STROOCK
SPECIAL BULLETIN

SIFMA's New Data Aggregation Principles and What They Mean for the Financial Sector

April 18, 2018

Last week, the Securities Industry and Financial Markets Association ("SIFMA"), a trade group for the United States securities industry, issued a set of Data Aggregation Principles ("the Principles").[1] In general, data aggregation applications are able to aggregate a customer's financial data across different accounts, from different institutions. While such applications provide customers with desired convenience, tools and analytics, they also pose security risks by virtue of their ability to access the accounts. The Principles are intended to provide guidance to organizations working with data aggregation applications on how to provide customers with secure access to their financial information.

The Principles are divided into four main areas: 1) Access; 2) Security and Responsibility; 3) Transparency and Permission; and 4) Scope of Access. Although brief, the Principles provide clear guidance.

With regard to **Access**, SIFMA member firms believe that "customers may use third-parties to access their financial account data" and "such access should be safe and secure." As such, the Principles essentially confirm the utility of and ability to provide data aggregation services. Customers want to be able to allow financial data to be aggregated across multiple platforms and utilize related tools without compromising security.

As to **Security and Responsibility**, "Customers should not have to share their confidential financial account credentials (*e.g.*, personal IDs and passwords) with third-parties" (*i.e.*, those third parties providing data aggregation).

This Principle implicitly addresses acceptable technological implementations. Currently, "screen-scraping" technology is utilized by many data aggregators and requires the customer to share its login credentials to allow the aggregator access to the account data. Such sharing of credentials potentially places financial or other non-confidential information at risk. One alternative previously suggested by SIFMA is the use of application programming interfaces (APIs) or other software technologies that can allow the financial data to be shared through a secure gateway and that do not require the customer to reveal its credentials.

[1] https://www.sifma.org/resources/general/data-aggregation-principles/

Also with regard to Security and Responsibility, the Principles provide that "customers deserve assurances that anyone accessing their financial account data will keep it safe and secure, adopt the same data and security standards followed by regulated financial institutions, and take full responsibility for any data that they receive and provide to others." Here, the Principles recognize that data aggregation providers are not always regulated member entities, but rather may be emerging FinTech providers. The expectation is clear: member firms working with such emerging providers should ensure adequate protections are in place at these providers.

As to **Transparency and Permission**, prior to access being granted, affirmative consent should be required from customers after they receive "a clear and conspicuous explanation of how third parties will access and use their financial account data." Additionally, withdrawal of consent should be easy and made available to customers "at any time with confidence that third parties will delete and stop collecting their financial account data and delete any access credentials or tokens."

These Principles reflect a basic premise that consumers should have more control over their personal data and how such data will be used. This is somewhat in line with the European General Data Protection Regulation (the "GDPR"), which becomes effective next month. Among other protections, under the GDPR, a user has a "right to be forgotten," a "right to restrict processing," a "right to data portability," and a "right to object." Consistent with these obligations under the GDPR, the Principles recognize that informed consent, an ability to withdraw such consent at any time and the ability to request deletion of information are all vital components to protecting a consumer's financial information.

Finally, with regard to **Scope of Access and Use**, the Principles delineate between "financial account data, such as holdings and account balances," and "non-public and confidential personal information." More specifically, the Principles set forth that customer information shared with third parties should not include "non-public and confidential personal information." The Principles also provide that for customer protection, services that go beyond financial account data aggregation, such as third-party trading or movement of money or assets, "should be subject to separate agreements and require separate informed affirmative consent." Here, the Principles echo the common privacy principle that collection and disclosure of personal data should be adequate, relevant and not excessive in relation to the purpose for which the data is processed.

With the number of high profile cybersecurity incidents continuing to rise each day, SIFMA has taken a first step to signal that it recognizes the potential issues inherent in data aggregation. Whether or not the Principles are the first step in a broader push that may include regulation or self-governance in the United States remains to be seen. However, it is clear that financial institutions and other companies that want access to financial data will need to prove to their customers that they have the procedures in place to make them worthy of receiving such access.

If you have any questions about data privacy, data aggregation, or any other question about how the Principles or GDPR may affect you, please contact one of the attorneys listed below.

By Ian G. DiBernardo, the co-head of the FinTech and Intellectual Property & Technology Groups of Stroock & Stroock & Lavan LLP, and Jeffrey Mann, a Special Counsel in those groups and a Certified Information Privacy Professional (CIPP/US).

For More Information

Ian G. DiBernardo
212.806.5867
idibernardo@stroock.com

Jeffrey M. Mann
212.806.5763
jmann@stroock.com

New York
180 Maiden Lane
New York, NY 10038-4982
Tel: 212.806.5400
Fax: 212.806.6006

Los Angeles
2029 Century Park East
Los Angeles, CA 90067-3086
Tel: 310.556.5800
Fax: 310.556.5959

Miami
Southeast Financial Center
200 South Biscayne Boulevard, Suite 3100
Miami, FL 33131-5323
Tel: 305.358.9900
Fax: 305.789.9302

Washington, DC
1875 K Street NW, Suite 800
Washington, DC 20006-1253
Tel: 202.739.2800
Fax: 202.739.2895

www.stroock.com

Stroock & Stroock & Lavan LLP provides strategic transactional, regulatory and litigation advice to advance the business objectives of leading financial institutions, multinational corporations and entrepreneurial businesses in the U.S. and globally. With a rich history dating back 140 years, the firm has offices in New York, Los Angeles, Miami and Washington, D.C.

For further information about *Stroock Special Bulletins*, or other Stroock publications, please contact publications@stroock.com.