



Ronald J. Kruszewski
Chairman and Chief Executive Officer
(314) 342-2155
ronk@stifel.com

December 1, 2014

By Electronic Mail (pubcom@finra.org)

Ms. Marcia E. Asquith
Office of the Corporate Secretary
FINRA
1735 K Street, N.W.
Washington, DC 2006-1506

Re: Regulatory Notice 14-37 – FINRA Requests Comment on a Rule Proposal to Implement the Comprehensive Automated Risk Data System (“CARDS”)

Dear Ms. Asquith:

As Chairman and Chief Executive Officer of Stifel Financial Corp., I appreciate the opportunity the Financial Industry Regulatory Authority (“FINRA”) has given me, and other interested parties throughout the industry, to comment upon your new proposed Comprehensive Automated Risk Data System (“CARDS”) Rule.

Background of Stifel

As you may be aware, Stifel Financial Corp. is a financial services holding company headquartered in St. Louis, Missouri, that conducts its banking, securities, and financial services business through several wholly owned subsidiaries. Stifel’s broker-dealer clients are served in the United States through Stifel, Nicolaus & Company, Incorporated; Keefe, Bruyette & Woods, Inc.; Miller Buckfire & Co., LLC; and Century Securities Associates, Inc. and in the United Kingdom and Europe through Stifel Nicolaus Europe Limited and Keefe, Bruyette & Woods Limited. The Company’s broker-dealer affiliates provide securities brokerage, investment banking, trading, investment advisory, and related financial services to individual investors, professional money managers, businesses, and municipalities. Stifel Financial’s largest operating subsidiary is Stifel, Nicolaus & Company, Incorporated, a full-service broker-dealer with over 2,000 registered representatives in more than 300 branches in 45 states with over \$175 billion in client assets under management. Of utmost concern to us is any proposed rule that would create unnecessary costs and potentially compromise individual client privacy without a corresponding meaningful benefit and, as an unintended consequence, create negative goodwill among both our clients and the securities industry. CARDS is such a rule.

Background of CARDS

FINRA describes its proposed 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 The stated objectives of CARDS are: (1) understanding the business profile of a firm; (2) tracking product mixes across firms; (3) identifying the firms that consistently sell products with higher risk; (4) understanding the overall risk profile of a firm; (5) identifying patterns of transactions that include bad behavior; and (6) identifying potentially suspicious activity in individual accounts that may call into question the adequacy of a firm’s anti-money laundering program².

CARDS Is an Unnecessary and Costly Burden Given Stated Objectives

I believe that the first four of CARDS’ stated objectives can be achieved with data currently supplied on an aggregate basis to FINRA or data that will be available through the SEC’s Consolidated Audit Trail initiative (“CAT”). There exists no need to supply individual client positions and money flows, on a monthly basis, in order for FINRA to understand a firm’s business or risk profile, track product mixes, or identify firms that consistently sell products with higher risk. A relatively simple review of a firm’s aggregate stock record and transaction blotters, compared with the prior year, provides the information required to meet these first four objectives.

The remaining two stated goals of CARDS (identifying patterns of transactions that include bad behavior and identifying potentially suspicious activity in individual accounts that may call into question the adequacy of a firm’s anti-money laundering program), while having seemingly obvious benefit, in fact represent an additional and unnecessary cost given the fact that these objectives are the primary supervisory responsibility of the broker-dealer, not FINRA. Stated another way, these objectives place FINRA squarely in the role of supervisor, and not overseer of those who supervise. In effect, FINRA will no longer be auditing the adequacy of a firm’s supervisory system but rather imposing its vision of what a proper supervisory system should be. Yet FINRA will be exercising this authority without the benefit of myriad subjective information that only a firm, and its employees, would know through its direct and personal contact with its clients. Of course, it is equally obvious that this will create an additional layer of costs without any obvious incremental benefit.

Privacy Concerns

It should be readily apparent that the stated objectives of CARDS can be and are currently met through other means. However, any marginal benefit that may be derived from CARDS must be weighed against the substantial individual privacy concerns that will be created through the establishment of a centralized database of client positions and money flows.

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

² Regulatory Notice 14-37 “Comprehensive Automated Risk Data System” p. 3 – 4

While FINRA believes it has addressed this concern through eliminating the need for firms to supply one or two personally identifiable information (“PII”) data points from its mandatory data submissions, the fact remains that individual privacy can, and most likely will, be compromised. Simply, there can be no assurance that a particularly talented hacker (or governmental agency) wouldn’t be able to ascertain the identity of the individual based on the other unique information still being sought (age, marital status, branch location, etc.). FINRA has also failed to address the very real concern that third parties could use the courts to access this data from FINRA for unintended purposes, including civil litigation.

The Securities Industry and Financial Markets Association (“SIFMA”) retained IBM to consult with it on this very topic (IBM’s report will be submitted with the SIFMA comment letter), and in it you will see several very plausible “re-engineering” scenarios in which potential bad actors could back their way into the identities of our clients and use the data supplied to FINRA to harm them. In one scenario, FINRA’s other databases containing PII, such as the Automated Exam Program (AEP), are also compromised, resulting in a “re-identification” of a firm’s client base. These are not outlandish hypothetical events, but real potential threats. The confidential client data of any one firm is an attractive target for would-be hackers. Consolidating the confidential client data of the entire securities industry in a single database creates an irresistible target and creates a risk which is not justified by the potential regulatory benefits.

Clients look to firms like ours to protect the integrity and confidentiality of the information they entrust to us. They expect us to do everything in our power to ensure that their confidential information is not improperly accessed or used in any unintended manner. CARDS limits our ability to protect our clients’ data, yet makes no express provision for the data’s protection by FINRA. And of course, should a data breach occur during transmission to or while at FINRA, there is a substantial risk that our clients will look to hold us liable for such breach. The CARDS proposal makes no provisions for indemnifying firms such as Stifel under such circumstances.

No Cost/Benefit Justification for CARDS

As you are aware, FINRA is obligated to perform and publicly share a complete and final cost/benefit analysis of CARDS before any proposal is filed with the SEC. It must also allow time for members to comment on such analysis before filing. While FINRA believes that CARDS would “serve to reduce the burdens on firms and lower costs”³ by “eliminating intermittent and sometimes frequent and extensive information requests,” it has done no comprehensive cost/benefit analysis that would support that position.

In addition to IBM’s re-identification analysis, SIFMA also retained IBM to do a cost analysis. IBM’s report, based on a broader range of sample firms than FINRA’s own analysis and more in-depth analysis of the ancillary costs associated with this proposal, concludes that the true costs of both creating this database and supplying it with information regularly will be several times what FINRA projects. For a firm such as Stifel, the CARDS proposal, if enacted, will result in millions more in

³ Regulatory Notice 14-37 “Comprehensive Automated Risk Data System” p. 4

annual costs. The IBM industry-wide estimate for implementing Phase 1 of CARDS and maintaining it annually is a staggering \$680 million and \$360 million, respectively⁴. My experience in these matters suggests that the costs will far exceed initial estimates due to the complexity of the overall program including architecture, data movement, security, storage, and personnel challenges. These costs are to be incurred without any formal analysis of the benefits to be derived from such expenditures.

The securities industry understands the severity of cyber threats and is spending hundreds of millions of dollars to secure, protect, mask and effectively isolate sensitive data. The very idea of establishing a broad central repository of confidential information moves in the exact opposite direction. Proceeding without an extensive analysis of security defies the foundational principles behind sound Data Governance advocated by well-known standards bodies including NIST and COBIT. We should not ignore these risks.

Client Surveys

In addition to the substantial privacy concerns and lack of any justifiable cost/benefit analysis, it is also clear that clients do not support the sharing or transmission of their personal trade data, account holdings, money flows, investment objectives, etc. with anyone, including the government or a quasi-governmental regulatory organization such as FINRA. I am not swayed by FINRA's survey, which asked if respondents either "Strongly Agree, Agree, Disagree or Strongly Disagree" with the following question:

"Would you support the introduction of additional regulatory protections to further safeguard investors from misconduct by brokers or brokerage firms?"⁵

Most respondents, including me, would either "Agree or Strongly Agree" with this question. However, I have conducted an admittedly unscientific "straw poll" of a cross-section of our retail client base, and have discovered (not surprisingly) that the vast majority of our clients object to the sharing of their individual account information and activity. In fact, when the following question was posed after FINRA's survey question above, the results were overwhelmingly "Strongly Disagree or Disagree":

"In order to achieve the additional regulatory protections to further safeguard investors, do you support the sharing of your individual account information, including positions, activity, and money flows to the Government or quasi-government agency?"

We are in the process of conducting a more comprehensive survey of a representative cross-section of our client base and will compile the results within a few weeks. Our clients' concerns, however, are

⁴ IBM CARDS Cost Analysis Report, December 1, 2014 p. 1

⁵ FINRA Investor Survey

understandable and well founded, in light of the cybersecurity threats posed both within the government and private sector.

Conclusion

In conclusion, I submit that this proposed rule, while well intentioned, is ill conceived for the following reasons:

1. It adds minimal, if any, additional protection to clients that enhancing the current firm reporting requirements, such as AEP, INSITE, and CAT, couldn't accomplish.
2. It presents serious privacy concerns for the entire universe of retail clients serviced by FINRA members.
3. No formal cost/benefit analysis as required by regulation has been done, and no perceived benefit could possibly justify the estimated \$1 billion in start-up and first-year costs of the CARDS proposal.
4. The idea which CARDS espouses, a centralized repository of confidential information, is at complete odds with the steps the securities industry is taking to deal with cyber risks.
5. Importantly, it is opposed by the very clients it is supposedly seeking to protect.

I urge you to reconsider this overly intrusive proposal and work with member firms to enhance the current regulatory reporting regime to achieve the worthwhile goals you seek.

Yours truly,

