



FINANCIAL  
SERVICES  
ROUNDTABLE

**Via electronic mail at [pubcom@finra.org](mailto:pubcom@finra.org)**

March 21, 2014

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

**Re: Comprehensive Automated Risk Data System: FINRA Requests Comment on a Concept Proposal to Develop the Comprehensive Automated Risk Data System (“CARDS”), Regulatory Notice 13-42 (Dec. 2013)**

Ms. Asquith:

The Financial Services Roundtable (“FSR”)<sup>1</sup> respectfully submits these comments on the Concept Proposal by the Financial Industry Regulatory Authority (“FINRA”), entitled “Comprehensive Automated Risk Data System.”<sup>2</sup> FSR believes that FINRA should address several significant issues inherent in CARDS, a program that would greatly expand FINRA’s collection and housing of information about more than 110

---

<sup>1</sup> *As advocates for a strong financial future*<sup>TM</sup>, FSR represents 100 integrated financial services companies providing banking, insurance, and investment products and services to the American consumer. Member companies participate through the Chief Executive Officer and other senior executives nominated by the CEO. FSR member companies provide fuel for America’s economic engine, accounting directly for \$98.4 trillion in managed assets, \$1.1 trillion in revenue, and 2.4 million jobs.

<sup>2</sup> Comprehensive Automated Risk Data System, FINRA Requests Comment on a Concept Proposal to Develop the Comprehensive Automated Risk Data System, Regulatory Notice 13-42 (“Regulatory Notice 13-42”), *available at* <http://www.finra.org/web/groups/industry/@ip/@reg/@notice/documents/notices/p413652.pdf>.

million<sup>3</sup> customers of the financial services industry in a manner duplicative of the consolidated audit trail (“CAT”).<sup>4</sup>

## Executive Summary

According to FINRA in Regulatory Notice 13-42, CARDS would be a “rule-based program” requiring clearing brokers and self-clearing brokers to provide to FINRA “on a standardized, automated and regular basis, account information [...] account activity and security identification information.” Initially, CARDS would require clearing and self-clearing firms to submit retail customer information to CARDS, including details of client account activity, account balances, customer identification information, and security descriptions.<sup>5</sup> Introducing firms would have to provide the specified information to their clearing firms.<sup>6</sup> FINRA intends to use the information, in conjunction with certain analytics, to identify possible sales practice and business conduct issues.<sup>7</sup> FSR’s comments on CARDS can be summarized as follows:

- Regulatory Notice 13-42 does not make clear whether FINRA intends to promulgate CARDS in accordance with formal rulemaking procedures as is required. FSR urges FINRA to follow the normal notice-and-comment rulemaking process in adopting CARDS.
- FINRA’s cost-benefit analysis is too limited; the data upon which it relies are unreflective of the costs to the broad range of firms. A more robust cost-benefit analysis is necessary to avoid inflicting severe financial harm on members and their clients.
- CARDS, as envisioned, would overlap substantially with CAT and thus clash with explicit Commission policy. FINRA does not articulate a rationale for having CARDS as a separate collection mechanism and repository of information.

---

<sup>3</sup> See Karen Donovan, *Arbitration Works, Says SIFMA; No it Doesn’t, Says PIABA*, WEALTH MANAGEMENT.COM, (Oct. 4, 2007), <http://wealthmanagement.com/legal-compliance/arbitration-works-says-sifma-no-it-doesn-t-says-piaba> (estimating the number of brokerage accounts in the United States to be more than 111 million).

<sup>4</sup> CAT was adopted by the Securities and Exchange Commission (the “Commission”) in 2012. See SEC. & EXCH. COMM’N, Consolidated Audit Trail, Exchange Act Release No. 34-67457 (May 26, 2010) (“Exchange Act Release No. 34-67457”).

<sup>5</sup> Regulatory Notice 13-42 at 2, 5, and 7.

<sup>6</sup> *Id.* at 2.

<sup>7</sup> *Id.* at 1.

- FINRA does not sufficiently address the data security concerns associated with CARDS, especially in light of broad governmental policy objectives related to the security of financial data.
- CARDS raises serious (potentially insurmountable) issues under foreign and state privacy laws. FINRA's possession of private client data also may undermine client confidence and drive clients away from broker-dealers to other financial services industry participants.
- FSR requests clarification on whether FINRA intends to adopt a collaborative or an enforcement-oriented, punitive posture with respect to members whose conduct actually or ostensibly raises "red flags" under CARDS. FINRA also should address the kind of supervisory role CARDS will impose on it.

## **Introduction**

FSR supports FINRA's role as a regulator and as a bulwark against unlawful behavior, and it applauds FINRA's efforts on those fronts. We believe that FINRA's current enforcement methods are effective both at identifying and punishing wrongdoing. For these reasons, we take this opportunity to comment on various aspects of the CARDS proposal. FSR urges FINRA to consider the issues raised in this letter, because we believe CARDS would create numerous problems and great expense for FINRA, the industry, and ultimately the brokerage firms' customers.

In particular, FSR is concerned about six broad issues. First, we believe CARDS must be promulgated *via* notice-and-comment rulemaking; however, certain language in the release leads us to believe that FINRA may intend to develop and implement CARDS without formal rulemaking. Second, we believe FINRA's cost-benefit analysis is inadequate, because it is grounded largely in FINRA's experience with two large firms that are not representative of the industry as a whole and fails to account for the deleterious effects CARDS would have on inter-firm and firm-client relationships. Third, given the similarity of CARDS's and CAT's features, CARDS would constitute unnecessary, duplicative regulation and clash with explicit Commission policy mandating the elimination of systems CAT renders duplicative. Fourth, public concern about governmental and private entities' collection of private data militates against adopting CARDS. Additionally, state and foreign privacy laws might make it impossible for certain FINRA members to comply. Fifth, the danger of compromises in data security and the concomitant undermining of broad governmental policy objectives regarding data security also militate against adopting CARDS in its current form. Sixth, FSR believes FINRA should clarify how it intends to use the information it gathers and analyzes, and whether it sees CARDS an enhanced enforcement tool or as a channel for collaboration between FINRA and its members.

For these reasons, FSR urges FINRA to reconsider many elements of CARDS. If FINRA decides nevertheless to move forward with CARDS, we plan to provide further comments on the specific details of the proposed system once FINRA submits a proposed CARDS rule set for notice-and-comment.

### **Procedural and Related Concerns**

FINRA’s description of how it intends to promulgate CARDS seems to imply that CARDS will not be subject to the requirements of a notice-and-comment rulemaking. FSR is specifically concerned by the statement saying that FINRA, “in developing CARDS,” is “not intending to amend FINRA’s rules governing books and records requirements.”<sup>8</sup> Such a statement suggests that FINRA believes CARDS can be implemented without a rulemaking. FSR believes that a rulemaking is required, and also urges FINRA to conduct the comprehensive cost-benefit analysis that typically accompanies a rulemaking.

#### Implementing CARDS without a Rulemaking Would Be Problematic

Section 19(b) of the Securities Exchange Act of 1934 (the “Exchange Act”),<sup>9</sup> provides that “no proposed rule change shall take effect unless approved by the Commission” or an exception applies. We do not believe any of the exceptions apply. Given the enormous increase in the scope of data collection under CARDS, the program is far more than a mere policy, practice, or interpretation with respect to the administration or enforcement of an existing rule, and it is not solely concerned with the administration of FINRA as a self-regulatory organization.<sup>10</sup>

Moreover, the benefits to FINRA, to the industry, and to investors flowing from the transparency, Commission feedback, and Commission approval that a notice-and-comment rulemaking would provide, strongly suggest FINRA should not forego the full process. Notice-and-comment would also allow for a more robust analysis of the costs and benefits of CARDS, permitting interested parties to provide feedback on more granular, detailed components of CARDS, rather than merely on a high-level concept. Finally, full rulemaking should occur so that FINRA can demonstrate why CARDS is needed in addition CAT.

---

<sup>8</sup> *Id.* at n. 8.

<sup>9</sup> Codified at 15 U.S.C. §78S.

<sup>10</sup> 15 U.S.C. §78S(b)(3)(A).

## Concerns Regarding Costs and Benefits Generally

While it is impossible to know precisely how to quantify the costs and benefits associated with CARDS, it is likely that the expense to individual members will be enormous. By way of comparison, some commentators estimated the cost per firm to adopt the technology necessary to implement CAT to be millions of dollars.<sup>11</sup> At least one firm has estimated that the costs associated with updating its systems to be CARDS-compliant would exceed \$2 million, followed by large costs to keep systems CARDS-compliant on an ongoing basis.<sup>12</sup> The data standardization CARDS calls for could prove especially costly, with commentators describing similar standardization in the context of CAT as “a monumental task,” and noting that standardization required firms to adopt whole new market-wide systems.<sup>13</sup> Estimates of expenditures in the millions may seem trivial to some organizations, but cost items like these, especially on the heels of many other large regulatory initiatives, leave little in the budget for upgrades to the client experience, an area that FINRA should consider of equal or greater importance.

FSR is concerned that FINRA is dramatically underestimating CARDS’s burden on firms. The regulatory notice indicates that FINRA derived its conclusions regarding the anticipated costs and benefits of CARDS largely from “experience with two major clearing firms.”<sup>14</sup> FSR recommends that FINRA also conduct research with firms that lack the resources of the large clearing firms FINRA studied. FINRA should confirm that firms of all kinds and sizes have ready access to the information CARDS would demand, and that it would not be burdensome for other kinds of firms to supply information in the standardized form FINRA contemplates. While FINRA suggests it would alleviate the burden by using a “phased approach”<sup>15</sup> to implementing CARDS, it is

---

<sup>11</sup> See, e.g., Comment Letter of Securities Industry and Financial Markets Association on the Consolidated Audit Trail *available at* <http://www.sifma.org/comment-letters/2010/sifma-submits-comments-to-the-sec-on-consolidated-audit-trails/> (estimating costs to the industry in implementing the consolidated audit trail; the real time reporting requirement, estimated to be the most expensive proposed requirement, was not adopted, but the major expense would have come from the extensive system changes needed to comply, similar to the expenses necessary to comply with CARDS as currently envisioned).

<sup>12</sup> See Comment Letter of Diamant Investment Corporation on the Comprehensive Automated Risk Data System Concept Proposal, at 2 *available at* <https://www.finra.org/web/groups/industry/@ip/@reg/@notice/documents/noticecomments/p437017.pdf>.

<sup>13</sup> Exchange Act Release No. 34-67457 at 127.

<sup>14</sup> *Id.* at 3.

<sup>15</sup> *Id.* at 3.

difficult to see how a phased approach would do much to lift the burden on smaller firms, which would, after all, still have to update or rebuild their systems to comply.

Moreover, CARDS could prove to be a significant obstacle for firms to overcome in the day-to-day conduct of their business affairs. Currently, FINRA examines a given firm's records essentially "as is," with only slight modifications necessary for certain examination submissions (such as the Branch Office Risk Assessment Matrix). With CARDS, by contrast, "standardization" means, essentially, that members are tasked with redesigning their books and records systems to accommodate FINRA. Yet, the design that suits the CARDS system is not necessarily the design that best supports members' providing aid and services to clients. The intrusiveness of the standardization requirement is thus much greater than it might appear, as standardization could greatly impair client service.

#### Cost-Benefit Analysis in Light of Existing Systems

FINRA would impose the enormous costs necessary to render members' systems CARDS-compliant after the industry has already updated or built systems to comply with INSITE, the Blue Sheets System, the Trade Reporting and Compliance Engine ("TRACE"), the Order Audit Trail System ("OATS"), ACT, and Large Trader Identification, and immediately before the industry will have to shoulder the costs of making their systems compliant with CAT, a very similar system. In light of all of these systems that provide data to regulators, FINRA should provide a detailed explanation of the role it envisions for CARDS and how its implementation will affect and be affected by these other systems. FINRA should also consider the expenses that members already have borne in complying with these myriad requirements. Moreover, FINRA should lay out its justification for the expense of CARDS in light of the upcoming expenses associated with building, implementing, and maintaining CAT.

These concerns bolster FSR's belief that FINRA should engage in the full rulemaking process. FSR understands the need for effective regulation. But it cannot be the case that all of these existing data collection systems need to be supplemented or supplanted a short time before CAT is implemented.

#### Burden on Inter-Firm Relationships

FSR is also concerned that FINRA may be overlooking CARDS's likely impact on clearing firm-introducing firm relationships. According to Regulatory Notice 13-42, "introducing firms would be required to provide their clearing firms with specified information they control so that clearing firms can provide this information in conjunction with other information the clearing firm provides."<sup>16</sup> In addition to the added

---

<sup>16</sup> Regulatory Notice 13-42 at 2.

expense on introducing firms (which FINRA does not address in its cost estimates), clearing firms are likely to pass the cost of CARDS onto their introducing brokers, subjecting the entire industry and, as a result, its clients, to even higher costs. In other words, CARDS will likely impose costs on clients and a double burden on brokers: first in having to build and maintain CARDS-compliant systems, and second in having to pay increased costs to clearing firms passing on their CARDS-associated expenses. These costs are likely to be high, because clearing firms do not typically hold, have custody of or transact in certain of the products about which CARDS would demand information. For example, clearing firms generally do not have information concerning direct mutual funds investments, direct participation programs, private placements, or any other products offered on a subscription basis from the issuer.

Moreover, FSR is concerned that CARDS could create broad new responsibilities for clearing firms under FINRA Rule 2111's "suitability" requirements.<sup>17</sup> Currently, FINRA Rule 2111, with a few exceptions, requires brokers to conduct their suitability analyses only with respect to information that customers have provided to them. Since clearing firms have much more limited information about customers than introducing firms do, clearing firms' suitability burdens are concordantly lighter. Under CARDS, by contrast, clearing firms would have much more information. Hence, it seems likely clearing firms would be required to conduct far more expansive suitability analyses, something they are not institutionally suited to do, and a task always allocated to the introducing broker, who has the direct client relationship. Thus, FSR recommends that CARDS, if adopted, include an appropriate limitation on clearing firms' suitability responsibilities under FINRA Rule 2111.

#### Costs Related to More Frequent Inquiries and Examinations

Our members are happy to cooperate with regulators and are determined to end bad practices and fix mistakes. FSR members expend considerable resources on their compliance functions and, as noted above, have already dedicated substantial personnel and other resources to plan, design, test, and implement a variety of regulatory compliance systems.

FSR is concerned that CARDS will result in a huge influx of new regulatory inquiries and in longer examinations as FINRA personnel pour over the CARDS data, resulting in a significant increase in work and expense for members to satisfy FINRA personnel that perceived improprieties do not exist. Moreover, FINRA's access to such a large volume of information could lead to a massive and rapid expansion of its supervisory reach. Although the likely escalation of inquiries to firms would enable FINRA to demonstrate that it was taking a close look at all the data at its disposal if a perceived market or regulator failure occurred, the industry simply will not be able to

---

<sup>17</sup> FINRA Rule 2111.

keep up with the additional demands on finite resources. However, FINRA does not consider these additional costs in assessing CARDS.

### Costs Related to Minor Reporting Errors

FINRA members must already comply with the demands of a plethora of systems, from OATS to TRACE to INSITE. Members must dedicate substantial resources to ensuring that data submissions are perfect, since members are fined for incorrect data submissions or formatting.<sup>18</sup> CARDS potentially represents another program in which syntactical or other immaterial mistakes in data submission or formatting would lead to firms' incurring large fines despite their best efforts. Hence, FSR suggests that, should FINRA adopt CARDS, it include a provision eliminating fines for data submissions that contain substantially all of the information CARDS demands and are substantially in the format CARDS requires.

### **Substantial Overlap with the Consolidated Audit Trail**

FSR believes that substantial overlap between CARDS and the Commission's recently adopted CAT rule militates strongly against adopting CARDS. While members are still waiting to hear what the self-regulatory organizations will require of them with respect to CAT, it appears likely, given the similarity of the information CARDS and the CAT rule call for, that CARDS will be largely duplicative of CAT.

### Areas of Overlap between CARDS and the Consolidated Audit Trail

There are a number of areas in which it appears likely CARDS and CAT will overlap. First, CARDS would require firms to submit customer-identifying and account-identifying information.<sup>19</sup> CAT's requirement to submit information about each "reportable event"<sup>20</sup> (defined capaciously) includes a customer identification along with "information of sufficient detail to identify the customer and customer account

---

<sup>18</sup> See, e.g., Disciplinary and Other FINRA Actions, Reported for January 2013, available at <http://www.finra.org/web/groups/industry/@ip/@enf/@da/documents/disciplinaryactions/p197674.pdf>. (discussing situations in which firms were fined for syntax or other minor errors in their OATS data submissions).

<sup>19</sup> *Id.* at 5. As discussed below, FINRA recently determined that it will not require firms to submit customer name, address or tax identification number. Nevertheless, the proposal still calls for a variety of information from which the customer can be identified.

<sup>20</sup> A "reportable event," under Rule 613(j)(9), includes but is not "limited to the original receipt or origination, modification, cancellation, routing, and execution (in whole or in part) of an order, and receipt of a routed order."



information.”<sup>21</sup> Second, CAT and CARDS both call for the highly detailed reporting of all trading and account activity, including the security that is the subject of an order, the date of each order, a description of the material terms of each order, and any changes made to or modifications of an order.<sup>22</sup> Third, both programs call for the identification of the brokers involved in each order.<sup>23</sup> These examples do not exhaust the list of areas in which CARDS and CAT overlap,<sup>24</sup> and the duplicative nature of CARDS is even more apparent in light of the fact that FINRA will have access, for surveillance and regulatory purposes, to the information stored in the CAT repository.<sup>25</sup> Such access will include the ability to conduct searches and generate reports.<sup>26</sup> It is far from clear why the CAT repository data are insufficient for FINRA’s purposes, and FINRA does not explain in Regulatory Notice 13-42 why CAT’s coverage of any particular area or CAT’s coverage *in toto* is inadequate.

To implement CARDS would appear inconsistent with the Commission’s policy mandating the elimination of rules and systems that CAT renders duplicative.<sup>27</sup> Accordingly, FSR urges FINRA to reconsider CARDS. As discussed above, FINRA should engage in a full rulemaking so that it can demonstrate that CARDS is necessary in light of CAT (and the various other systems mentioned above).

---

<sup>21</sup> Exchange Act Release No. 34-67457 at 339.

<sup>22</sup> *Id.* at 336-7, 339. *See also* the definition of “reportable event” in footnote 21, above.

<sup>23</sup> Regulatory Notice 13-42 at 5; Exchange Act Release No. 34-67457 (May 26, 2010) at 338- 339.

<sup>24</sup> *See* Regulatory Notice 13-42, at 5 and Exchange Act Release No. 34-67457 (May 26, 2010), at 340. (both calling for the storage of data in a standardized format); *see also* Rule 613(c)(3) (calling, as in CARDS, for the regular, periodic submission or required data: under the CAT rule, each member and each self-regulatory organization must collect and provider order event data to the central repository by 8:00 AM Eastern Time on the trading day following the day such information has been recorded by the member or self-regulatory organization).

<sup>25</sup> Exchange Act Release No. 34-67457 at 341 (stating that “All plan sponsors and their employees, as well as all employees of the central repository, agree to use appropriate safeguards to ensure the confidentiality of such data and agree not to use such data for any purpose other than surveillance and regulatory purposes”).

<sup>26</sup> Rule 613(e)(3).

<sup>27</sup> *See* Exchange Act Release No. 34-67457 at 12.

## Privacy and Privacy Law Concerns

Given widespread public concern about governmental and private entities' collection and use of individuals' data,<sup>28</sup> a program, like CARDS, designed to collect far-ranging financial and personally identifying data is likely to drive many members' clients away from the investment market. Indeed, since clients have many options concerning how to invest their money (from registered investment advisers and mutual funds to bank products) they are especially likely to eschew broker-dealers in favor of market participants whose regulators do not collect and review such an extensive amount of personal data.

Equally problematic, state and foreign privacy laws might well make it illegal for members to collect the information CARDS demands. Thus, some members may be incapable of complying with CARDS.<sup>29</sup> Many European Union nations, for example, have strict prohibitions on the circumstances under which financial information may be disclosed to foreign entities.<sup>30</sup> Analogously, attempts by broker-dealers to comply with their social media-monitoring obligations led to great industry confusion regarding the conflict between the social media rules and state privacy laws.<sup>31</sup> Even in cases where FINRA rules preempt state privacy laws or foreign laws are technically inapplicable, CARDS could create a regulatory maze, leaving broker-dealers perpetually uncertain as to how they will comply with actually or ostensibly conflicting legal requirements and regimes, raising compliance costs, and subjecting firms to new, expensive legal

---

<sup>28</sup> See, e.g., The Republican Newsroom, *Poll: 57% fear U.S. government will use NSA data to harass political opponents* (Jun 14, 2013, 11:59 PM), [http://www.masslive.com/politics/index.ssf/2013/06/poll\\_57\\_fear\\_us\\_government\\_wil.html](http://www.masslive.com/politics/index.ssf/2013/06/poll_57_fear_us_government_wil.html) (citing a Rasmussen poll indicating widespread fear that government-collected data will be used for punitive political purposes).

<sup>29</sup> *C.f.* Comment Letter of the European Banking Federation and the Swiss Bankers Association on the Proposed Large Trader Reporting System, available at <http://www.sec.gov/comments/s7-10-10/s71010-92.pdf>. (explaining how the conflict between the Commission's large trader reporting system requirements and the requirements of non-U.S. privacy laws makes simultaneous compliance impossible).

<sup>30</sup> *C.f.* Robert S. Ladd, *Swiss Miss: The Future of Banking Secrecy Laws in Light of Recent Changes in the Swiss System and International Attitudes*, 20 *Transnat'l L. & Contemp. Probs.* 539 (2011-2012) (2009) (discussing the Swiss banking secrecy laws and the difficulty of getting financial information out of Switzerland).

<sup>31</sup> See, e.g., Scott E. Rahn and Michael Lawrence, *California Declines FINRA "Friend Request": The Impact of State Social Media Privacy Legislation on Broker-Dealers' Ability to Comply with FINRA Rules*, *Securities Litigation & Enforcement News: Current Legal Developments in the Broker-Dealer Arena* (Nov. 16, 2012), available at <http://www.gtlaw.com/News-Events/Publications/Alerts/165600/California-Declines-FINRA-Friend-Request-The-Impact-of-State-Social-Media-Privacy-Legislation-on-Broker-Dealers-Ability-to-Comply-with-FINRA-Rules>.

challenges. Increased compliance complexity could prove especially burdensome for smaller firms, raising barriers to entry, creating an uneven playing field and damaging competition to the detriment of consumers.<sup>32</sup>

In light of these considerations, FSR recommends that FINRA provide a safe harbor from any requirement to collect or furnish data or other customer information when a firm reasonably believes that doing so could violate state or foreign privacy or data disclosure laws.

Moreover, FSR is concerned that CARDS could violate broader governmental policy objectives concerning data privacy. For example, CARDS would seem to conflict with the Privacy Act of 1974,<sup>33</sup> designed to remediate “potential abuses presented by the government’s increasing use of computers to store and retrieve personal data by means of a universal identifier.<sup>34</sup>” Since FINRA is a quasi-governmental entity,<sup>35</sup> it should eliminate the customer identification submission requirements of CARDS to the extent it has not already done so in its update (discussed below) and adopt the practices for data recording, maintenance, and disclosure outlined in the Department of Justice’s overview of the Privacy Act.<sup>36</sup>

## Data Security Concerns

The public also has heightened concerns regarding the data security measures taken by governmental entities and private companies that house their personal information.<sup>37</sup> FINRA should provide greater detail regarding the “current and effective

---

<sup>32</sup> *C.f.* Juliet Chung, *Compliance Costs Rise at Hedge Funds* (Oct. 17, 2013, 7:39 AM), <http://blogs.wsj.com/moneybeat/2013/10/17/compliance-costs-rise-at-hedge-funds/> (noting that rising compliance costs for hedge funds and an increasing regulatory complexity are raising barriers to entry burdening smaller participants in the hedge fund industry).

<sup>33</sup> 5 U.S.C. §552 a.

<sup>34</sup> *Overview of the Privacy Act of 1974*, 2012 ed., DEPT of JUSTICE., (Dec. 2012), <http://www.justice.gov/opcl/1974privacyact-2012.pdf>, 4.

<sup>35</sup> *Standard Inv. Chartered, Inc. v. Nat’l Ass’n. of Sec. Dealers*, 637 F.3d 112 (2nd Cir. 2011) (stating that the National Association of Securities Dealers, FINRA’s predecessor, is a “quasi-governmental” organization).

<sup>36</sup> *Overview of the Privacy Act of 1974*, 2012 ed., DEPT of JUSTICE., (Dec. 2012), <http://www.justice.gov/opcl/1974privacyact-2012.pdf>.

<sup>37</sup> *See, e.g.*, Brian Fung, *The bright side to the Target Hack? It’s getting Congress moving*. (Jan 10, 2014, 3:36 PM), <http://www.washingtonpost.com/blogs/the-switch/wp/2014/01/10/the-bright-side-to-the-target-hack-its-getting-congress-moving> (discussing possible Congressional action in the wake of revelations concerning Target systems being hacked); *see also* Devin Dwyer, *Exclusive: Security*

information security methods” it intends to employ to protect account-identifying information.<sup>38</sup> FINRA also should provide more information about who will monitor security protocols and systems to protect against hacking and other unauthorized access or use of the system and the data stored on it. FSR urges that, at a minimum, FINRA implement “information barriers” between regulatory and non-regulatory staff, similar to those mentioned in rule 613(e)(4)(i)(B)(1) under the Exchange Act (implementing CAT), as well as measures to prevent regulatory employee abuse of access to information. FINRA also should ensure that its data security measures at a minimum meet the standards outlined in the National Institute of Standards and Technology’s *Framework for Improving Critical Infrastructure Cybersecurity*.<sup>39</sup> Further, in order to reassure the investing public, FINRA should undertake a campaign to educate consumers about its collection and use of data.

However, even these measures are unlikely to be sufficient. Given the increasing sophistication of computer hackers (including state-sponsored actors<sup>40</sup>), the difficulty of ensuring that systems are truly safe, and the mere presence of enormous amounts of financial data likely to present an attractive target,<sup>41</sup> FSR recommends FINRA not adopt

---

*Risks Seen at HealthCare.gov Ahead of Sign-Up Deadline.* (Dec 20, 2013, 6:36 AM), <http://abcnews.go.com/blogs/politics/2013/12/exclusive-security-risks-seen-at-healthcare-gov-ahead-of-sign-up-deadline/> (discussing unanticipated security concerns arising in the context of implementation of the Affordable Care Act computer systems).

<sup>38</sup> Regulatory Notice 13-42 at 6.

<sup>39</sup> National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2014), <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf>.

<sup>40</sup> See, e.g. Edward Wong, *Hacking U.S. Secrets, China Pushes for Drones*, N. Y. Times, Sep. 20, 2013 at A1, available at [http://www.nytimes.com/2013/09/21/world/asia/hacking-us-secrets-china-pushes-for-drones.html?\\_r=0](http://www.nytimes.com/2013/09/21/world/asia/hacking-us-secrets-china-pushes-for-drones.html?_r=0) (discussing Chinese governmental actors’ attempts to hack secure U.S. systems); see also Executive Order no. 13636, *Improving Critical Infrastructure Cybersecurity*, DCPD-201300091 (Feb. 12, 2013) (discussing, *inter alia*, the need for “improved cybersecurity” to protect the “economic security” of the United States in light of the growing “cyber threat to critical infrastructure”).

<sup>41</sup> Exchange Act Release No. 34-67457 (May 26, 2010), n. 357 (quoting a comment letter regarding the consolidated audit trail stating that “Although the SEC has a strong record of protecting investor privacy, the very presence of potentially billions of unique customer identifiers tied to personal information in a central repository would create a substantial risk of misuse and identity theft”); see also Ken Dilanian, *Several cybersecurity initiatives lost after Snowden’s NSA leaks.*, L.A. Times (Feb. 1, 2014, 6:51 PM), <http://www.latimes.com/nation/la-na-snowden-cyber-20140202,0,5845248.story#axzz2sH4wRrMD/> (noting that U.S. entities have found it enormously difficult to thwart the “daily onslaught” of hacking attempts aimed at stealing Americans’ financial data from banks, telecommunications systems, and other institutions).

CARDS in its current form. FINRA’s own discussion of its examination priorities notes the increase in the “frequency and sophistication” of cyber-attacks on the “nation’s largest financial institutions,” aimed at stealing “sensitive customer data.”<sup>42</sup> For the reasons outlined above, FSR believes that CARDS is likely to undermine client data security, and hence FINRA (and Commission<sup>43</sup>) cybersecurity goals.

Even if data could be secured, the mere perception that sensitive financial information could be leaked, abused, or misappropriated is likely to undermine investor confidence, while subjecting firms to liability to their customers if there is a data breach. Clients concerned about data security (like those concerned about data privacy) might well choose to take their business away from broker-dealers and give it to other market participants (such as registered investment advisors) with whom they believe their data to be more secure. FSR is concerned about the reputational damage that the industry would suffer and the customer claims and complaints that would arise from a FINRA data security breach. Perhaps as part of the CARDS rulemaking, FINRA will consider indemnifying its members.

Given the data security concerns outlined above, FINRA should use existing or already contemplated systems (like INSITE or the Commission’s CAT repository) to avoid creating a new repository of highly sensitive information attractive to hackers<sup>44</sup> or other unscrupulous actors or otherwise susceptible to inadvertent disclosure.

### Gramm-Leach-Bliley

If CARDS were implemented as described in the Concept Proposal, we believe it would severely undermine the aims of Title V of the Gramm-Leach-Bliley Act (“GLB”) (implemented with respect to broker-dealers by Regulation S-P).<sup>45</sup> GLB mandates widespread restrictions on a financial institution’s power to disclose personal information

---

<sup>42</sup> Letter from FINRA on FINRA’s 2014 Regulatory and Examination Priorities (Jan. 2, 2014), *available at* <http://www.finra.org/web/groups/industry/@ip/@reg/@guide/documents/industry/p419710.pdf>.

<sup>43</sup> *See, e.g.* National Exam Program Office of Compliance Inspections and Examinations, Examination Priorities for 2014 (Jan 9, 2014), *available at* <http://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2014.pdf> (“The [Commission] staff will focus on... information leakage and cyber security.”).

<sup>44</sup> *C.f.* Tom Foremski, *How secure are the National Security Agency spy lines?* ZDNET, (Jun. 12, 2013, 10:19 PM), <http://www.zdnet.com/how-secure-are-the-national-security-agency-spy-lines-7000016752/> (arguing that increasing centralization of sensitive data facilitates hacker theft of those data).

<sup>45</sup> 17 C.F.R. Part 248 *et seq.*

about consumers, in part in order to “protect the security and confidentiality of those customers’ nonpublic personal information.”<sup>46</sup> Though FINRA is not subject to the confidentiality and privacy requirements of GLB, for FINRA to create a new centralized system for gathering financial and other personal data undermines one of GLB’s central purposes, *viz.* the protection of members’ clients’ data.

#### FINRA Update of March 4, 2014

On March 4, 2014, FINRA updated Regulatory Notice 13-42 to revise the CARDS proposal such that CARDS would no longer require firms to submit account names, addresses or tax identification numbers (the “Update”).<sup>47</sup> FSR believes this narrowing is an appropriate step and appreciates FINRA’s decision in this regard. Nevertheless, FSR does not believe that the Update significantly alters the privacy and data security concerns raised by the CARDS proposal. For example, FINRA would still require firms to submit a variety of sensitive information about customers, including age, investment objective(s), net worth, and risk tolerances, as well as detailed information about each customer’s trading activity. Merely omitting name, address, and tax identification number does not make any less private these other data points. Nor does it explain how FINRA will seek to prevent an unscrupulous actor from accessing the information and from piecing together data to identify a particular investor. FSR continues to urge FINRA to address these issues during the notice-and-comment rulemaking process so that customers and the industry will understand how their private information will be protected.

#### **Use of Information by FINRA**

It is unclear from Regulatory Notice 13-42 whether FINRA conceives of CARDS as a collaborative or enforcement-oriented mechanism. More specifically, if FINRA detects a suspicious pattern or “red flag,” will FINRA notify the relevant broker-dealer so that the broker-dealer can collaborate with FINRA to address the problem, or will FINRA simply take enforcement action against the broker-dealer? Clarification on this point would be helpful.

FSR believes it would be appropriate for FINRA to take a collaborative approach and put faith in the supervisors, as well as compliance and legal personnel, of members to address issues FINRA detects through CARDS. Firms have dedicated substantial

---

<sup>46</sup> 15 U.S.C. §6801(a).

<sup>47</sup> *Update Regarding Regulatory Notice 13-42 – Comprehensive Automated Data System*, FINRA, (Mar. 4, 2014), available at <http://www.finra.org/Industry/Regulation/Notices/2013/P451243>.

resources<sup>48</sup> to fulfill their regulatory obligations. To implement CARDS solely as a punitively-oriented enforcement mechanism would be to fail to leverage the substantial compliance resources that firms have created at great expense and which could be used to address in a more timely fashion specific market abuses detected through CARDS.

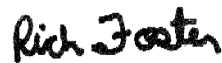
## Conclusion

Given the concerns identified in this letter, FSR respectfully submits that FINRA not implement CARDS without substantial revisions consistent with the analysis presented above. If FINRA moves forward with CARDS, FSR believes it should do so only via notice-and-comment to allow for Commission approval and to provide FSR and other interested parties with the opportunity to comment on the details of the program.

\* \* \*

FSR appreciates the opportunity to submit comments on FINRA's proposed Comprehensive Automated Risk Data System. If it would be helpful to discuss FSR's specific comments or general views on this issue, please contact me at [Richard.Foster@FSRoundtable.org](mailto:Richard.Foster@FSRoundtable.org).

Sincerely yours,



Richard Foster  
Vice President & Senior Counsel  
For Legal and Regulatory Affairs

Financial Services Roundtable

---

<sup>48</sup> See David McClellan, Broker-Dealer Sales Practices Oversight 2012 Study Updated, ALBRIDGE, (Sep. 17, 2012), [http://www.albridge.com/why\\_albridge/industry\\_perspectives/broker-dearler-sales-practices-oversite-2010-study-update.html](http://www.albridge.com/why_albridge/industry_perspectives/broker-dearler-sales-practices-oversite-2010-study-update.html) (noting that 86% of firms spend up to 10% of their overall revenue on compliance-related expenses, and that 14% spend up to 20%).