Data Aggregation Principles

Cite

Bureau of Consumer Financial Protections (CFPB), Consumer-Authorized Financial Data Sharing and Aggregation

Recommended Distribution:

Fintech, Corporate Development, Policy, Risk Management, Legal, Government Relations

Website:

http://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf

Impact Assessment

- Who owns a consumer's data and the manner in which third parties can access them at banks is among the most critical franchise-determining strategic factors dependent on regulatory-policy decisions.
- New CFPB principles attempt to balance consumer rights and the need for security and privacy, providing little clarity on how data aggregation will proceed in the U.S.
- In sharp contrast to an initial CFPB proposal, the Bureau does not now demand that banks be required to release data upon request by a consumer even though the principles establish clear ownership rights by consumers to their PII for the first time.
- A more gradual approach to sorting out rights, responsibilities, and risks will slow fintech innovation, limit consumer choice, and facilitate innovation within banks but there will also be more consumer certainty over privacy and cyber-security.
- New transparency standards could create extensive disclosure and consumer-relations burdens for banks and other consumer-data repositories.
- Actual transfer of liability to parties at fault outside the sphere of prudential regulation could prove problematic.

Overview

Retreating from an aggressive stance on data aggregation implicit in an earlier request for input (RFI),[1] the CFPB has laid out principles that will guide its thinking about the extent to which third-party data aggregators can access personally-identifiable information (PII) housed at banks and other financial institutions. Most importantly for the long run is a principle establishing that consumers own their PII and thus have rights to its use, distribution, storage, and security. The extent to which this principle is established in actual law and rule will determine the degree to which traditional banks "actually own" the customers they acquire or if consumers can dictate that banks share data with aggregators or others the consumers believe provide them with desired products and services. If ownership rights are enforceable and then used by consumers to cherry-pick their financial relationships, consumers may well be advantaged but banks could end up "relegated" or disintermediated as a pending Basel fintech consultation observes.[2]

Impact

The CFPB believes that data aggregation has significant potential to enhance consumer financial-product choice and increase personal control over "financial lives," along with enhancing retail-finance competition. These themes were heavily emphasized in the RFI, but the final policy statement is now considerably more circumspect about the risks to PII that are obtained by data-aggregation and other fintech firms exempt from prudential regulation and related cybersecurity and privacy standards. CFPB awareness of these risks was doubtless increased by the Equifax hack. Although credit bureaus are not a traditional fintech channel, the Equifax case nonetheless shows what can happen when regulated financial institutions share PII with third parties. Because the principles are aspirational, what is specifically to be done to meet the Bureau's transparency, security, and privacy goals remains to be determined. Any binding actions require rulemaking, but near-term interventions are possible based on the Bureau's view that consumers – not the financial entities with which they deal – own PII provided by the consumer and perhaps also the conclusions or related data amassed or gathered on the consumer by the institution with which the consumer does business. Congress is now considering a proposal to make these ownership rights far more clear in law, but the Bureau's views will influence near-term fintech and data-aggregation actions, especially if they are made more clear and reinforced in subsequent statements.

In addition to ownership rights, the final principles detail consumer powers with regard to understanding and controlling not only who is granted access to

1 See **FINTECH6**, *Financial Services Management*, November 1, 2016.

2 See **FINTECH13**, *Financial Services Management*, September 20, 2017.

PII and related data, but also to controlling how data are stored, transferred, corrected, and – if used for payment – reversed. The principles do not make clear whether the financial institution or the third party obtaining these data bear some or all of these responsibilities. It is likely that, regardless of rules or law in these arenas, the initial point of contact by a consumer for all concerns will be the financial institution holding the data, not the third party using it. This could put banks and other repositories in a difficult consumer-relations bind, executing transactions as requested by a consumer that moves certain services outside the bank but nonetheless taking the criticism and the cost of data-use errors.

The Bureau's conclusions echo aspects of the European Union's revised Payment Services Directive (PSD2), which is set for EU-national implementation in January of 2018. Under it, banks are required to share account information with fintech companies. The EU intends this to redefine banking, reducing reliance on the few very large banks that often dominate national banking markets, but EU policy-makers also readily acknowledge that fintech firms outside the scope of prudential regulation are likely to gain considerable market share from banks with uncertain safety, soundness, and inclusion results. However, most EU central banks have broad authority over national payment systems along with far more latitude to provide emergency liquidity than allowed in the U.S., perhaps limiting this downside risk. PSD2 also requires each national regulator to design "application-program interfaces" to govern third-party access to bank systems. The extent to which these interfaces facilitate access – as fintech demands – or inhibit it, as banks insist, remains to be determined in each nation and across the EU.

What's Next

This statement was issued on October 18. Although the initial CFPB request for input appeared to be a precursor to regulatory action, these final principles leave much to be resolved without binding any financial entities or fintech firms. The Bureau is also free to pursue any course of action it decides upon, although any rules would of course be subject to public notice and comment. The principles expressly indicate that enforcement actions will not be premised on them. However, entities seeking CFPB direct or implicit approval of their ventures will wish to take them carefully into account.

As Director Cordray contemplates his political future and faces an end of his term in July of 2018, the long-term future of these principles will be determined by the Trump Administration's director or any interim heads pending that director's Senate confirmation. A pending Treasury fintech report will thus be an important guide to the future of consumer-data ownership

Federal Financial Analytics, Inc.
1140 Nineteenth Street, N.W., Washington, D.C. 20036
Phone: (202) 589-0880 Fax: (202) 589-0423
E-mail: info@fedfin.com Web Site: www.fedfin.com

absent legislation in intervening months based on the hard lessons of the Equifax hack.

Analysis

Because this statement only lays out principles, it expressly establishes no binding precedent or obligations, nor is it necessarily a statement about future CFPB enforcement or regulatory policies. The principles, which are meant to be read as a whole, are:

- Consumers should obtain access to information about ownership and use of their data on request in a timely fashion. Consumers should also be able to obtain access to their data for a third party of their choice for access to their benefit in a safe fashion. Access by a consumer should not be predicated on use of a third party. Data use, access, and related activities are to be fully transparent to the consumer, who controls these functions at all times.
- Data shared covers all relevant product terms and features, with third parties selected by a consumer gaining access only to data relevant to the service selected by the consumer and only for the limited time necessary to accomplish the consumer's objectives.
- Authorized terms of access, storage, use, and disposal are fully and effectively disclosed in ways that do not coerce data-sharing. Consumers can readily revoke access that is then executed in a timely fashion.
- Authorized access should not be construed as authorized payment, with transactions executed only upon demonstration of authorized access and payment.
- Consumer data are fully secured at all points, with data transmitted only to third parties with demonstrable security protections.
- Consumers should expect that data they access or that others access is accurate and timely, with "reasonable means" to dispute and correct these data regardless of the inaccuracy's source.
- Consumers also have reasonable and practical means to resolve unauthorized data sharing, access, payments, or failure to comply with other obligations (e.g., terms of authorization). Consumers are not required to identify the unauthorized party to gain redress.
- Commercial participants in data sharing are accountable to the consumer for their adherence to all of the principles described above and agreements related to them. Incentives also support performance of these principles.