ELECTRONICALLY SUBMITTED VIA pubcom@finra.org

October 11, 2018

Jennifer Piorko Mitchell
Office of the Corporate Secretary
Financial Industry Regulatory Authority
1735 K Street, NW
Washington, DC 20006-1506

Re: Special Notice dated July 30, 2018, FINRA Requests Comment on Financial Technology Innovation in the Broker/Dealer Industry

Dear Ms. Mitchell:

cleverDome, Inc.™ (cleverDome) is grateful for the opportunity to submit this comment letter in response to Special Notice dated July 30, 2018, FINRA Requests Comment on Financial Technology Innovation in the Broker-Dealer Industry. cleverDome is an Arizona Benefit Corporation (B Corporation) that operates as a Co-Op. Members include FinTech vendors, custodians, managed security service providers broker/dealers, registered investment advisers, financial advisors and ultimately their investor clients.

In collaboration with financial industry thought-leaders, cleverDome has created a revolutionary community-driven platform that addresses the cybersecurity risks of data aggregation and data integrations[1]. Accordingly, this comment letter will focus on cybersecurity risks created when confidential consumer information is shared, accessed, sent or received through data aggregation services and data integrations. It will also explain why a community driven solution is necessary and what role FINRA can and should take in addressing the cybersecurity risks of data aggregation and data integrations.

[1] Data integrations connect or integrate data from one entity holding the data with another entity. They typically establish direct connections using an "application programming interface" (APIs) with a set of protocols for developing direct transfers of data between the financial institution (e.g. a custodian) to another financial institution (e.g. a broker/dealer) and/or to a third party vendor that is providing services to the broker/dealer (e.g. a financial planning vendor).

207 N Gilbert Road, Ste 001, Gilbert, AZ 85234
(855) 609-9929 | (480) 588-2459
www.cleverdome.com

Cybersecurity Risks of Data Aggregation

Over the last 20 years third party data aggregation services and data integrations have been used to meet consumer demand for accessible financial information and the financial services industry's need to efficiently manage data available from multiple sources. This consumer and industry demand has fueled an exponential growth of companies offering financial technology services ("FinTech vendors") that share, access, send or receive confidential consumer information to serve the financial services industry.

Historically, FINRA has addressed compliance concerns regarding consolidated statements and data aggregation issues such as accessibility, accuracy and completeness of the data.[2] Only recently has FINRA and other regulators focused on the cybersecurity risks involving data aggregation.[3] Even these recent publications fail to address the underlying issues that exist with FinTech vendors.

Data aggregation and data integration creates significant cybersecurity risks for the following reasons:

1. **There is no oversight.** FinTech vendors are unregulated. They are not bound by the same requirements as broker/dealers and other financial services firms to protect confidential consumer information.
2. **There are no common standards.** There are no common due diligence requirements and no common minimum cybersecurity standards that FinTech vendors must meet to share, access, send or receive confidential consumer information.

[2] See Regulatory Notice 10-19 (Apr. 2010). Regulatory Notice 10-19 reminds firms of their responsibilities to ensure that they comply with all applicable rules when engaging in the practice of providing customers with consolidated financial account reporting (e.g., reports offering a single document that combines information regarding most or all of the customer's financial holdings, regardless of where those assets are held). In addition, Regulatory Notice 10-19 highlights a number of sound practices related to these types of activities.

[3] In October 2017, the Consumer Financial Protection Bureau (CFPB) outlined principles for consumer protection in the area of consumer-authorized financial data sharing and aggregation, with a particular focus on data protection and privacy. CFPB, Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation (Oct. 18, 2017). In March, 2018 FINRA published Know Before You Share: Be Mindful of Data Aggregation Risks. (March 29, 2018). http://www.finra.org/investors/alerts/know-you-share-be-mindful-data-aggregation-risks. The Securities Industry and Financial Markets Association (SIFMA) has also issued data aggregation principles. (April 12, 2018). https://www.sifma.org/resources/news/sifma-releases-data-aggregation-principles-to-help-consumers-better-protect-their-data/

207 N Gilbert Road, Ste 001, Gilbert, AZ 85234
(855) 609-9929 | (480) 588-2459
www.cleverdome.com

3. **There is no traceability.** Confidential consumer information is shared, accessed, sent or received by unidentified or unknown third parties because FinTech vendors use other vendors (i.e. vendors of the FinTech vendors) to provide their services to their broker/dealer clients. Those unidentified or unknown vendors of the FinTech vendors also are unregulated and not subject to due diligence requirements or minimum cybersecurity standards.
4. **There is limited informed consumer consent.** Consumers receive limited information about the FinTech vendors that share, access, receive or send their confidential information through data aggregation services or data integrations, i.e. direct connections between one or more FinTech vendors, completed at the request of broker/dealers. They receive no information about the third party vendors used by FinTech vendors to provide services to their broker/dealer clients because they are unidentified or unknown.
5. **There is no accountability.** Most current contracts between broker/dealers and FinTech vendors lack terms requiring FinTech vendors to:
    - Notify the broker/dealer of a data security breach involving its confidential consumer information
    - Complete due diligence and identify their own third party vendors or data integration partners that access, send, receive or share confidential consumer information
    - Comply with common minimum cybersecurity requirements
    - Take financial responsibility for their failure to protect confidential consumer information

These risks are enhanced by two additional factors:

1. Confidential consumer information is accessed, sent, received and shared over the open internet which is not secure.
2. Individuals are using devices (phones, tablets, computers) which are unknown and/or not secure (i.e. do not meet common minimum cybersecurity requirements) to access, send, receive and share confidential consumer information.

The Financial Services Industry Led Community-Driven Solution

Both broker/dealers and FinTech vendors are struggling with how to address the cybersecurity risks inherent in data aggregation and data integrations. Broker/dealers lack the expertise and resources to complete meaningful due diligence of FinTech vendors let alone identify and complete due diligence on the vendors of the FinTech vendors and integration partners who access, share, send or receive their confidential consumer information. FinTech vendors are

207 N Gilbert Road, Ste 001, Gilbert, AZ 85234
(855) 609-9929 | (480) 588-2459
www.cleverdome.com

barraged with multiple disparate due diligence requests from their broker/dealer clients, all applying a variety of different cybersecurity standards. Further, the lack of regulatory oversight of FinTech vendors and the lack of accountability render it nearly impossible for broker/dealers to compel FinTech vendors to complete due diligence or adhere to minimum cybersecurity standards.

The cybersecurity risks of FinTech vendors providing data aggregation services and data integrations with broker/dealers and other FinTech vendors is significant. This is an industry problem that requires a community based solution. Broker/dealers and FinTech vendors must work together and agree to:

1. Adopt common minimum cybersecurity standards that all broker/dealers and FinTech vendors follow when accessing, sending, receiving or sharing confidential consumer information ("Minimum Cybersecurity Standards").
2. Comply with the Minimum Cybersecurity Standards when accessing, sending, receiving or sharing confidential consumer information.
3. Complete a due diligence process that identifies all FinTech vendors, the vendors of the FinTech vendors and integration partners who access, send, receive or share confidential consumer information and require that they also complete due diligence and comply with common minimum cybersecurity standards ("Common Due Diligence").
4. Only use private secure connections, i.e. not the open internet ("Secure Network"), to share, send, receive or access confidential consumer information.
5. Only use known secure devices, i.e. known phones, tablets and computers which meet the Minimum Cybersecurity Standards ("Secure Devices"), to share, send, receive or access confidential consumer information.

Collaboration within the financial services industry is critical to successfully implement these steps. And there are already efforts underway with real solutions.

The BD/RIA Cyber Consortium is a group of broker/dealers, registered investment advisers, FinTech vendors and industry thought leaders that have joined together to discuss these issues and explore solutions.[4] Its members have worked together to create Minimum Cybersecurity Standards and Common Due Diligence for FinTech vendors, have shared recommended terms for FinTech vendor contracts, and have identified solutions for Secure Devices and a Secure Network.

[4] To join the BD/RIA Cyber Consortium contact Paul Osterberg at paul@strategybasecamp.com or Bridget Gaughan at bridget@cleverdome.com. Membership is open to all industry participants and there is no fee to join.

207 N Gilbert Road, Ste 001, Gilbert, AZ 85234
(855) 609-9929 | (480) 588-2459
www.cleverdome.com

Collaboration of financial industry thought-leaders has also led to the development of a revolutionary community-driven platform that addresses the cybersecurity risks of data aggregation and data integrations. cleverDome is an Arizona Benefit Corporation (B Corporation) that operates as a Co-Op. Its members include FinTech vendors, custodians, managed security service providers, broker/dealers, registered investment advisers, financial advisors and ultimately, in the future, will include investors.

As a B Corporation, cleverDome's mission is to protect confidential consumer information through a community-driven platform that redefines the standards for protecting confidential consumer information by taking that information "under the Dome", i.e. secure and off the open internet. cleverDome members complete and share member Due Diligence and comply with the Minimum Cybersecurity Standards. They share, send, receive and access confidential consumer information under the Dome using a safe, reliable and fast Secure Network and Secure Devices. [5]

FINRA's Role in the Community-Driven Solution

Industry led community-driven solutions like cleverDome are necessary to address the cybersecurity risks of data aggregation and data integration. It is highly unlikely that FINRA can or will regulate FinTech vendors, so broker/dealers and FinTech vendors must work together to implement effective and efficient Due Diligence based on Minimum Cybersecurity Standards which identify hold all parties that share, access, send or receive confidential consumer information accountable.

FINRA's role is to educate and inform its members as well as the FinTech vendors who service its members. Specifically, FINRA can and should:

- Publish the Minimum Cybersecurity Standards created by the BD/RIA Cyber Consortium and encourage FINRA member firms to adopt them as recommended best practices.

[5] The "Dome" is a revolutionary model built on a community driven platform that delivers a software defined perimeter (SDP), a logical set of disparate, network-connected participants within a secure computing enclave, for the cloud. Confidential data is hidden from public discovery via the cleverDome secure network, and access is restricted by cleverDome to the specified cleverDome Members, removing confidential client data from public visibility and reducing the surface area for attack. For additional information, see https://cleverdome.com/ or contact Alan Gleghorn, President of cleverDome at alan@cleverdome.com.

207 N Gilbert Road, Ste 001, Gilbert, AZ 85234
(855) 609-9929 | (480) 588-2459
www.cleverdome.com

The Draft Minimum Cybersecurity Standards were shared with members of the FINRA cybersecurity examination staff in July 2017 and comments received from FINRA staff were incorporated into the final version of the Minimum Cybersecurity Standards. Further review or comments from FINRA staff is welcomed.

- Publish guidance and recommended best practices on Due Diligence that includes identifying and completing due diligence on FinTech vendors, vendors of FinTech vendors and integration partners.
- Publish the list of FinTech vendors who have voluntarily agreed to complete Due Diligence and comply with the Minimum Cybersecurity Standards. This will assist FINRA member firms in identifying FinTech vendors who have already completed Due Diligence and meet the Minimum Cybersecurity Standards.
- Publish guidance and recommended best practices on use of Secure Devices to access, send, receive or share confidential consumer information.
- Publish guidance and recommended best practices on use of Secure Networks to access, send, receive or share confidential consumer information.
- Identify and share information with FINRA member firms and FinTech vendors about cybersecurity risks of data aggregation and data integrations, and the solutions available to address the risks.

Conclusion

The cybersecurity risks of data aggregation and data integration is an industry problem that requires a financial services industry led community-driven solution. Financial services firms and the FinTech vendors who service them must work together to protect confidential consumer information. FINRA plays an important role by providing guidance and recommending best practices as detailed above, and also by identifying and sharing information with its member firms and FinTech vendors regarding solutions that address the cybersecurity risks of data aggregation and data integration.

cleverDome thanks FINRA for the opportunity to provide comments on the important issue of data aggregation, and looks forward to working with others in the financial services industry to address the cybersecurity risks of data aggregation and data integration. For further information, you may reach the undersigned at bridget@cleverdome.com.

Respectfully submitted,
cleverDome, Inc.
Bridget M. Gaughan
Bridget M. Gaughan
Co-Founder and Chief Risk Officer

207 N Gilbert Road, Ste 001, Gilbert, AZ 85234
(855) 609-9929 | (480) 588-2459
www.cleverdome.com