WASHINGTON
LEGISLATIVE OFFICE

December 3, 2014

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

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

AMERICAN CIVIL LIBERTIES UNION
WASHINGTON
LEGISLATIVE OFFICE
915 15th STREET, NW, 6TH FL
WASHINGTON, DC 20005
T/202.544.1681
F/202.546.0738
WWW.ACLU.ORG

LAURA W. MURPHY
DIRECTOR

NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500

OFFICERS AND DIRECTORS
SUSAN N. HERMAN
PRESIDENT

ANTHONY D. ROMERO
EXECUTIVE DIRECTOR

ROBERT REMAR
TREASURER

Dear Ms. Asquith:

We write to express our continued concern with the CARDS rule proposal (the "Notice"),[1] which, despite assurances that this massive repository of millions of Americans' most sensitive financial information will be safe from breach, we fear continues to present very serious security and privacy concerns.

While we appreciate FINRA's role in monitoring and policing brokers and investment firms, we urge you to address these continuing privacy concerns in any final CARDS proposal and to delay implementation of the system until these issues are resolved.

We briefly address three issues below.

First, we suggest that the increased harm by a breach in such a centralized database requires FINRA to recalibrate the risk-reward calculus, even if, which we do not concede, the risk of breach is "remote."[2] Second, we note the privacy threats inherent in the CARDS database even without the collection of personally identifiable information ("PII"). Third, we reiterate our concern that the CARDS database could be used or misused as another means by which the government could engage in mass surveillance of Americans' activities, similar to the bulk telephone metadata collection program revealed by Edward Snowden, which also does not collect PII but nonetheless poses awesome privacy risks.

---

1 Request for Comment on a Rule Proposal to Implement the Comprehensive Automated Risk Data System, Regulatory Notice 14-37 (Sept. 2014).

2 *Id.* at 6.

1. "Big Data" Presents Privacy Risks that Are Different in Scope and Kind than the Piecemeal Collection In Which FINRA Currently Engages

The Notice states 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."[3] Further, it says that FINRA "has been maintaining high security standards and safely hosting highly confidential broker data for decades," without any specificity about which standards would be applied to this new database.

As we have documented in the context of the mass telephone surveillance program revealed by Edward Snowden, privacy risks increase significantly in the content of "bulk" (i.e., indiscriminate and wholesale) collection and centralization of information.[4] The larger the universe of data collected, the more revelatory the data—irrespective of whether it includes PII. And, as we note below, the more valuable the data, the greater the incentive for cybercriminals and others to acquire it.

Accordingly, the proposal to collect, en masse, virtually all transactional records from entities regulated by FINRA and store them in a central repository for an indeterminate period of time raises privacy concerns different in scope and kind than those posed by the information already collected by FINRA. While FINRA may have had a laudable security record in the past, the bulk financial database proposed in CARDS limits the comfort one can take from a mere continuation of current practices.

Additionally, the costs of a CARDS breach would be more dire than a breach of current databases. Because the information here is centralized and collected in bulk, it would allow an attacker far more detailed information about individual investors' investment practices, risk tolerances, general financial health and a myriad of other sensitive details. FINRA needs to take this added risk into account when determining whether the benefit in fraud prevention outweighs this novel risk to personal financial privacy.

Finally, as noted, the added risk to privacy inherent in a centralized CARDS database will translate into a greater threat of breach. In other words, the fact this database will be far more revelatory of personal financial information than the data already collected by CARDS—it will be a "honeypot"—means that potential criminals will have a much greater incentive to exploit it. Existing cybersecurity measures currently in place at FINRA may not be able to contend with the added threat.

---

[3] *Id.*

[4] *See* Decl. of Professor Edward Felten, Am. Civil Liberties Union v. Clapper, Case No. 13-cv-03994 (WHP) (S.D.N.Y. filed Aug. 26, 2013), *available at* http://bit.ly/1BaocE0.

2. Simply Removing PII, While Helpful, Is Not Sufficient to Resolve Privacy Concerns in a Database of This Scope and Size

The Notice proposes to collect a significant amount of information under four categories of data. Under "Account Profiles," the Notice would require the transmission of:

- "Information regarding all securities accounts on the books and records of the member firm, such as account classification and registration, and whether the account can transact on margin;

- "Information about the type of persons (i.e., whether a natural person, corporation, partnership, trust or otherwise) associated with a securities account;

- "Information about account servicing representatives; and

- "Information regarding each securities account at the member firm related to know-your-customer and suitability obligations (excluding PII)."

Despite the exclusion of PII, the volume and various datapoints of information thus collected continue to present privacy concerns for two primary reasons.

First, as we noted in our earlier submission in response to Regulatory Notice 13-42, even anonymized datasets can be easily deanonymized when cross-referenced with other data. The larger the number of unique datapoints, the easier such re-identification.

Second, broad surveillance—irrespective of whether it involves the collection of personally identifiable information—implicates core privacy values of great importance to Americans. Americans increasingly feel they have lost control over their personal information and ability to retain confidences in sensitive personal activity, like their finances. Among other things, this sense of a lack of control leads to diminished engagement in civic life, less vigorous political discourse and the consequent reduction in accountability for public officials. Mass surveillance of financial activity has the potential to further this unfortunate trend.

It also poses the same problem as mass surveillance in other contexts. In the context of the mass phone surveillance program, part of the civil liberties concern is that it turns the notion of individualized suspicion—a cornerstone of American notions of privacy and due process—on its head. In effect, the phone program says, "we'll collect all the information and then search it for bad patterns" when the appropriate approach is to only collect the information upon some showing of possible wrongdoing. We fear CARDS would facilitate the same approach.

3. The CARDS Database Could Become a Tool of Government Surveillance

The Notice continues to lack sufficient information on how the database could or would be accessed by other non-government or, especially, government actors. We reiterate our concern that CARDS could be used by government actors, including the Securities and Exchange

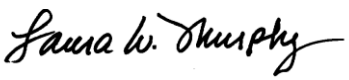
Commission, to generate leads for law enforcement purposes or, just as troublingly, for foreign intelligence gathering.

* * *

In sum, we urge FINRA to delay implementation of the CARDS system until these and other essential questions concerning privacy and civil liberties can be answered satisfactorily. We applaud FINRA's role in protecting investors and markets, but that role must not imperil core American values of privacy and due process.

Please do not hesitate to contact Legislative Counsel/Policy Advisor Gabe Rottman at 202-675-2325 or grottman@aclu.org if you have any questions or comments.

Sincerely,



Laura W. Murphy
Director, Washington Legislative Office

Gabriel Rottman
Legislative Counsel/Policy Advisor