# Client Alert

**October 19, 2017**

# CFPB Outlines Principles for Consumer-Authorized Financial Data Sharing and Aggregation

**By Rick Fischer, Obrea O. Poindexter, Trevor R. Salter, and Jennifer S. Talbert**

On October 18, the Consumer Financial Protection Bureau (CFPB or Bureau) released a set of guiding principles for participants in the financial data sharing and aggregation industry. The publication of the consumer protection principles follows a November 2016 Request for Information (RFI) in which the CFPB asked stakeholders in the data sharing and aggregation market to comment on consumer benefits and risks associated with developments that rely on financial account information. The publication of the principles was accompanied by a press release and a 12-page summary of issues raised by stakeholders (stakeholder report) that informed the development of the principles.

The stakeholder report emphasizes that aggregation market participants generally called for "[consumer protection] practices that are based on a shared set of standards and expectations." The principles reflect a response to this desire for uniformity.

## SUMMARY OF THE CFPB'S NINE PRINCIPLES FOR FINANCIAL DATA SHARING AND AGGREGATION

1. *Access*: Consumers should be able to access information about their use of a financial product. Consumers should be able to authorize third parties, such as aggregators, to obtain their information from account providers. However, the CFPB believes that access should not require consumers to share their account credentials with third parties.

2. *Data scope and usability*: Consumers may authorize third-party access to any aspect of consumer account information, including transactions, service terms (such as fee schedules), and realized costs and benefits to the consumer. Third parties with authorized access should only access the data necessary to provide the product or service requested by the consumer and should only maintain such data as long as necessary.

3. *Control and informed consent*: Consumers must understand the implications of third-party access to their data, including authorized terms of access, storage, use, and disposal. The terms of data access authorization should include the frequency, data scope, and retention period. Disclosures must be fully and effectively disclosed to the consumer, understood by the consumer, "not overly broad," and consistent with the consumer's reasonable expectations. Consumers must be able to revoke third-party data sharing authorizations in a timely manner.

4. *Authorizing payments*: Authorized data access is not payment authorization, and payment service providers may reasonably require consumers to supply both payment and data sharing authorization.

5. *Security*: Users and distributors of consumer data should implement "strong protections and effective processes" to protect consumer data. Data should only be transmitted to third parties that also have "such protections and processes."

6. *Access transparency*: Consumers must be able to readily ascertain the third parties that they have authorized to access their data, their use of such data, and the frequency at which the third parties access the data.

7. *Accuracy*: Data sharers and aggregators are expected to provide accurate and current data, and consumers should be able to reasonably dispute and resolve data inaccuracies.

8. *Ability to dispute and resolve unauthorized access*: Consumers should have a reasonable means to dispute and gain redress for unauthorized data access, regardless of whether they can identify the parties who gained or enabled the unauthorized access.

9. *Efficient and effective accountability mechanisms*: Commercial participants must be held accountable for the risks, harms, and costs they introduce to consumers by aggregating and sharing data. Commercial participants must have incentives to employ effective measures to prevent unauthorized data sharing.

## ANALYSIS OF REPORT AND PRIORITIZATION OF FINANCIAL PRIVACY

The CFPB notes the tension between (1) widespread access to information that contributes to consumer financial product innovation and (2) the need to protect consumer data and ensure that consumers have a meaningful choice in how their data is shared. The Bureau asserts that, while there may be disagreement as to which types of data consumers should be able to share and the resulting innovation benefits, all stakeholders agreed that consumer data security is a top priority and should not be sacrificed to realize the benefits of the aggregation services market.

Accordingly, the CFPB's principles reflect both a push for greater consumer control over financial data access and enhanced accountability on the part of commercial participants, such as banks, service providers, and data aggregators. Nonetheless, the principles and stakeholder report acknowledge the potential for "consumer-friendly innovations" that data aggregation services may bring to the financial services space.

## CONTEMPLATION OF DISPUTE RESOLUTION MECHANISM

The principles and stakeholder report discuss possible dispute resolution mechanisms for consumers whose data was inaccurately reported or whose data was shared with unauthorized third parties.

The seventh principle regarding accuracy contemplates a dispute resolution framework similar to that applicable to furnishers of information and consumer reporting agencies under the Fair Credit Reporting Act. While the bank or data source bears the bottom-line responsibility for correcting inaccurately reported information, the seventh principle raises the question of whether an aggregator or product provider should provide a mechanism for a consumer to dispute the accuracy of the data they obtained.

Similarly, the eighth principle, which describes dispute resolutions for unauthorized access, appears to propose an error or fraud resolution framework similar to those for payment card issuers under Regulations E and Z. The CFPB emphasizes that consumers should be entitled to redress regardless of whether they can identify who is responsible, which raises the question of whether the bank, the aggregator, or the product provider should be held liable for unauthorized access in such an event.

## ENHANCED DISCLOSURES

According to the CFPB, responses to the November 2016 RFI indicated that consumers often do not read existing third-party data sharing authorizations or disclosures. This, in conjunction with the principles' emphasis on access transparency, suggests that the CFPB may scrutinize data sharing disclosures more closely going forward. Additionally, the CFPB seems particularly concerned that consumers often do not have the ability to readily limit or revoke third-party sharing authorizations. When proposing solutions to these issues in response to the November 2016 RFI, consumer advocates expressed a preference for enforcing effective disclosures, while data account holders and aggregators preferred that consumers be given the opportunity to provide explicit consent for data access and the ability to easily confirm, revoke, or modify access.

## LIABILITY ALLOCATION

Despite the fact that stakeholders generally asserted in the report that "all parties involved in data aggregation are or should be held responsible for ensuring that consumers' data are [used] securely," and that "not all participants in the data sharing market are currently held to the same data security standards and regulatory requirements and oversight," the fifth principle on security is notably silent on the question of liability allocation. Instead, the principles press for shared responsibility and uniform standards across industry participants, as described by the ninth principle on accountability mechanisms.

## POTENTIAL CFPB SUPERVISORY MEASURES

In the stakeholder report, the CFPB emphasizes that it has regulatory and enforcement jurisdiction over aggregators and account data users. Additionally, consumer advocates suggested that "the Bureau [should] take steps to extend oversight formally to aggregators and account data users, through, for instance, its supervisory authority." In this respect, the principles and stakeholder report suggest potential future regulatory action on the part of the CFPB:

- The stakeholder report draws attention to the notion that using "a regulator or governance body that could assess and credential companies as safe and trusted third parties" may be an effective way to ensure consumers can easily ascertain who has access to their information.
- Some stakeholders urged the Bureau to clarify whether the Electronic Fund Transfer Act and Regulation E apply to consumers using aggregation services regarding their ability to dispute and resolve unauthorized charges.

While the principles do not establish binding requirements on firms, banks and other financial institutions involved in data aggregation, they offer the CFPB's view of what should be best practices and indicate the lens through which the CFPB will "closely monitor developments" in the data aggregation market.

**Contact:**

**Rick Fischer**
(202) 887-1566
lfischer@mofo.com

**Obrea O. Poindexter**
(202) 887-8741
opoindexter@mofo.com

**Trevor R. Salter**
(202) 887-1527
tsalter@mofo.com

**Jennifer S. Talbert**
(202) 887-1563
jtalbert@mofo.com

# Client Alert

## Financial Services Team

### California

| | |
|---|---|
| Alexis A. Amezcua | (415) 268-6557 |
| Elizabeth Balassone | (415) 268-7585 |
| Roland E. Brandel | (415) 268-7093 |
| Sarah N. Davis | (415) 268-7478 |
| Henry M. Fields | (213) 892-5275 |
| Joseph Gabai | (213) 892-5284 |
| Angela E. Kleine | (415) 268-6214 |
| Jim McCabe | (415) 268-7011 |
| James R. McGuire | (415) 268-7013 |
| Mark David McPherson | (212) 468-8263 |
| Ben Patterson | (415) 268-6818 |
| Sylvia Rivera | (213) 892-5734 |
| Nicholas Alan Roethlisberger | (415) 268-7534 |
| William L. Stern | (415) 268-7637 |
| Nancy R. Thomas | (213) 892-5561 |
| Lauren Lynn Wroblewski | (415) 268-6458 |

### New York

| | |
|---|---|
| James M. Bergin | (212) 468-8033 |
| Meghan E. Dwyer | (212) 336-4067 |
| David J. Fioccola | (212) 336-4069 |
| Marc-Alain Galeazzi | (212) 336-4153 |
| Adam J. Hunt | (212) 336-4341 |
| Jessica Kaufman | (212) 336-4257 |
| Mark P. Ladner | (212) 468-8035 |
| Jiang Liu | (212) 468-8008 |
| David H. Medlar | (212) 336-4302 |
| Barbara R. Mendelson | (212) 468-8118 |
| Michael B. Miller | (212) 468-8009 |
| Judy Man Ni Mok | (212) 336-4073 |
| Jeffrey K. Rosenberg | (212) 336-4130 |
| Mark R. Sobin | (212) 336-4222 |
| Joan P. Warrington | (212) 506-7307 |

### Washington, D.C.

| | |
|---|---|
| Rick Fischer | (202) 887-1566 |
| Adam J. Fleisher | (202) 887-8781 |
| Natalie A. Fleming Nolen | (202) 887-1551 |
| Calvin D. Funk | (202) 887-6930 |
| Julian E. Hammar | (202) 887-1679 |
| Oliver I. Ireland | (202) 778-1614 |
| Crystal N. Kaldjob | (202) 887-1687 |
| Steven M. Kaufmann | (202) 887-8794 |
| Donald C. Lampe | (202) 887-1524 |

### Washington, D.C. (continued)

| | |
|---|---|
| Jeremy R. Mandell | (202) 887-1505 |
| Amanda J. Mollo | (202) 778-1609 |
| Obrea O. Poindexter | (202) 887-8741 |
| Ryan J. Richardson | (202) 887-8761 |
| Sean Ruff | (202) 887-1530 |
| Trevor R. Salter | (202) 887-1527 |
| Nathan D. Taylor | (202) 778-1644 |
| Jennifer S. Talbert | (202) 887-1563 |

**About Morrison & Foerster:**

We are Morrison & Foerster—a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer*'s A-List for 13 straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

*Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.*