969	\$180,769
Infrastructure				
Less Disk Storage	\$683,991	\$512,993	\$752,390	\$649,791
Traditional Disk	\$120,000	\$90,000	\$132,000	\$114,000
<i>Big Data</i>	<i>\$12,000</i>	<i>\$9,000</i>	<i>\$13,200</i>	<i>\$11,100</i>

Small Firm Estimate Drivers - Design/Build/Deploy		
Rationalized Source Attributes	517	<i>Number of Source Attributes to populate the Target Attributes X the Target Attributes</i>
Unique Target Attributes	196	<i>Unique attributes out of the 399 listed in the Record Type definitions</i>
FINRA Record Types	21	<i>Per FINRA data definition document</i>
Effort hours per Source Attribute	18	<i>Based on detailed bottom-up estimate using IBM estimating techniques</i>
Source Data Redundancy Factor	10%	
Calculated Source Data Attribute Count	517	
DBD Cost Distribution		
Design	23%	
Build	45%	
Test	24%	<i>Note testing does not include FINRA mandated testing</i>

By Role		
Business Requirements	4%	
Architecture	18%	
Data Modeling	3%	
Data Mapping	3%	
Data Integration	36%	
Reporting and Analytics	7%	
Testing	24%	<i>Note total testing hours are allocated across testing roles and design/development roles</i>
Project Management	5%	
Resource Distribution		
Local	45%	
Off shore	55%	

Small Firm Estimate Drivers - Run/Maintain		
Effort Basis	20%	
Infrastructure Factor	30%	

Large Firms Estimate

Finally, the effort required by large firms to design, build, and deploy CARDS is estimated at 42,315 hours, or \$8.5M. This reflects large firms' increased complexity in terms of multiple lines of business with multiple source systems that vary by products, lines of business, and divisions. The midpoint of hours required by this large firm to run and maintain CARDS is 8,463 hours, or \$847k. Total annual expenses for this firm will run an average of \$5.4M, factoring in \$3M in infrastructure costs (ex-storage) and approximately \$1.5M for storage of CARDS data in a "big data" repository.

Large Firm Cost Estimate assuming high complexity environment				
Design/Build Deploy(DBD)	Estimator	Low (-25%)	High (+10%)	Mid-Point
Hours	45,746	34,310	50,321	42,315
Average Rate	\$200	\$200	\$200	\$200
Total Cost	\$9,149,280	\$6,861,960	\$10,064,208	\$8,463,084
Run/Maintain				
Hours	9,149	6,862	10,064	8,463
Average Rate	\$100	\$100	\$100	\$100
Labor	\$914,928	\$686,196	\$1,006,421	\$846,308
Infrastructure				
Less Disk Storage	\$3,202,248	\$2,401,686	\$3,522,473	\$3,042,136
<i>Traditional Disk</i>	<i>\$24,988,000</i>	<i>\$18,741,000</i>	<i>\$27,486,800</i>	<i>\$23,738,600</i>
<i>Big Data Cloud 500/TB</i>	<i>\$1,664,000</i>	<i>\$1,248,000</i>	<i>\$1,830,400</i>	<i>\$1,539,200</i>

Large Firm Estimate Drivers - Design/Build/Deploy		
Rationalized Source Attributes	1,906	<i>Number of Source Attributes to populate the Target Attributes X the Target Attributes and assumes 30% redundancy in source data</i>
Unique Target Attributes	196	<i>Unique attributes out of the 399 listed in the Record Type definitions</i>
FINRA Record Types	21	<i>Per FINRA data definition document</i>
Effort hours per Source Attribute	24	<i>Based on detailed bottom-up estimate using IBM estimating techniques</i>
Source Data Redundancy Factor	30%	
Calculated Source Data Attribute Count	2,723	
DBD Cost Distribution		
Design	23%	
Build	45%	
Test	24%	<i>Note testing does not include FINRA mandated testing</i>
By Role		
Business Requirements	4%	
Architecture	18%	
Data Modeling	3%	
Data Mapping	3%	
Data Integration	36%	
Reporting and Analytics	7%	
Testing	24%	<i>Note total testing hours are allocated across testing roles and design/development roles</i>
Project Management	5%	
Resource Distribution		
Local	45%	
Off shore	55%	

Large Firm Estimate Drivers - Run/Maintain		
Effort Basis	20%	
Infrastructure Factor	35%	

Total Industry Cost

Using the median firm as a model and FINRA's estimate that 200 Clearing and Carrying Brokers will fall within this regime, we estimate that the total cost to firms in the industry will be approximately \$680M to build CARDS Phase 1, and \$360M to operate it on an annual basis. We separately calculated this estimate using a mix of 15% large firms, 35% medium firms, and 50% small firms and arrived at a materially similar total cost.

Additional technology costs to FINRA

As noted in FINRA's Regulatory Notice 14-37, FINRA estimates its own costs to develop CARDS to be between \$8M and \$12M over a three year period. However, FINRA it continues to evaluate additional technology costs.

FINRA's costs to implement phases 1 and 2 of CARDS would include costs to develop and maintain the technology infrastructure to collect, compile, standardize, reconcile, store and archive the CARDS data. Additional phase 2 costs would be incurred to develop and maintain a portal for introducing firms to submit phase 2 data directly to FINRA. There would also be costs associated with developing and sharing performance benchmarks and other information with firms. Based on the proposed rule requirements, FINRA's preliminary estimate of the cost to develop CARDS technology systems and processes ranges from \$8 million to \$12 million over a three-year period. There would be no direct impact to member firms associated with this investment. FINRA continues to assess the additional technology costs to maintain these systems, as well as costs to support an analytics program to run against the CARDS data."⁶

An additional cost to consider and emphasize is the cost to store CARDS data from 200 clearing and carrying firms. We estimate a cost of \$230,880 annually for the mean firm to store its own CARDS data, which would mean that FINRA could face data storage costs in excess of \$50M annually.

Note that the cost per terabyte of storage is ever-changing and can vary widely depending on the service levels required. We do assume, due to the nature of the data in CARDS, that this information will be need to be stored in a secure and resilient manner. The storage cost estimate is based on the total cost of a single terabyte written to a disk-based storage device, including all hardware overhead, disk specific infrastructure, energy costs, system administration, real estate, and HVAC costs.

Other costs

Duplication with CAT

FINRA doesn't believe there is an overlap between CARDS and the SEC's Consolidated Audit Trail (CAT) mandate, which is under development.

Fundamentally, CAT and CARDS collect different information. Unlike CARDS, CAT will not contain information regarding customer risk tolerance, investment objectives, money movements, margin requirements and position data that FINRA uses to conduct its reviews. This distinction is a core feature of CARDS and emphasizes FINRA's investor protection mission. In addition, an analysis by FINRA staff of any potential overlap between the data fields proposed to be collected by CARDS and CAT indicated that there was limited overlap. Any transaction information proposed to be collected by CARDS that

⁶ <http://www.finra.org/web/groups/industry/@ip/@reg/@notice/documents/notices/p600964.pdf>.

*would also have to be collected by CAT would require significant additional information such as commissions and fees and final settled moneys that CAT would not collect.*⁷

While suitability information will not be required in the CAT, as currently conceived, the largest record sets in CARDS, Purchase & Sales records, Security Reference data, and Securities Account Records, will all reside in the CAT in one form or another.

Firms with reporting obligations under CAT and CARDS would be required to submit the same data twice. Moreover, firms with overlapping reporting obligations would be required to complete two separate technology builds, two sets of testing, and would be transmitting that data twice.

As FINRA will be a consumer of CAT data, it will have access to much of this same information, and on a much timelier basis (day after trade date)⁸ than the monthly submissions as currently proposed for CARDS. It would seem that supplementing data FINRA will already receive from CAT would be a much more cost effective approach to obtaining the information FINRA desires.

Additionally if retail customer risk tolerance and investment objectives are CARDS' core feature, it might be more cost effective to exclude institutional transactions from CARDS all together.

Duplication with AEP and INSITE

As previously noted, FINRA's Automated Exam Program (AEP) and INSITE systems would become redundant with the CARDS requirement, however there would be additional costs incurred by running both systems in parallel prior to switching over to CARDS.

Increase in regulatory inquiry

Additional questions in our survey focused on whether participants expected regulatory inquiries to increase or decrease as a result of CARDS. All of the firms in our survey who answered this question (14 of 16) stated that they believe regulatory inquiries would *increase* as a result of CARDS. On average, participants estimated that regulatory inquiries will increase by 41%, with a minority predicting it will rise as much as 100%.

Most participants agreed that the CARDS system will drive a substantial increase in false positives in the data set. In comparison a study of over 600 Anti Money Laundering Professionals produced by Dow Jones and the Association of Certified Anti-Money Laundering Specialists, the authors cited the "majority of organizations [are] seeing over 50% or more of their alerts as false positives,"⁹ and that is in a much more mature area of regulation.

⁷ <http://www.finra.org/web/groups/industry/@ip/@reg/@notice/documents/notices/p601010.pdf>.

⁸ <http://www.sec.gov/divisions/marketreg/rule613-info.htm>.

⁹ http://www.dowjones.com/riskandcompliance/AML_e-Book_04.pdf.

Due to the likelihood of a substantial increase in false positives, firms will have to increase higher-salaried Legal and Compliance staff to respond to an expected increase in the number of inquiries triggered by the false positives.

Electronically surveilling for issues around suitability will be much more complicated, especially given that investors will tend to have multiple accounts with multiple objectives across multiple firms and these accounts will *not* be linked in CARDS.

Furthermore, there are no standardized definitions for risk tolerance and investment objectives. Each firm will have their own terminology, suitability categories, and guidelines for measuring suitability, especially across different types of businesses and client bases. This will further complicate the challenge of discerning clean signals out of this data and require enhanced diligence from regulators in order to resolve false positives.

CARDS may also force firms to alter existing surveillance practices, with some purchasing new systems or add-on functionality in order to tailor monitoring more closely to FINRA's actual use of CARDS data. This would be an additional cost borne by firms over and above their straight CARDS-compliance technology builds that may or may not have benefits to firms' overall surveillance programs.

AEP, currently an annual process, will be effectively run on a monthly basis with the initiation of CARDS reporting. This too could cause additional inquiries requiring follow-up throughout the year that might otherwise have been part of an annual examination.

Additional obligations for clearing firms

FINRA will also be imposing new burdens on clearing brokers to provide information on the securities accounts of their introducing firms. Previously, if there were an exam of the introducing broker, it would be their responsibility to provide evidence around proper sales practices; CARDS now places some of this burden on the clearing broker to maintain these records. As FINRA describes:

In Phase 1, CARDS would impose new obligations on approximately 200 carrying or clearing firms. These firms would be required to provide to FINRA a regular data submission that includes specified data, some with specified values, and in a specified file format. The information submitted in Phase 1 would cover securities accounts of these firms along with those of approximately 1,850 fully-disclosed introducing brokers.¹⁰

Conclusion

In this paper we analyzed the costs to clearing and carrying broker and to FINRA of Phase 1 of its currently proposed CARDS program. We examined the CARDS build and ongoing technology, staff, and outsourcing costs to impacted broker dealer communities and our survey and analysis estimated the mean cost for firms to implement CARDS will be \$3.4M, with \$1.8M

¹⁰ <http://www.finra.org/web/groups/industry/@ip/@reg/@notice/documents/notices/p601010.pdf>.

Ms. Marcia E. Asquith

December 1, 2014

Page 19 of 19

annually to operate their internal systems. The run rate figure is comprised of \$340k labor, infrastructure costs of \$1.2M, and storage under a “big data” model of \$230k. Using traditional disk storage methods, this run rate would be substantially higher. These estimates are based on data provided by 16 firms, large and small, administered by IBM through an anonymous survey using its proprietary Business Intelligence Estimating Model. These estimates are substantially higher than other earlier estimates of the costs to the financial industry to implement CARDS.

We estimate that total cost to the financial industry to implement CARDS Phase 1, based on average firm costs and FINRA’s estimate that some 200 clearing and carrying brokers would fall within this regime will be approximately \$680M to build, with an additional \$360M required annually to operate the regime.

In addition, we calculated that FINRA would incur an additional annual data storage cost based on the average record volumes of firms in our survey and determined that the costs to store this data could exceed \$50M annually. This cost is above and beyond FINRA’s prior estimates of its own costs to develop CARDS to be between \$8M and \$12M over a three year period.



Appendix B

COMPREHENSIVE AUTOMATED RISK DATA SYSTEM (CARDS) Re-Identification Risk Study (RRS)

December 1, 2014



This whitepaper explores the confidentiality risks associated with requiring Clearing Firms to regularly submit sensitive customer account, position, and transaction data to FINRA via its proposed Comprehensive Automated Risk Data System (CARDS). CARDS will centralize this information for both retail and institutional investors in a single location. Although Personally Identifiable Information has been removed from FINRA's initial concept for CARDS, we will demonstrate that CARDS data includes sufficient detail for an attacker to reverse engineer an investor's identity using only a handful of other data points and target both specific, highly sensitive persons and members of the general investing public for fraud, market manipulation and other crimes.

Table of Contents

Contributors	4
Introduction	4
Data Breach Threat	5
Types of Harmful Actors	6
External Actors.....	6
Internal Actors.....	7
Motivations	8
Cybercriminals	8
Hacktivists.....	9
Nation States	9
Reidentification Risk Defined.....	10
Attack Scenarios.....	10
Scenario 1: Control Person Attack.....	10
Scenario 2: Registered Representative Attack	12
Scenario 3: Additions and Withdrawals Attack.....	15
Scenario 4: Politically Exposed Persons Attack	17
Scenario 5: FINRA is compromised	19
Other Attacks	19
Aggregate Risks	19
Specific Firm Surveillance.....	20
Proprietary Trading Accounts	20
Trading Pattern Reverse Engineering	20
Investor Class Surveillance	20

Formation/unwinding of Concentrated Positions	20
Long-term analytics	21
Future Considerations	21
Conclusion	21

Contributors

The paper is commissioned by SIFMA and produced by IBM, which was engaged as a consultant to this process.

IBM

Robert James Stanich, Financial Markets Strategy, IBM Global Business Services

Kevin P Thomsen, Security Intelligence & Operations, IBM Global Technology Services

Mary Cosgrove, Business Transformation, IBM Global Business Services

Introduction

This whitepaper is aimed both at the general reader in the investing public as well as financial market participants and their regulators. Our goal is to help all parties understand some of the risks involved with consolidating sensitive customer account, position, and transaction data in a single data store. As such, we will assume the reader is not familiar with all of the terminology used here, and will attempt to introduce concepts as we proceed.

FINRA describes its proposed Comprehensive Automated Risk Data System (CARDS) as “a rule-based program that would allow FINRA to collect on a standardized, automated and regular basis, account information, as well as account activity and security identification information that a firm maintains as part of its books and records.”¹

As currently proposed, CARDS will include every purchase and sale of any financial product by every retail investor (individuals) and every institutional investor (e.g., pensions, hedge funds) in the Financial Markets. It will include flags to identify control persons in public companies and politically exposed persons,² and to identify foreign residents and foreign nationals. It will include all of the positions held in their accounts, as well as any incoming or outgoing checks, ACH, wire, debit card, or bill pay transactions made from their account(s); as well as all interest payments, dividend payments, margin calls and account transfers. In total, CARDS will provide a detailed map of assets held in brokerage accounts in the United States as well as flows of cash, securities, and payments in and out of these accounts.

The scope of information proposed to be available in CARDS stored in a central location would be valuable in the hands of threat actors such as cybercriminals, social and political hackers, and hostile nation states. CARDS could provide bad actors with information that could be used to commit financial fraud and to exploit nonpublic information for

¹ <http://www.finra.org/Industry/Regulation/Notices/2013/P412658>.

² These terms will be defined later in this paper.

financial gain; to expose or embarrass individuals, financial firms, and corporations; to perpetrate espionage, blackmail, or retribution against politically exposed persons; or to undermine public faith in our financial system.

Protecting the identities of individual account holders is key to mitigating some of the risks of consolidating such a broad range of financial and customer data in a single location. The initial CARDS proposal under Regulatory Notice 13-42³ left an open question as to whether the CARDS database would contain Personally Identifiable Information (PII) on individual retail investors.

PII refers to information that would identify individual account owners to FINRA (or an outside actor who has compromised the CARDS database). Such information might include data points such as the name, address, date of birth and social security number associated with an account. FINRA modified the CARDS proposal in Regulatory Notice 14-37 to exclude the collection of PII in response to “written comments on the CARDS concept proposal and the views expressed in FINRA staff’s discussions with industry participants regarding investor privacy.”⁴

Although PII has been ruled out of the current CARDS proposal, this paper demonstrates that substantial re-identification risk still exists in the CARDS dataset, which provides sufficient detail to reverse engineer an individual investor’s identity with only a handful of other data points – a risk that exists for both highly sensitive individuals as well as members of the investing public. We explore reidentification or reverse engineering risks associated with requiring firms to regularly submit sensitive customer account, holdings, transactions, transfers, and other information to FINRA via CARDS, even in the absence of PII.

Aggregate risks also exist in the CARDS dataset, and an attacker with access to the data doesn’t have to identify specific individuals in order to cause harm. Metadata concerning account types and surveillance of trading patterns are sufficient clues to obtain nonpublic information that could be used for fraud or market manipulation.

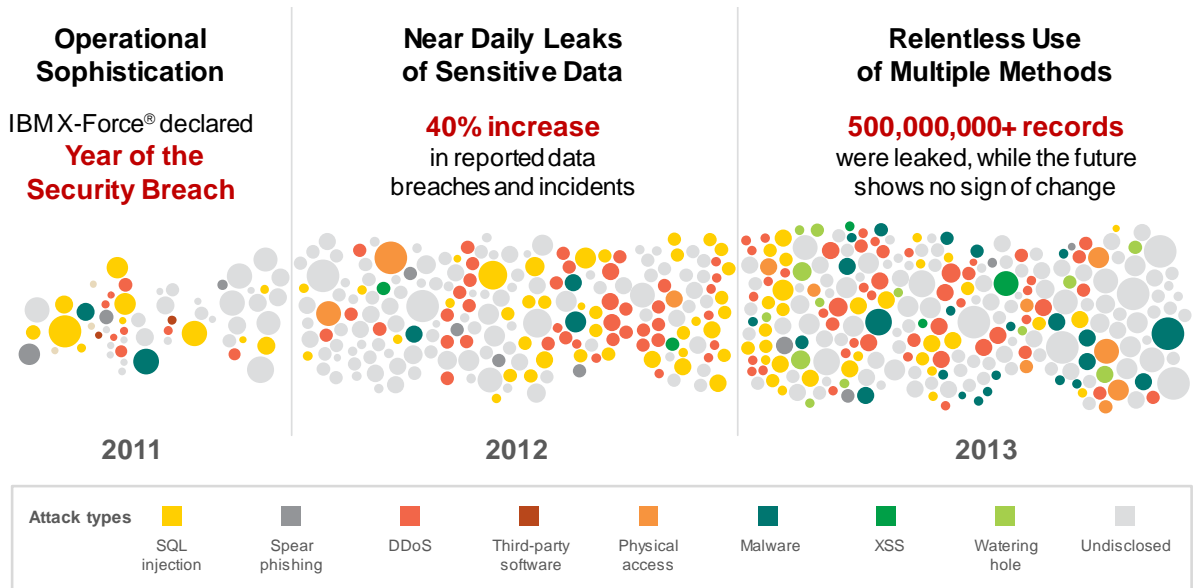
Data Breach Threat

In exploring risks presented by the consolidation of customer account information in the CARDS system, there are real risks that CARDS data will be breached, either by an external actor or an internal leak. There is risk in consolidating this sort of data in systems like CARDS. Even with cyber security protections in place, the number of data breaches US companies and government agencies experience continues to increase every year. The evolving threat landscape combined with a rise in the sophistication of threat actors means data breaches are a “new normal” and the number and different types of attacks will

³ <http://www.finra.org/web/groups/industry/@ip/@reg/@notice/documents/notices/p413652.pdf>.

⁴ <http://www.finra.org/Industry/Regulation/Notices/2013/P451243>.

continue to increase. The simple truth is that anytime there is an attractive target, actors with malicious intent will attempt to compromise sensitive systems and networks. It would not be safe to assume that FINRA would be immune from a significant hack or data breach.



Source: [IBM X-Force® Threat Intelligence Quarterly – 1Q 2014](#)

Types of Harmful Actors

There are a number of harmful actors that present real threats to systems containing sensitive data. Harmful actors can be divided into external and internal threat actors. External threat actors can include cybercriminals, hacktivists, and nation states. Internal threat actors are insiders with access to sensitive data who can be knowingly or unknowingly release or damage data. We will explore some of these hostile actors, their motivations and why the CARDS system would be a valuable target.

External Actors

External actors cover a broad range of individuals or groups who have different motivations to attack sensitive and confidential databases with damaging consequences. Recently a major home improvement retailer experienced a data breach by an external actor that affected up to 56 million customers after harmful malware was installed on its cash register system across 2,200 stores.⁵ The malware, thought to have been installed by hackers working for a foreign government, compromised customer payment card details.

⁵ <http://online.wsj.com/articles/home-depot-breach-bigger-than-targets-1411073571>.

Another major external breach at a retailer that occurred in 2013 compromised credit card information and personal information of as many as 70 million customers.⁶

Even sensitive government systems are susceptible to external breaches. In 2014, hackers thought to be working for a foreign government compromised unclassified systems at the White House.⁷ In 2008 an attacker breached the US military's classified computer network, and launched a major cyber-attack against the US Department of Energy, in which the personal information of several hundred employees was compromised.⁸ The Director of the National Security Agency (NSA), Admiral Michael Rogers, warned the House Intelligence Committee on November 20, 2014 that multiple nation states have the capability to disrupt US critical infrastructure through cyber operations. The Director also expects a major cyberattack against the U.S. in the next decade. "It's only a matter of the 'when,' not the 'if,' that we are going to see something dramatic."⁹

Finally, just this month, security specialist firm Symantec released a report on a highly sophisticated malware dubbed Regin that has been used, undetected, since 2008 to "infiltrate email databases, monitor network traffic, and steal passwords, snag screenshots and record mouse clicks."¹⁰ It is reported that this may be the most advanced attack discovered to date and its code is still being studied.

Internal Actors

Internal actors are one of the greatest threats to data security. SIFMA's recently published whitepaper, *Cybersecurity Insider Threat Best Practices Guide (July, 2014)*, noted the following:

Insider attacks on firms' electronic systems can result in financial and intellectual property theft, damaged or destroyed assets, and firm-wide disruption to internal systems and customer operations. Preventing and detecting attacks, however, has proven to be difficult, as insiders are often able to capitalize on their familiarity with firm systems to launch attacks without attracting notice.¹¹

⁶ <http://online.wsj.com/articles/SB10001424052702303754404579312232546392464>.

⁷ http://www.washingtonpost.com/world/national-security/hackers-breach-some-white-house-computers/2014/10/28/2ddf2fa0-5ef7-11e4-91f7-5d89b5e8c251_story.html.

⁸ <http://www.foxnews.com/politics/2013/02/04/sophisticated-cyber-attack-hits-energy-department-china-possible-suspect/>.

⁹ <http://online.wsj.com/articles/nsa-director-warns-of-dramatic-cyberattack-in-next-decade-1416506197>.

¹⁰ <http://www.cnet.com/news/advanced-regin-malware-poses-biggest-threat-outside-us/>.

¹¹ http://www.sifma.org/uploadedfiles/issues/technology_and_operations/cyber_security/insider-threat-best-practices-guide.pdf.

Several headline incidents in recent years highlight the risk that insiders pose to data security, even in well protected government systems. In 2010 Bradley Manning, an American soldier working as an intelligence analyst in Baghdad, over an eight month period leaked hundreds of thousands of highly classified intelligence documents to WikiLeaks.¹² Manning had legitimate access to files as part of his job responsibilities and described his attack as “childishly easy.”

Separately, in 2013, while working as a systems administrator for the NSA, Edward Snowden copied and released a vast range of top-secret documents in response to his concerns about US government programs.¹³ In response to the Snowden incident, the NSA cut back the number of system administrators by 90%, and imposed a “buddy” system to obtain access to certain sensitive data stores.¹⁴

Another common risk is the unwitting insider. According to a 2013 Cost of Data Breach Study by the Ponemon Institute, 64% of data breaches are due to employee or system error.¹⁵

Motivations

For the purposes of this paper, we will divide hostile actors into three distinct segments, each with their own unique motivations to target CARDS:

Cybercriminals

Comprehensive financial data sets like CARDS can provide an opportunity for criminals to exploit nonpublic financial information. For example, analysis of non-public financial information may allow cybercriminals to reverse engineer firms’ proprietary trading strategies or trade on information before it becomes publicly available. Cybercriminals could also use CARDS data to facilitate fraud by carrying out sophisticated social engineering attacks like spear phishing. Such schemes can be used to facilitate account takeover and allow criminals to monetize stolen information through wire fraud. Access to the CARDS dataset could be particularly attractive to cybercriminals because it points to specific accounts, provides precise details on customer holdings and identifies wealthy individuals with large account balances. Information about recent transactions in the CARDS dataset could be used to help facilitate fraud.

¹² <http://www.nytimes.com/2010/07/09/world/09breach.html>.

¹³ <http://www.biography.com/people/edward-snowden-21262897#blowing-the-whistle>.

¹⁴ http://www.sifma.org/uploadedfiles/issues/technology_and_operations/cyber_security/insider-threat-best-practices-guide.pdf.

¹⁵ <http://www.ponemon.org/local/upload/file/2013%20Report%20GLOBAL%20COADB%20FINAL%205-2.pdf>.

Cybercriminals with access to CARDS data can also sell sensitive information on the Darknet.¹⁶ For example, other criminals who obtain access to the data could cross reference stolen data or incorporate it into sophisticated fraud or market manipulation activities.

Hactivists

Hactivists are inspired by social or political goals and often use stolen information to draw attention to their campaign. The broad range of financial and customer account data available in CARDS could be used to support a broad range of hactivist goals. For example, hactivists may wish to target the clients or advisors of a particular financial institution or undermine the image of financial institutions in general. A hactivist could further embarrass specific individual clients (e.g., the CEO of a corporation perceived to oppose their cause, or a political leader with whom they disagree) by disclosing the sources or size of their assets, the nature of their investments, or target institutions (e.g., pension funds, corporations, university endowments) who have holdings in companies with whom the hactivist has social or political differences.

Hactivists could expose advisor compensation, the fees and commissions earned by particular individuals or firms, or attack the clients or the accounts of a specific advisor – all information available in the CARDS dataset. Hactivists could also attempt to illustrate the unequal distribution of wealth, draw conclusions about assets held by foreign investors within the US, or investments held by politically exposed persons that they view unfavorably. For example, hactivists supported the Occupy Wall Street movement with an online campaign called “Operation Robin Hood.”¹⁷

Nation States

Nation states’ motivations to access confidential information may include espionage, blackmail, retribution or harassment against individuals, theft of trade secrets, and disruption of the US markets. They can target large data sets like CARDS to gain information that can map back to persons of interest (e.g., critics, defectors, and political opponents). In November of 2014, NSA Director Michael Rogers, speaking to the House Select Intelligence Committee admitted that China and “possibly one or two more other countries” have the ability to shut down critical infrastructure systems in the US, including power utilities, aviation networks and financial companies.¹⁸

¹⁶ A darknet is a private network where connections are made only between trusted peers — darknets are often associated with illegal activities and dissident political communications.
http://en.wikipedia.org/wiki/Darknet_%28file_sharing%29.

¹⁷ <http://www.itsecurity.be/hactivists-join-forces-with-occupy-wall-street-movement>.

¹⁸ <http://www.reuters.com/article/2014/11/21/us-usa-security-nsa-idUSKCN0J420Q20141121>.

Insiders

The motivation for insiders to deliberately release data could be due to a number of factors including being disgruntled and wanting to embarrass the company or profit from the dataset. It is possible, although rare, that insiders may be blackmailed by an external threat actor to provide secure confidential information. Conversely insiders may expose sensitive data by mistake. They may fail to follow sound security practices, leaving systems and data exposed, may be tricked into revealing sensitive information through various social engineering attacks or be victimized by malware that utilizes their credentials to obtain elevated privileges in order to further penetrate sensitive systems.

Reidentification Risk Defined

Reidentification risk is the ability to use specific information within CARDS to determine the identity of investors by connecting CARDS data with other public or non-public information, even though PII has been removed from the dataset.

FINRA has put forward a point of view that without PII, the CARDS dataset cannot be used to identify specific individuals. “In the absence of PII,” they write, “FINRA believes that CARDS would not contain information that would enable accounts to be linked across firms or that would reasonably enable a potential hacker to determine the identity of an account’s owner.”¹⁹

In this section we will demonstrate five scenarios in which investors could be reidentified from data in CARDS. Moreover, the probability of a successful reidentification increases with the ability of hackers to cross reference other data sources to accurately narrow down potential account holders.

Attack Scenarios

We will demonstrate several scenarios where hackers can successfully reidentify investors in CARDS by using either publically available information or secondary data sources in combination with CARDS data.

Scenario 1: Control Person Attack

Attackers could use public SEC filings in combination with compromised CARDS data to reidentify and target investors.

An attacker may have interest in gaining access to positions, balances, and transactions of a specific control person of a large US publicly traded company. This could be an officer of the company or a large shareholder. The attacker could search a financial news website and

¹⁹ <http://www.finra.org/web/groups/industry/@ip/@reg/@notice/documents/notices/p600964.pdf>.

obtain a list of publicly disclosed insider transactions in a target company's stock. For example, an attacker notes that the CEO of the target company disclosed a sale of 10,518 shares of her company stock on August 27, 2014.

Figure: Publically Disclosed Insider Transactions

Aug 27, 2014	 Officer	10,518	Direct	Sale at \$191.57 - \$191.78 per share.
--------------	--	--------	--------	--

The attacker then queries CARDS Purchase and Sales records for an account transacting the net number of shares of this stock on this specific date. The attacker can then reference the CARDS Securities Account Suitability table to determine whether this account belongs to a control person of a public company and confirm their year of birth.

Figure: Securities Account Suitability Table

Element Sequence Number	Element Name	Element Definition (from Data Dictionary Tab)	Primary Key	Element Data Type (from Data Dictionary Tab)	Element Validation	Mandatory (M) or Business Conditional (BC) or Conditional (C)	Element Comments
8	ACCOUNT NUMBER	The value assigned by a member which uniquely identifies an account within that firm. If the account number is only unique with the concatenation of a branch identifier, then the account number must be concatenated. The account number must not include the type code (i.e., code representing, Margin, Cash, etc.).	PK	ALPHA(100)	The ACCOUNT NUMBER provided shall exist in SECURITIES ACCOUNT for the given DATA AS OF DATE.	M	
14	CONTROL PERSON FOR PUBLIC COMPANY FLAG	Indicates if the account participant or control person is a senior officer, director or 10% or more shareholder of a public company.		ALPHA(2)	If at least one of account participants is a person entity (i.e. SECURITIES ACCOUNT PARTICIPANT.ACCOUNT PARTICIPANT NATURAL PERSON FLAG = 'Y'), this element shall be populated with the following values: Y = Yes N = No If not applicable, this element shall be populated with NA = Not Applicable	M	
21	ACCOUNT OWNER BIRTH YEAR	The birth year of the youngest account owner participant on the account.		INTEGER	If account participant is a person entity (i.e. SECURITIES ACCOUNT PARTICIPANT.ACCOUNT PARTICIPANT NATURAL PERSON FLAG = 'Y') and ACCOUNT PARTICIPANT ROLE TYPE CODE = 'ACCTOWNR' and this data point has been captured by the member then this element shall be required. Format is yyyy.	BC	

This is a simplified example for the purposes of illustration, but there are multiple variations of this attack with high probability of reidentification against one or more transactions publically disclosed by insiders.

The attacker now has additional information that can help identify their target's other accounts held within the same firm, revealing other securities they hold, their cash balances, debit card activity and more. The attacker can also monitor future reportable transactions in these accounts before they are publically disclosed, depending on the timing of the transactions relative to firms' CARDS submissions.

While this simplified example targeted a specific investor, in practice, an attacker with this skill and knowledge would likely be able to run this type of attack against all control persons of all US listed companies *en masse* with a single automated interrogation of the database. This would afford the attacker opportunities for additional illegal activity.

This is a high probability, high impact attack for both cybercriminals and hacktivists. As described above, a nation state could seek to monitor the financial activities of their own citizens or enemies within the United States. This risk could have the unintended consequence of persuading investors to move financial accounts and assets to institutions that would not fall under the CARDS regulatory framework.

Scenario 2: Registered Representative Attack

Our next scenario will demonstrate how the CARDS database could be used to target financial professionals. As with the Control Persons attack, this is another high probability, high impact attack that requires only information accessible to the public, in this case from FINRA itself. Financial professionals often are required to direct their own personal accounts with the broker dealers where they are registered. Because of specific identifying information available in the CARDS dataset, this leaves employees of broker dealers vulnerable to reidentification.

In this scenario, the attacker queries the CARDS Securities Account table for accounts identified as belonging to an employee of the broker dealer.

Figure: Securities Account Table

Element Sequence Number	Element Name	Element Definition (from Data Dictionary Tab)	Primary Key	Element Data Type (from Data Dictionary Tab)	Element Validation	Mandatory (M) or Business Conditional (BC) or Conditional (C)	Element Comment
8	ACCOUNT NUMBER	The value assigned by a member which uniquely identifies an account within that firm. If the account number is only unique with the concatenation of a branch identifier, then the account number must be concatenated. The account number must not include the type code (i.e., code representing, Margin, Cash, etc.).	PK	ALPHA(100)		M	
19	EMPLOYEE ACCOUNT FLAG	Indicates if the account is held by an employee of the member.		ALPHA(2)	Allowable Values: Y = Yes N = No NA - Not Applicable	M	

Figure: Securities Account Servicing Rep Table

Element Sequence Number	Element Name	Element Definition (from Data Dictionary Tab)	Primary Key	Element Data Type (from Data Dictionary Tab)	Element Validation	Mandatory (M) or Business Conditional (BC) or Conditional (C)	Element Comments
8	ACCOUNT NUMBER	The value assigned by a member which uniquely identifies an account within that firm. If the account number is only unique with the concatenation of a branch identifier, then the account number must be concatenated. The account number must not include the type code (i.e., code representing, Margin, Cash, etc.).	PK	ALPHA(100)	The ACCOUNT NUMBER provided shall exist in SECURITIES ACCOUNT for the given DATA AS OF DATE.	M	
13	REGISTERED REP CRD NUMBER	Unique number assigned to the registered representative by the CRD system during the registration process.		INTEGER		M	

The attacker then looks up each of those accounts in the Securities Account Servicing Representative table to obtain the Registered Representative's *Central Registration Depository* (CRD) number. The CRD system allows them to connect with specific brokers:

FINRA operates Web CRD, the central licensing and registration system for the U.S. securities industry and its regulators. It contains the registration records of more than 6,800 registered broker-dealers and the qualification, employment, and disclosure histories of more than 660,000 active registered individuals.²⁰

Using the CRD number on the account, the attacker goes to FINRA's Web CRD site or FINRA BrokerCheck and looks up the Registered Rep's CRD number to obtain his full name, firm, branch address, registrations, history and other information.

²⁰ <http://www.finra.org/Industry/Compliance/Registration/CRD/>.

Figure: FINRA BrokerCheck Showing Rep Name, Business Address, and History

The screenshot displays the FINRA BrokerCheck search interface. At the top, there is a navigation bar with the FINRA logo and links for 'FINRA Home', 'About FINRA', and 'Newsroom'. Below this is a blue 'Investors' header with sub-links for 'Tools & Calculators', 'Contacts', and 'Subscriptions'. A red navigation bar contains 'Protect Yourself', 'Smart Investing', and 'Market Data'.

The main section is titled 'BrokerCheck®' and contains a search form. The form asks the user to choose between 'Individual' (selected) and 'Firm'. The search criteria are as follows:

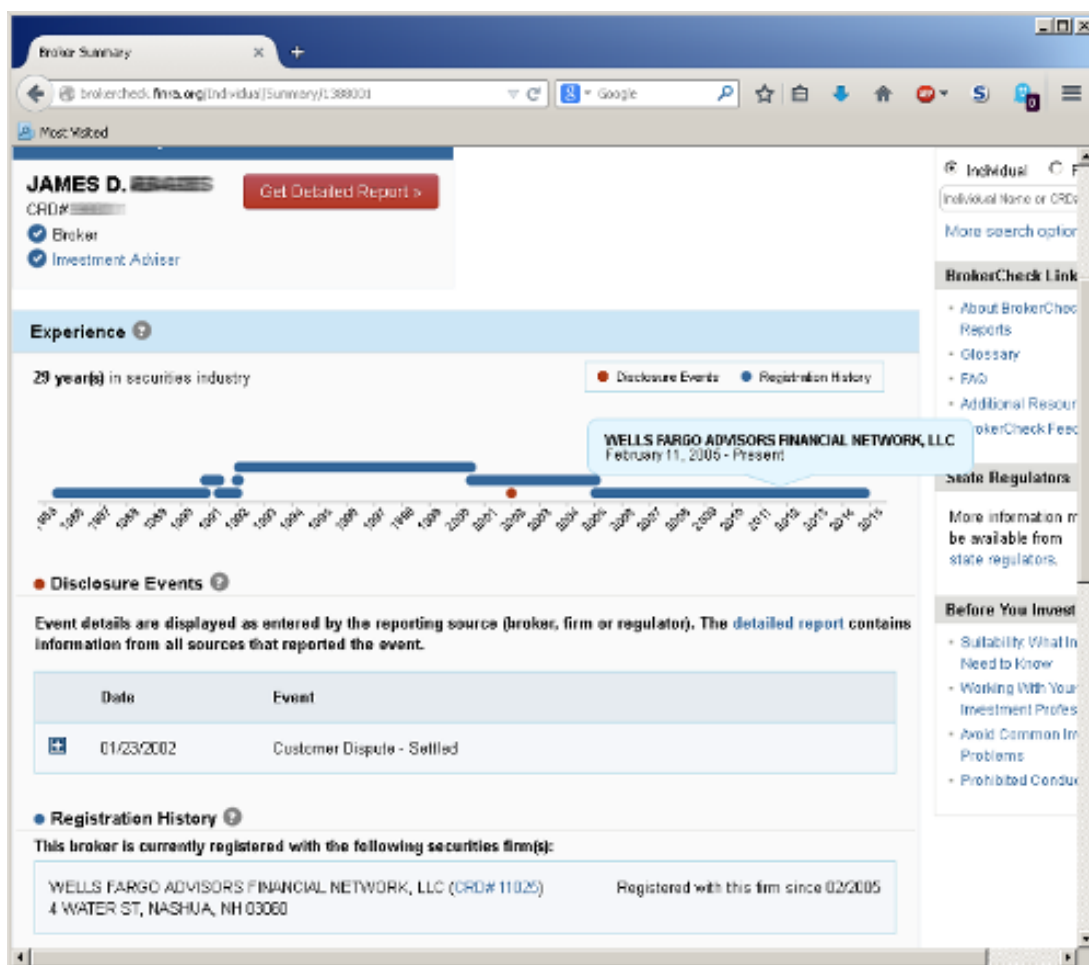
- Individual Name or CRD#: 8675309
- Employing Firm Name or CRD# or SEC#: (Current or Previous)
- Zip Code: (empty)
- Within: 5 Miles

A 'Search' button is located below the form. Below the search form, there is a note: 'Need help searching? Review the online help or call the FINRA BrokerCheck Hotline at (800) 289-9999.'

On the right side of the page, there are three sections:

- BrokerCheck Links:** About BrokerCheck Reports, Glossary, FAQ, Additional Resources, BrokerCheck Feedback.
- State Regulators:** More information may be available from state regulators.
- Before You Invest:** Suitability: What Investors Need to Know, Working With Your Investment Professional, Avoid Common Investor Problems, Prohibited Conduct.

At the bottom of the page, there are links for 'Sitemap', 'Privacy', and 'Legal', and a copyright notice: '© 2014 FINRA. All rights reserved. FINRA is a registered trademark of the Financial Industry Regulatory Authority, Inc.'



Referring back to CARDS, an attacker can now see how many customers the broker has, total assets under management, and other information which might be of interest. The attacker can also see what the broker’s customers are trading, their account balances, their last transaction, etc. Again, we have demonstrated a relatively simple, single-person version of the attack for purposes of illustration. In practice such an attack could be automated to interrogate the entire dataset. There are also several variants of the attack in which an attacker could target specific brokers, brokers of a certain firm, brokers handling a certain type of business, or in combination with other potential attacks highlighted in this paper.

Scenario 3: Additions and Withdrawals Attack

In scenario 3, we will demonstrate an attack against all investors with accounts at FINRA member firms. While the impact of this attack is high and the probability of identifying a large group of individuals is high, it is more of a “shotgun” approach that will help an attacker identify a certain subset of vulnerable investors.

This attack relies on a secondary dataset outside of CARDS which includes PII and also has overlapping data with CARDS.

While this may at first seem like a remote possibility, one of the coauthors of this whitepaper discovered this risk first hand after using his brokerage-account-linked debit card at a popular home improvement chain whose data had been breached. When that particular breach was eventually detected and disclosed by the retailer, the coauthor's fast-thinking financial advisor issued him a new, uncompromised debit card. However, the data breach in combination with his brokerage account information might also have made him personally identifiable in CARDS. Other datasets obtained in similar breaches are still available and new breaches are occurring every day. Specifically, PII data associated with recent breaches is available for sale in some corners of the internet familiar to criminals.

More generally, any payment made from an individual's account, be that via ACH, wires, checks, bill pay, or debit card transactions, will appear in the CARDS Account Additions and Withdrawals table. Whether an investor has been paying their mortgage via bill pay, or using their debit card at a retail store, somewhere there is another database containing the other side of that transaction, providing a set of keys to their CARDS data.

In this scenario, the attacker obtains one or more of the many datasets of breached payments information available on the Darknet. They can then join that information against the CARDS Account Addition and Withdrawals table, matching payment types, amounts, and dates over a period of time tied to the same account number. In this manner, the attacker will have successfully reidentified every person who utilized their brokerage account to make payments that existed in both data sets.

Figure: Account Additions and Withdrawals Table

Element Sequence Number	Element Name	Element Definition (from Data Dictionary Tab)	Primary Key	Element Data Type (from Data Dictionary Tab)	Element Validation	Mandatory (M) or Business Conditional (BC) or Conditional (C)	Element Comments
8	ACCOUNT NUMBER	The value assigned by a member which uniquely identifies an account within that firm. If the account number is only unique with the concatenation of a branch identifier, then the account number must be concatenated. The account number must not include the type code (i.e., code representing, Margin, Cash, etc.).	PK	ALPHA(100)	The ACCOUNT NUMBER provided shall exist in SECURITIES ACCOUNT.	M	
10	TRANSACTION TYPE CODE	Identifies if the transaction is in the cash or margin component of the account.	PK	ALPHA(20)	Allowable Values: ACH = ACH FED = Fed Wire CHK = Check CSHEQVLT – Cash equivalents like Money Order, Cashier’s Checks DVDND = Dividend payment INTRST = Interest Payment MRGNINTRST = Margin Interest FEE_MNGDACCT = Managed Account Fee FEE_CUSTODIAL = Custodial fee FEE_OTHER = Other fee DBTCRD – Debit Card BILLPAY – Bill Pay LOAN = Loan Repayment	M	
11	TRANSACTION DATE	The date the transaction was posted.		DATE	Format should be YYYYMMDD.	M	
15	TRANSACTION AMOUNT	The dollar amount of the transaction.		SIGNED DECIMAL	Include sign where applicable.	M	

The impact of this scenario is high in the hands of a cybercriminal. The attacker can now see how much money is in individual accounts, the firm where they are held, their spending habits, and other information which they could sell or use in an attempt to steal money out of an account. Specifically, many “challenge questions” firms ask when individuals seek to withdraw large amounts from an individual account include questions regarding recent account activity.

An attacker could also filter for accounts with large cash balances, or use the location of the registered rep or address information in the second compromised dataset to search for persons of interest like politicians, financiers, or celebrities and cross reference them to locations like Washington DC, New York, or Los Angeles.

Scenario 4: Politically Exposed Persons Attack

We will now examine a much smaller but important cross section of the population of particular interest to a formidable and tenacious actor, the nation state.

An attacker in this scenario could in some cases reidentify individuals in CARDS without additional data, it is more likely to be used in combination with other approaches in order to achieve a highly-targeted attack on a specific class of individuals.

“Politically Exposed Persons” (PEPs) are individuals who are or have been entrusted with prominent public functions in a foreign country, for example heads of state or of

government, senior politicians, senior government officials, judicial or military officials, senior executives of state owned corporations, or important political party officials.²¹

The CARDS Securities Account Suitability table contains a flag for PEPs in its Securities Account Participant table, which makes such persons easy for attackers to identify. Coupled with other data such as the Country of Residence, Country of Origin, Birth Year, or restricting searches to a specific geographic locale (by branch/registered representative), it becomes possible to reidentify specific individuals in the dataset. The more specific the target, and the more that is known about the target (e.g., the firm or branch where they hold their accounts, the identity of their advisor and positions that may be in their accounts), the easier it will be to reidentify them.

Figure: Securities Account Suitability Table

Element Sequence Number	Element Name	Element Definition (from Data Dictionary Tab)	Primary Key	Element Data Type (from Data Dictionary Tab)	Element Validation	Mandatory (M) or Business Conditional (BC) or Conditional (C)	Element Comments
8	ACCOUNT NUMBER	The value assigned by a member which uniquely identifies an account within that firm. If the account number is only unique with the concatenation of a branch identifier, then the account number must be concatenated. The account number must not include the type code (i.e., code representing, Margin, Cash, etc.).	PK	ALPHA(100)	The ACCOUNT NUMBER provided shall exist in SECURITIES ACCOUNT for the given DATA AS OF DATE.	M	
11	ACCOUNT PARTICIPANT POLITICALLY EXPOSED PERSON FLAG	As per the Financial Action Task Force (FATF) definition, "Politically Exposed Persons" (PEPs) are individuals who are or have been entrusted with prominent public functions in a foreign country, for example Heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. Business relationships with family members or close associates of PEPs involve reputational risks similar to those with PEPs themselves. The definition is not intended to cover middle ranking or more junior individuals in the foregoing categories.		ALPHA(2)	If at least one of account participants is a person entity (i.e. SECURITIES ACCOUNT PARTICIPANT.ACCOUNT PARTICIPANT NATURAL PERSON FLAG = 'Y'), this element shall be populated with the following values: Y = Yes N = No If not applicable, this element shall be populated with NA = Not Applicable.	M	
21	ACCOUNT OWNER BIRTH YEAR	The birth year of the youngest account owner participant on the account.		INTEGER	If account participant is a person entity (i.e. SECURITIES ACCOUNT PARTICIPANT.ACCOUNT PARTICIPANT NATURAL PERSON FLAG = 'Y') and ACCOUNT PARTICIPANT ROLE TYPE CODE = 'ACCTOWNR' and this data point has been captured by the member then this element shall be required. Format is yyyy.	BC	

An attacker may wish to narrow his target down to a single individual or group of individuals, such as PEPs with registered representatives in the Washington, D.C. area that might be associated with a particular foreign mission.

Another variation on this scenario could be to develop a "Wealth Map" of all PEPS from a specific country of origin: where they are custodialing their assets, what positions they hold, and what financial transactions they are making from their accounts. These accounts or their registered reps can then be targeted for further data mining by the attacker.

²¹ <http://www.fatf-gafi.org/media/fatf/documents/recommendations/guidance-pep-rec12-22.pdf>.

Scenario 5: FINRA is compromised

If we assume that the CARDS database can be breached, it is fair to explore the scenario of a more general breach at FINRA in which other data sources containing PII are also compromised.

Data stores associated with the Automated Exam Program (AEP),²² Electronic Blue Sheets (EBS),²³ Web CRD²⁴ and other FINRA systems contain account information or personally identifiable information (PII) including name, address, date of birth and Tax Identification Number.

A cyber attacker obtaining access to one or more of these other systems can merge these datasets together to reidentify a large number of investors in the CARDS database. An attacker would then be able to monitor an individual investor's transactions, understand their positions and trading behavior, and observe payments in and out of their accounts.

Other Attacks

We have examined five scenarios under which an attacker can positively identify and exploit investors using CARDS data even though CARDS no longer plans to contain PII.

As many CARDS data elements are common to other data sets, some of them public, it is possible to reidentify individuals even with relatively unsophisticated attacks. For instance, reidentifying a specific individual in CARDS is as simple as stealing their account number, a fairly low bar for a nation state interested in obtaining a digital audit trail of an individual's financial life.

To a sufficiently sophisticated analyst with access to CARDS data, an attacker may easily identify a targeted investor through analysis of the target's trading patterns, positions, returns, product types, or volumes of transactions. It might not be necessary to identify an investor by name, if for instance, an attacker selects consistently profitable accounts with certain characteristics (e.g., a hedge fund account with a particular prime broker), and simply begins to either mirror their trading activity or reverse engineer their trading strategy. We will highlight some additional attacks that do not specifically hinge on reidentification in the next section of the paper.

Aggregate Risks

Aggregate risks are much more likely to be exploited by sophisticated consumers of CARDS data with some computing capabilities and knowledge of the financial markets as

²² <http://www.finra.org/web/groups/industry/@ip/@comp/@rf/documents/appsupportdocs/p124271.pdf>.

²³ <http://www.finra.org/web/groups/industry/@ip/@reg/@notice/documents/notices/p194655.pdf>.

²⁴ <http://www.finra.org/Industry/Compliance/Registration/CRD/>.

opposed to individual fraudsters. Examples might include a rogue trader or hedge fund looking to purchase nonpublic information or a nation state seeking to provide an information advantage to its own state-controlled interests.

Specific Firm Surveillance

An attacker may wish to observe and analyze the trading activity or positions of a specific firm. CARDS would make this task rather easy, as an attacker could simply filter data on a firm's CRD number in the Purchase and Sales table.

In another variation on this scenario, the attacker might limit monitoring to the activities of a single registered rep, branch, or account type that the attacker knows to be associated with the activity in which the attacker is interested, alone or in combination with the Registered Rep Attack described above.

Proprietary Trading Accounts

Similarly, a sophisticated attacker might focus attention on surveilling a firm's proprietary trading accounts by further filtering his specific firm surveillance to return only accounts flagged in CARDS as having the Proprietary Trading Account Classification.

Trading Pattern Reverse Engineering

A sophisticated attacker can identify an account of interest - ,either through reidentification, observing a pattern of positive returns in the account, or in combination with an Account Registration Code of interest (e.g., Hedge Fund, Prime Broker). Once identified this sophisticated attacker could reverse engineer the trading strategy used in that account.

Investor Class Surveillance

CARDS is also susceptible to surveillance by Investor Class, which would provide useful market intelligence. If a sophisticated attacker wishes to know what hedge funds have been purchasing in aggregate over the prior period, what assets institutional investors are accumulating, how much investor funds are available in cash, what assets retail investors are accumulating, how their spending is increasing or decreasing, all of this information would be available in CARDS.

Formation/unwinding of Concentrated Positions

Another use of the CARDS dataset could be to observe the accumulation of concentrated positions in a single security just under a mandated reporting threshold, or, depending on the timing of transactions, prior to public disclosure.

Long-term analytics

Finally, a sufficiently sophisticated attacker of CARDS data could analyze the entire dataset looking for their own relationships and correlations in historical CARDS data. Marrying a “big data approach” common to quantitative traders against total information awareness of every transaction that has transpired in the financial markets over the past year, this actor is likely to develop sophisticated insights based on nonpublic information not yet conceived by the authors of this paper.

Future Considerations

Even if CARDS does not contain PII today or is only being used by FINRA in a certain manner, it does not preclude a change in its nature or purpose in the future. For instance, a change in administration or political sentiment in the US could quickly result in the reestablishment of PII in CARDS. If CARDS comes into being, it will not only become the target of persons who will wish to exploit it, but will also be a target for political forces that will wish to use this data differently, or in ways we have not yet conceived.

Conclusion

This paper set out to explore whether reidentification or reverse engineering risks associated with the FINRA CARDS database exist. We laid out five plausible scenarios in which a person with access to this data could reidentify individuals in the data set, including high-value targets such as control persons of public companies and politically exposed persons. We also demonstrated how, by using transactions common to both CARDS and a secondary source of breached data, just about any investor who exists in both data sets could be reidentified.

Finally, we covered several aggregate risk scenarios which, even in the absence of placing a name against a specific account, CARDS could be abused by a sophisticated attacker for financial gain.

As one of the biggest consolidated repositories of nonpublic financial information, CARDS will continue to represent a high-value target for various classes of attackers. Even though CARDS itself cannot be used to effect financial transactions, it could still be used to facilitate fraud, cause serious damage to investors, and to undermine confidence in our financial markets.