October 12, 2018

Jennifer Piorko Mitchell
Office of the Corporate Secretary
FINRA 1735 K Street, NW
Washington, DC 20006-1506

Re: FINRA's Special Notice 7/30/18 request for comments regarding Financial Technology Innovation in the Broker-Dealer Industry

Dear Ms. Piorko Mitchell,

Hearsay Systems, Inc. ("Hearsay") appreciates the opportunity to submit this letter in response to the request for comments by the Financial Industry Regulatory Authority ("FINRA") on the future of financial technology innovation. As an industry leader in social media compliance specifically, and electronic communications compliance generally, within the financial services industry over the past decade, Hearsay believes that technology advances such as data aggregation and artificial intelligence, when used responsibly, are necessary tools for broker-dealers to meet the needs of their clients now and in the foreseeable future.

Hearsay is an industry leading technology platform that enables financial professionals to build and deepen relationships with current and prospective clients. Advisors leverage Hearsay's technology to connect with clients through omnichannel communications that provides a full funnel digital experience. Hundreds of thousands of data points provide robust analytics for both the advisors and corporate sales/marketing teams all of which can be automatically fed into enterprise CRM systems. Hearsay has over 150,000 advisors from top global financial services firms leveraging the Hearsay platform to drive business and deliver a personalized client experience. Through social media, email, and text messaging, advisors are able to connect with clients when and where it is convenient for both parties. All the while, compliance teams can supervise and enforce their internal policies, consistent with FINRA's regulatory guidance-- primarily through automation.

Data aggregation is a fundamental piece of the puzzle when it comes to the digital experience. In financial services, data aggregation is critical for consumers. It allows them to have a holistic view of their financial well-being. For the broker-dealer, data aggregation provides endless opportunities to improve and deliver a personalized digital experience for clients. Per FINRA's request for comments on data aggregation we provide the following insights.

Data Aggregation

Recent passage and enforcement of cybersecurity laws relating to the collection, processing and storage of data has made the concept of data aggregation an extremely important topic. While the Special Notice framed this issue within the context of aggregating financial information within a personal financial management (PFM) portal, the same issues and concerns exist within the electronic communications space.

Technology has created new communication channels that allow consumers to connect with their broker-dealer. One study reported that 60% millenials prefer two-way texting with companies because of the ease and speed of communication.[1] Recent articles suggest that communication via Whatsapp and other encrypted communication

[1] *See* https://www.openmarket.com/press/why-millennials-prefer-two-way-texting-with-businesses-infographic/

apps are becoming more popular, allowing more sensitive information to be transmitted on such channels.[2] While FINRA has clearly communicated that any electronics communication channel is subject to supervision per Rule 3110 and compliance oversight as articulated in Rule 2210, these technological trends are important in the context of data aggregation.

As broker-dealers and consumers interact and communicate on a more frequent basis (bank by phone, email alerts, online policy formation, texting with advisors, etc.), there is an increased likelihood that financial data (including personally identifiable information) will be shared on these channels. It is important to think about the methodology of data aggregation and the exploitation of that data, rather than narrowly focusing on PFMs and the user interface to view the aggregated data. In its goal to protect investors, FINRA should take an active role in defining principles and guidance on how member firms can balance the privacy of consumers against regulatory requirements of record keeping.

Legal Risks Associated with Data Aggregation Technology

The Special Notice mentions two basic methodologies of collection of data: scraping (also known as "page scraping") and collection of information via API. While there are other methodologies, data collection via scraping or via API raise the basic question: who should be the ultimate arbiter of determining what type of information may be aggregated?

There is a growing trend within the regulatory world that there be increased transparency and disclosure between data aggregators and consumers regarding the use of personal data. For instance, the General Data Protection Regulation (GDPR) in Europe, among other requirements, vests power within the individual consumer by giving the consumer an ability to request how third parties use personal data, as well as a right of erasure, requesting that third parties delete personal data from their systems. California has passed similar legislation that also gives power to the consumer over his or her data in business-to-consumer transactions.[3] Consumers clearly should have some agency over their personal data.

On the other hand, member firms have a compelling interest in order to protect personal data within their control. For instance, the state of New York has passed recent legislation that compels financial services companies to adopt certain cybersecurity measures, as well as supervise the cybersecurity practices of their vendors, when handling sensitive financial data.[4] Failure to adhere to these laws can result in fines to the member firms and potentially even criminal liability for corporate officers. Member firms are increasingly seeing more and more scrutiny from local, state and federal regulators on their cybersecurity practices and to ensure that personal data of their customers is secure.[5]

Scraping

Scraping can be an effective method to aggregate information that the consumer believes is valuable, independent of the beliefs of the broker-dealer and/or member firm. Using this logic, consumers could grant data aggregators access to their own accounts in order to collect data that the consumer finds valuable.

---

[2] *See* https://www.bloomberg.com/news/articles/2017-03-30/wall-street-s-whatsapp-secret-illegal-texting-is-out-of-control
[3] *See* https://www.nytimes.com/2018/06/28/technology/california-online-privacy-law.html
[4] 23 NYCRR Part 500
[5] *See* CO HB 18-1128, available at

Unfortunately, this benefit is more theoretical than practical. While there may be a contractual agreement between the consumer and aggregator of the scope of collection, functionally once a consumer grants a data aggregator access to the account, the data aggregator has the technological ability to collect any data that it deems relevant without any mechanism for the consumer to stop or restrict such collection.

And even if the data aggregator stays within the contracted boundaries of data collection, data aggregators are unable to guarantee the accuracy of the data collected. Scraping requires a static page, where simple field code changes and user interface modifications may potentially "break" the scraping function, such that the aggregator either can no longer collect the relevant data (e.g., a user interface change moves a critical piece of information to a different area of the page) or the information might be inaccurate (for instance, a field code may change such that the information the page renders may be different than the codes the aggregator maintains). Therefore, scraping cannot produce a consistent predictable outcome that will serve a consumer's best interest.

Scaping also creates a potential hazard for broker-dealers and member firms. With the recent passage of the aforementioned cybersecurity laws, member firms may be held responsible if information that was scraped from their sites is ultimately made public through security flaws or other handling practices of data aggregators. Member firms may be held liable in these scenarios. Even though they were not the proximate cause of the data security breach, the member firm was the original source of information for the breach and may be held responsible for not create adequate safeguards to protect such information. Because member firms do not have any control over the actions and activities of aggregators, member firms retain substantial risk that they may be held liable for the security breaches or impermissible use of financial information of the data aggregator.

Finally, promoting the practice of scraping for the purposes of financial transparency raises serious legal issues. Cases such as *United States v. Nosal*,[6] *Facebook v. Power Ventures, Inc.*,[7] and *hiQ Labs, Inc. v. LinkedIn*[8] all address the issue of whether data aggregators have the legal right to continue to "scrape" and collect data when a website operator has taken measures to prevent such activity. Currently, courts are split on this issue and there is much uncertainty about both the limits of how website operators can limit access to their websites and what forms of scraping (if any) aggregators may use to collect information. Because of this uncertainty, FINRA should not further confuse the situation by either promoting rules or providing guidance on how broker-dealers and member firms should treat scraping by data aggregators.

APIs

While scraping places responsibility within the hands of the data aggregator, APIs allow member firms and custodians of information to determine the manner and method in which they share information to third parties. APIs, unlike scraping, are provided in a much more predictable and structured format. Furthermore, use of APIs require a contractual agreement between the data custodian and the aggregator; the aggregator, in turn, may have a separate agreement with the consumer to set the boundaries of what data may be viewable.

---

[6] United States v. Nosal, 676 F.3d 854 (9th Cir. 2012) (en banc) ("*Nosal I*") and United States v. Nosal, 844 F.3d 1024 (9th Cir. 2016) ("*Nosal II*")

[7] Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058 (9th Cir. 2016)

[8] hiQ Labs, Inc. v. LinkedIn, 2017 WL 3473663 (N.D. Cal. Aug. 14, 2017)

Because of this arrangement, APIs set a clear chain of custody of data ownership throughout the transfer process. This provides assurances to the member firm when handing information to a data aggregator, since there is a defined contractual relationship for how the information will be secured and handled. This would allow member firms to comply with various cybersecurity laws and regulations currently in place; similarly, the consumer will have a predictable pipeline of information available at its disposal.

While it is true that member firms can still heavily restrict the type of information shared in a API model, APIs present a more balanced approach to information sharing than scraping.

Data Aggregation and Compliance

Data aggregation also provides a unique opportunity to further FINRA's general mission of investor protection by allowing more rigorous and thorough compliance.

For instance, member firms are tasked with performance compliance oversight for all retail electronic communication. Member firms can literally comply with this requirement by maintaining records of all electronic communications in a WORM archive, consistent with FINRA and SEC regulations. The benefit of this approach is that member firms can review all communications, message by message or channel by channel, in order to ensure compliance. The downside of this approach, however, is that compliance in this piecemeal format cannot properly scale with current technological innovations and the ever increasing communication touchpoints between broker-dealers and consumers. Whereas fifteen years ago, the broker-dealer/consumer relationship was primarily defined by in-person interaction and mail correspondence, a broker-dealer and consumer can now exchange messages and financial information via social media, email, text message, websites, instant messenger and a host of other technology channels. Analyzing retail consumer communications channel by channel by compliance teams may be sufficient to meet the current rules, but it does not necessarily best advance the general principle of investor protection.

Data aggregation, combined with the use of artificial intelligence, has the ability to solve some of these problems. If a member firm were able to aggregate communications or conversational threads into a single data set, communications can be reviewed in context to better understand the nature and circumstances of the interaction between the broker-dealer and the consumer. When thinking about applying compliance in the context of data aggregation, Hearsay believes applying the principles of "prohibit, prevent and evaluate" help create a richer, more complete form of compliance.

Prohibit & Prevent

Aggregated data can "prohibit and prevent" potential consumer fraud by using the complete context of an interaction to determine the nature of the relationship between the broker-dealer and consumer. For instance, many member firms categorically prohibit the use of the word "guarantee" in retail communications because, absent context, the word "guarantee" may be used to improperly influence a consumer into entering a financial transaction. It is equally as plausible, on the other hand, that the word "guarantee" can be innocuous and does not represent an opportunity for fraud or misrepresentation (for instance, a broker-dealer could simply post on social media that, "I guarantee that attendees of my birthday party will have a good time"). If member firm could use an aggregated data set to evaluate how the word "guarantee" or other similar problematic words were used within the context of a conversation, it might be able to identify specific scenarios or uses where there is a genuine concern to the investor. Close examination

of an aggregated data set can reveal rules or patterns of problematic behavior that require heightened scrutiny. In this way, member firms could then concentrate their compliance efforts on mitigating and addressing those specific scenarios, instead of casting a wide net and looking at every use of the potential troublesome word. Just as data aggregation can create interesting consumer insights, it can also be used to creating interesting compliance insights; as more and more data collected, the accuracy and effectiveness of these compliance-driven automation will inevitably improve and give member firms the opportunity to deploy their compliance resources more efficiently across more channels.

Evaluate

Aggregated data can also be used to "evaluate" the totality of the broker-dealer contact with a consumer. In today's world, it is highly likely that a consumer and broker-dealer could begin a conversation on social media, continue that conversation via text message and finally complete a financial transaction via email. To comply with current rules, a member need only to monitor each channel and ensure that the communications made within that channel adhere to the firm's communications policy. However, data aggregation can "stitch" together these channels so that a conversation can be read entirely in context. This gives member firms a much deeper look at investor protection, because it allows compliance teams to evaluate communications and the exchange of information in a more realistic and sensible way. Compliance evaluation will be performed with the same level of insight as the original consumer communications.

FINRA historically has not advocated or promoted a specific use or method of technology in its rules and guidance. Given the legal complexities associated with data aggregation technology, FINRA would be wise to continue its approach in this respect. Continued technological innovation and consumer demand will increase the amount of data aggregation. At the same time, this trend also provides a tremendous opportunity to provide a a deeper and more robust method of compliance. In this way, Hearsay believes that FINRA should continue to provide principle-based guidance such as "prohibit, protect and evaluate" that encourages member firms to seek opportunities to leverage data aggregation in ways that benefit consumers not only from a consumer demand perspective but from a compliance perspective as well.

Sincerely,

Deep Kingra | Customer Success Manager & Compliance Specialist

Donna Prlich | Chief Business Officer