

FG Consulting & Advising, LLC

Digital & Strategy
Research, Trading and Investing

September 24, 2018

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

Re: FINRA Request for Comments on Financial Technology Innovation in the Broker-Dealer Industry

Dear Ms. Mitchell:

FG Consulting & Advising, LLC ("FG" or "I") is grateful for the opportunity to comment on Financial Technology Innovation in the Broker-Dealer Industry. These comments are focused on data aggregation issues and are based on over 15 years of experience and interactions primarily with retail, self-directed investors and traders.

Data Aggregation

Data aggregation provides consumers a valuable service. It enables those individuals with multiple accounts from different financial providers to obtain a holistic view of their financial flows and wellbeing.

As FINRA has noted¹, data aggregation presents risks and benefits to the consumer. Any rules established should be grounded in a basic set of principles or common understandings. Using these principles as explicit guideposts will help FINRA better define necessary future rulemaking that appropriately balances the needs of customers, broker-dealers, and other financial technology providers.

Basic Principles

1. **Customers should have explicit ownership rights in their financial data.** As such, no entity having access to that data can use or distribute that data without permission of the customer.

¹ <http://www.finra.org/investors/alerts/know-you-share-be-mindful-data-aggregation-risks>

2. **Broker-dealers cannot hold customers' data "hostage", i.e. establish undue barriers to customers obtaining their data in machine-readable form.** This is important not only for financial technology providers, but also for customers that want to use financial planners that are not affiliated with their broker-dealer(s) or who need to give this data to their independent tax professionals. This principle is comparable to that of the UK's Open Banking regulations that forced banks to provide standardized digital access to customer data.²
3. **Broker-dealers should be able to establish "reasonable" protections against screen scraping and/or impose reasonable guidelines for the use of data access APIs.** These firms need to ensure that appropriate data safeguards are in place for customer data and that screen scraping does not negatively impact systems performance.

Recommendations

Principle #1

- Any firm, broker-dealer or financial technology provider, that is aggregating data obtained from external sources, must provide to users a printable/downloadable user agreement that defines:
 - What data will be accessed.
 - How often will the data be accessed, e.g. on-demand by the customer or at specified regular intervals without a specific customer interaction.
 - Whether the aggregator will be storing the customer's login credentials, and if so, how will this data be protected.
 - How long will data be stored.
 - How the data will be used for the customer's benefit.
 - Explicitly define any other uses of the customer's data, either individually or aggregated with other customers' data, and whether such uses will include any personally identifiable Information (PII)³.
- This agreement should also include a summary of the terms of the agreement in simple, easy-to-understand language. Online user agreements today are often written in multi-page, difficult to understand, legal language that even sophisticated customers have little chance of understanding.
- Any changes in the way that a company wishes to use a customer's data must be shared with the customer, and affirmative consent for that new use obtained.
- Customers need the right to have their *aggregated data deleted upon request*.

² <https://www.openbanking.org.uk/>

³ PII data is uniquely tied to a customer and can include demographic data (e.g. age, gender, race), contact information (e.g., name, address, telephone #, email address), financial information (e.g. account balances, holdings) as well as other data (e.g. IP address) that could partially or fully identify an individual and/or could be used to facilitate financial fraud against that customer or invade their privacy.

Principle #2

- Broker-dealers should have an ***affirmative obligation*** to provide customers with digital access to basic information from the customer's interactions with the broker-dealer.
 - Current positions and the cost basis of these positions. Current is defined as real-time when appropriate (e.g. for securities that trade intraday).
 - Any loans outstanding, e.g. margin loans
 - A 24-month history of transactions in the account
 - Positions bought and sold with their transaction prices and associated gains and losses
 - Income and distributions from the customer's account(s) - dividends, interest, capital gains distributions, and other investment distributions (e.g. non-taxable return of capital)
 - Corporate actions associated with a customer's position(s)
 - Deposits and withdrawals from the account(s) including distributions from tax favored accounts such as IRAs, 529s, and HSAs
 - Direct fees and commissions paid to the broker-dealer including transaction-based fees, service fees (e.g. printed statement or wire transfer fees), asset-based fees (e.g. wrap accounts), fees for guidance services, or interest on margin balances
- Broker-dealers should make this data available to customers via their websites. Access could be provided:
 - Via a downloadable .CSV or another standard file type
 - By providing access to the data via an application programming interface (API) or
 - Enabling screen scraping
- As an alternative, this customer information could be provided via removable media such as a USB drive
- Broker-dealers' account agreements should be updated to reflect how they enable (or block) specific types of customer data access and sharing

Principle #3

- Broker-dealers should have the right to block screen scraping for their protection and the protection of their customers
 - They must provide an alternative mechanism for customers to obtain access to their data
- Broker-dealers should have the right to block access from any third party that does not follow the recommendations listed in Principle #1. This is critically important since most financial technology providers and many other financial providers exist outside of FINRA's regulatory scope.
- The terms for a firm seeking to get automated access to a customer's data via a broker-dealer cannot be onerous. While each broker-dealer may have somewhat differing requirements, FINRA should establish rough guidelines as a best practice to be followed.
- A digital file that could be downloaded by the customer and given to another firm should be considered as an option. This alternative might make it easier for new Fintech firms to get access to customers' data without having to sign agreements with a large number of broker-dealers.

Other Issue to Resolve

Security identifiers such as CUSIP® identifiers or SEDOL codes are generally needed to identify non-U.S. or non-equity securities in customer accounts. These identifiers are the property of commercial enterprises and their use requires a license. FINRA and the Securities and Exchange Commission need to address how the industry will function if these become standards required by broker-dealers. Effectively, broker-dealers could predicate their cooperation based on a smaller firm acquiring a license they could not afford. This could become a gating or delaying factor to new startups. This issue should be solved fairly to all parties across the industry, simplifying the pricing and contracting for this needed information.

Reasons for the Change

While many individuals prefer to work with a single financial services provider for all their needs, others prefer to work with multiple firms in different areas that better meet their requirements. The emergence of financial technology (Fintech) firms with targeted digital products has highlighted the need for safe, secure, and open access to customer data. Large financial institutions should not be allowed to block customers from engaging with other firms. At the same time, there is an expectation that financial firms holding customers' assets and

FG Consulting & Advising, LLC

Digital & Strategy
Research, Trading and Investing

data will protect those assets and data from harm and exploitation. A principles-based set of guidelines can help all parties better and safely meet the needs of customers.

* * * * *

FG Consulting & Advising, LLC appreciates the opportunity to provide comments on Financial Technology Innovation in the Broker-Dealer Industry. Well structured changes to the rules will make the market for financial services more competitive while better protecting customers and broker-dealers. I would be happy to answer any questions or provide additional detail as requested by FINRA.

Sincerely,



Franklin Gold
President
FG Consulting & Advising