sifma
Invested in America

February 21, 2017

VIA EMAIL: FederalRegisterCommments@CFPB.gov
Monica Jackson
Office of the Executive Secretary
Consumer Financial Protection Bureau
1700 G Street, NW
Washington, DC 20552

Re: CFPB Request for Information Regarding Consumer Access to Financial Records

Dear Ms. Jackson:

The Securities Industry and Financial Markets Association ("SIFMA")[1] appreciates the opportunity to comment on the above-referenced request for information ("RFI") from the Consumer Financial Protection Bureau ("CFPB"). SIFMA fully support a customer's right to access financial information in a format that provides the same level of security as required for an institution governed by the Gramm-Leach-Bliley Act ("GLBA") or equivalent regulations. Data aggregation provides valuable benefits to customers and, as such, our member institutions may currently provide those services to customers as well. The sharp increase in the use of independent data aggregators over the last decade provides further evidence that consumers value these services but also highlights the need for additional attention to the security of these services. We believe that the financial industry can continue to work with data aggregators to develop policies and procedures that would benefit consumers such that their information would be properly protected, but that additional regulation of data aggregators not currently regulated by GLBA may be necessary.

We further encourage the CFPB to work with the primary financial regulators, including the Office of the Comptroller of the Currency ("OCC") and the Securities and Exchange Commission ("SEC"), to ensure consistent regulation and guidance and benefit from their expertise on particular issues surrounding various types of financial institutions. For example, certain information held by broker-dealers regarding their customers' activities (*e.g.*, open orders for securities transactions, unvested stock awards and grants and information about thinly traded stocks) should be given special attention before regulators consider regulations that could require the disclosure or access of this sensitive information to third parties. Further study is needed on the ability of consumers to

[1] SIFMA represents these broker-dealers, banks and asset managers whose nearly one million employees provide access to the capital markets, raising over $2.5 trillion for businesses and municipalities in the U.S., serving clients with over $20 trillion in assets and managing more than $67 trillion in assets for individual and institutional clients including mutual funds and retirement plans. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA).

have unfettered access to financial institutions' websites during times of market stress or volatility, when these systems might also be affected by data calls from aggregation services. The SEC should take the lead on these issues.

As the RFI notes, there are generally two standards being used by data aggregators to collect financial information from customers: (1) "screen scraping" and (2) an application programming interface ("API"). The former requires customers to provide their log-in credentials to the aggregator, and then the aggregator "scrapes" the data from the financial institution website. In other instances, the data aggregator and the financial institution agree on an API where the financial institution provides the agreed upon information to the data aggregator for participating customers. Neither is a perfect system. Screen scraping comes with many security concerns for customers and financial institutions. While APIs generally provide more security for customers and financial institutions, they take longer to negotiate and implement and are generally inconsistent across the industry.

SIFMA commends the Center for Financial Services Innovation ("CFSI") for its development of the *Consumer Data Sharing Principles: A Framework for Industry-Wide Collaboration* ("CFSI Framework").[2] CFSI worked with many industry stakeholders including large and small financial institutions, data aggregators, fintech companies and regulators. Although there are some matters that were not resolved through the drafting process, it should be held as an example of industry collaboration to establish a framework to achieve a necessary goal in lieu of government-imposed guidance or new regulations.

1. Security Requirements

The top priority for regulators, financial institutions, and data aggregators must be safeguarding customer financial information regardless of how it is accessed or stored. SIFMA does not believe that customers desire to use data aggregation platforms should outweigh the threat of unauthorized access to customer data and exposure to unauthorized transactions. As such, financial institutions are held to high standards under GLBA and the many regulations promulgated thereunder, and data aggregators not currently subject to such regulations (or an equivalent regulatory standard) should be required to comply with such standards.

Many data aggregators do not use the data security protocols or fraud monitoring system that regulated financial institutions use. As a result, data aggregators are more vulnerable to cyber-attack. Data aggregators may be particularly attractive targets for cyber criminals because they may hold customer account information, log-in credentials, and personally identifiable information ("PII")..A cyber-attack on data aggregators may expose financial institutions to significant potential liability for any unauthorized transactions. The risks increase in a faster payments environment because it is harder to intercept the transactions.

Although the retention and use of data is of particular concern, the practice of "screen-scraping" puts both consumers and financial institutions at risk. Providing log-in credentials to a data

[2] Available at http://www.cfsinnovation.com/getattachment/News-Stories/New-Research!-Consumer-Data-Sharing-Principles-A-F/2016-Consumer-Data-Sharing-CDAWG-white-paper-Final.pdf

aggregator exposes the consumer's financial accounts to potential breach, theft and misuse of both personal information and financial assets, especially if the data aggregator is not required to store that information in a secure manner, such as through encryption. Further, the use of certain dual factor authentication methodologies utilized by financial institutions in response to regulations can create technical difficulties to this type of data acquisition.

Financial institutions would like to work with aggregators to find secure methods for transferring relevant customer data and, therefore, SIFMA supports the use of technology that does not require customers to turn over their log-in credentials to the aggregators. We acknowledge, however, that such technology is not yet perfected and its use may not be consistent across financial institutions.

2. Access Principles

SIFMA is advocating for the following principles for aggregator access to customer information held on our members' systems: (1) proper disclosure; (2) data access and use transparency; and (3) customer choice.

First, data aggregators should give customers clear, conspicuous disclosure before obtaining customers' consent to access financial information. Such disclosures should use plain English and prominently displayed prior to any information being collected or requested by the aggregator. The disclosure should identify what data is being collected, how it is used and secured and the categories of third parties with whom it is shared. This is consistent with a financial institution's obligation under GLBA, particularly Federal Reserve Reg P and SEC Reg S-P, to provide a privacy notice with required disclosures when a customer account is created.

Second, consumers have a right to control how their financial information is used. Data aggregators should only collect and use disclosed information as necessary to provide the services expressly requested by the consumer.

Third, consumers should have a clear and easy way to terminate the aggregator's access to their information and to confirm that their information is no longer being collected. This necessitates the use of an API, instead of screen scraping, where customers can cut-off an aggregator's access through their own financial institution. Aggregators should securely delete any information held except as required to be retained pursuant to relevant laws or regulations.

3. Third Party Data Use

Data aggregators may be putting consumers at additional risk through the transfer to and use of customer data by third parties. The use and sale of customer financial information by financial institutions is currently regulated under several regimes including GLBA. However, the uncertainty of how and under what conditions an aggregator may use, assemble, evaluate, or repackage a consumer's information once it leaves the financial institution creates risk for both consumers and financial institutions.

Consumers may not have transparency into how their data is repackaged or shared with others, thus obscuring their rights to challenge data that may not be accurate or limit its use. Further, unlike with

financial institutions, consumers have no separate federal legal basis allowing them to opt-out of their data being shared with third parties for marketing or related purposes. These risks highlight the compelling necessity to ensure the parties' respective rights and obligations are clearly set forth in these transactions.

4. Incident Response Reporting to Federal Regulators

Although 47 states currently have data breach notification laws, all financial institutions are independently bound by the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (the "Interagency Guidance") which set additional standards for consumer and regulatory notifications of data breaches. Importantly, the Interagency Guidance requires that a financial institution's primary federal regulator be notified in the event of *any* exposure of sensitive information. This is a stricter standard than consumer notification standards under the Interagency Guidance or under most state data breach notification laws, which are generally triggered by a consumer harm threshold.

Given the breadth and scope of highly sensitive consumer data that some aggregators may have, we think there is value in aggregators being subject to a similar federal regulatory notification standard. This will help regulators to identify and address key risks in the aggregator community and ensure that consumer data is being properly secured.

5. Equivalent Regulation

We believe that the current privacy and security requirements that govern financial institutions regulated by GLBA should be made equally applicable to data aggregators not affiliated with a regulated financial institution. Customers would be assured of the safe and secure treatment of their financial information. Such a regulatory scheme would put all data aggregators – both those affiliated with financial institutions and those not – on the same playing field when holding the same sensitive customer information.

If you have any questions or need any additional information, please contact me at 202-962-7385 or mmacgregor@sifma.org.

Sincerely,

/Melissa MacGregor/

Melissa MacGregor
Managing Director and Associate General Counsel

cc: Hon. Michael S. Piwowar, Acting Chair, SEC
Thomas J. Curry, Comptroller of the Currency
Robert Colby, General Counsel, FINRA