CFSI Center for Financial Services Innovation

CFSI's Consumer Data Sharing Principles: A Framework for Industry-Wide Collaboration

October 2016

Kaitlin Asrow, Associate
Beth Brockland, Managing Director

CFSI Center for Financial Services Innovation

The Center for Financial Services Innovation (CFSI) is the nation's authority on consumer financial health. CFSI leads a network of financial services innovators committed to building a more robust financial services marketplace with higher quality products and services. Through its Compass Principles and a lineup of proprietary research, insights and events, CFSI informs, advises, and connects members of its network to seed the innovation that will transform the financial services landscape.

For more on CFSI, visit our website and join the conversation online:

www.cfsinnovation.com
@CFSInnovation
/CFSInnovation
Center for Financial Services Innovation
Center for Financial Services Innovation

Authors

Kaitlin Asrow, Associate
Beth Brockland, Managing Director

Acknowledgements

Consumer Data Sharing Principles: A Framework for Industry-Wide Collaboration was supported by a grant from CFSI's Founding Partner, the Ford Foundation.

FORDFOUNDATION

Executive Summary

Consumers' ability to understand, manage and improve their financial health requires having a full picture of their financial lives.

Over the last two decades, the emergence of new intermediaries that aggregate data from numerous sources has enabled financial services providers of all kinds to provide consumers with a more complete view of their financial lives. This, in turn, has contributed to the recent growth of financial technology ("fintech") companies that are using these data to provide new tools and services to consumers.

These trends have empowered consumers to more effectively manage their financial lives and improve their financial health, but they have also raised important questions around data security and privacy, consumer control and transparency, and the need for greater industry coordination and shared standards.

In consultation with industry experts, the Center for Financial Services Innovation (CFSI), the authority on consumer financial health in the United States, developed the following set of principles to guide the financial services industry as it works to establish a data-sharing ecosystem that is secure, inclusive and innovative. This effort builds upon CFSI's previous work to establish principles and best practices guides for specific products, leveraging CFSI's Compass Principles framework for quality in financial services.

An inclusive and secure financial data ecosystem is one in which financial institutions, data aggregators and third-party application providers coordinate to provide data to consumers that are:

- **Available**: Consumers have the ability to view their financial information within the trusted and secure third-party application of their choice. ("Availability")
- **Reliable**: Consumer financial data are timely, consistent, accurate and complete. ("Reliability")
- **User-permissioned:** Consumers provide explicit consent for access to and use of their data. Consumers can easily view, modify and revoke consent for data sharing. ("Consent")
- **Secure**: All entities follow applicable laws and industry best practices with regard to data privacy and security. ("Security")
- **Limited to the application functionality:** Only the minimum amount of data required for application functionality are collected, and the data are stored for the minimum amount of time needed. ("Minimization")

While these shared principles provide an important starting point, there is still significant work to be done to ensure they are applicable across the industry. While there are challenges to their implementation, there are also encouraging examples and models that can help point the way toward possible solutions.

Further coordination among all of the stakeholders in this debate – financial institutions, data aggregators, fintech providers, regulators and consumers themselves – will be critical to achieving a secure, inclusive and innovative financial data-sharing ecosystem that supports consumer financial health.

Introduction

Access to one's financial data, often from multiple sources, is an important enabler of consumer financial health, yet making those data available to consumers creates unique business and technological challenges for the U.S. financial services industry.

The Center for Financial Services Innovation (CFSI) is the authority on consumer financial health in the United States, leading a network of committed financial services innovators to build better consumer products and practices. In recent months, CFSI has utilized its network and research expertise to understand the opportunities and challenges of consumer financial data sharing.

CFSI recognizes that consumers' ability to understand, manage and improve their financial health requires having a full picture of their financial lives. Today, as a result of technological advances and market developments, many of the products and services that provide consumers with this 360-degree view of their finances rely on data from numerous sources. There is a critical need for industry collaboration to ensure that consumers have secure and reliable access to their financial data and to support continued innovation in the financial services marketplace.

This work builds upon CFSI's previous work to establish principles and best practices guides for specific products, leveraging CFSI's Compass Principles framework for quality in financial products and innovations.

Why Consumer Data Sharing Principles?

Consumer banking in the United States has grown from local institutions serving their surrounding communities to global companies serving millions of customers. In the past, a consumer may have had a relationship with only one or two financial institutions; today, it is rare that one bank or credit union has a complete picture of a consumer's financial life. Over the last two decades, the emergence of new intermediaries that aggregate financial data from numerous sources has both helped traditional financial institutions to better understand their own customers and contributed to the rapid growth of financial technology ("fintech") companies.

These developments have empowered consumers to see, and manage to, a more complete picture of their financial lives. However, these advances have also raised important new questions for the financial services industry.

For example, numerous industry participants and observers have voiced concerns that current methods of data sharing, which typically require the consumer to share his or her bank account credentials with third parties, are insecure and expose the various parties (including consumers themselves) to unknown liability in the event of a breach. At the same time, direct data feeds through Application Programming Interfaces (APIs) with a tokenized or alternative authentication method, a solution many favor as a way to eliminate credential-sharing, can be inconsistent among financial institutions, creating new challenges for fintech providers and limiting interoperability in the overall system. Moreover, the significant technical and legal costs that are required to build and maintain APIs and negotiate bilateral data-sharing agreements can effectively exclude smaller financial institutions and fintech providers (and the millions of consumers they serve) from full participation in the data-sharing ecosystem.

While initiatives such as the Open Banking Working Group in the United Kingdom have created roadmaps for the design of open banking infrastructure, often in response to regulatory mandates, no U.S. guidelines currently address the unique complexity of our financial system. Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act grants the Consumer Financial Protection Bureau (CFPB) the authority to prescribe rules governing access to consumer data, but the CFPB has not yet formally signaled its intention to take up this issue. In the absence of a regulatory requirement, there is an important self-regulating role that the industry can play through the development of shared principles and standards.

Purpose of this Brief

This brief proposes aspirational *principles* to guide the development and operation of the financial data-sharing ecosystem and recommends specific *practices* to lay the foundation for achieving those principles. Taken together, these principles and practices (the "framework") represent a first step in achieving CFSI's vision for a data-sharing ecosystem that enables consumers to safely access and control their financial data, is inclusive of smaller financial institutions and fintech providers, and engenders trust among consumers, providers and the broader financial system.

To develop this framework, CFSI engaged in conversations with regulators, large and small financial institutions, data aggregators, business-to-business and direct-to-consumer fintech companies, industry trade groups, consumer advocacy organizations and research entities. In addition, we facilitated two in-person meetings of a Consumer Data Sharing Working Group made up of many of these stakeholders. However, it is important to note that this framework represents CFSI's point of view only, and does not necessarily reflect the individual views of working group participants.

This framework is intended to inform:

1. Financial institutions' efforts to develop policies regarding access to consumer data and the terms of contracts they negotiate with third parties;

2. How data aggregators and third-party application providers coordinate with financial institutions;

3. Future industry-wide efforts to create new, more secure, data-sharing infrastructure, including the development of technical standards;

4. A policy and regulatory response to consumer financial data sharing and protection.

CFSI's Consumer Data Sharing Principles

Addressing the challenges in the data sharing ecosystem requires unifying principles to which all parties can agree, but that are not so specific that they quickly become outdated with the natural progression of technology and business practices. The aspirational principles outlined below are intended to stand the test of time, while the action-oriented recommendations that follow each principle can and should evolve with the industry.

An inclusive and secure financial data ecosystem is one in which financial institutions, data aggregators and third-party applications coordinate to provide data to consumers that are:

- **Available:** Consumers have the ability to view their financial information within the trusted and secure third-party application of their choice. ("Availability")

- **Reliable:** Consumer financial data are timely, consistent, accurate and complete. ("Reliability")

- **User-permissioned:** Consumers provide explicit consent for access to and use of their data. Consumers can easily view, modify and revoke consent for data sharing. ("Consent")

- **Secure:** All entities follow applicable laws and industry best practices with regard to data privacy and security. ("Security")

- **Limited to the application functionality:** Only the minimum amount of data required for application functionality are collected, and the data are stored for the minimum amount of time needed. ("Minimization")

Availability

Consumers have the ability to view their financial information within the trusted and secure third-party application of their choice.

Consumers' ability to understand and ultimately improve their financial health depends, in part, on having a range of secure options to view, understand and engage with their financial information. Stronger relationships and greater transparency among the financial institutions, data aggregators and third-party application providers that participate in the ecosystem will enable the development of more secure and accessible means of sharing consumer data and further facilitate the creation of new, innovative products and services for consumers.

The predominant practice of using consumer credentials to access data, without coordination among the various entities, creates challenges and costs across the data-sharing ecosystem. It limits financial institutions' ability to monitor the security of their customers' accounts, while requiring data aggregators and third-party application providers to frequently adapt to changing electronic interfaces and continually monitor the quality of data being transferred. Additionally, financial institutions' lack of visibility into the security capabilities and practices of third parties that are accessing data on behalf of their customers may lead them to unnecessarily cut off access in an effort to mitigate risk.

Financial institutions, data aggregators and third-party application providers should therefore coordinate to build business-to-business relationships that provide ongoing and secure data-sharing choices for consumers.

Recommended Practices

- Financial institutions and data aggregators agree on audit standards for new third-party application providers intended to promote security and minimize fraud.
    - The audit approach is tiered to be commensurate with a third-party application's functionality. It does not create undue barriers to innovation or competition.
    - Third-party application providers are made aware of agreed-upon audit standards and the detailed requirements for meeting them.
    - The entity with the direct relationship with the third-party application provider, most often the data aggregator, performs the agreed-upon audit.
    - The auditing entity is responsible for upholding agreed-upon standards and the ongoing monitoring of the security and capability of third-party application providers.
    - The auditing entity provides regular reports to all relevant parties, including financial institutions, as to the efficacy of the audit program, any remedial actions recommended and subsequent corrections.
    - Financial institutions have the opportunity to engage with the auditing entity around ongoing standards enforcement and remedial actions.
- Financial institutions, data aggregators and third-party application providers may collaborate in the development of a centralized auditing entity that would certify the security of new entrants and be responsible for the ongoing maintenance of a single industry-wide auditing standard.
- To the greatest extent possible, financial institutions, data aggregators and third-party application providers exchange data under mutually agreed-upon terms.
    - If data are collected outside of mutually agreed-upon terms, data aggregators identify themselves within the data-collection process.
    - Financial institutions reach out to self-identifying aggregators with any concerns and work collaboratively to resolve them.

Reliability

Consumer financial data are timely, consistent, accurate and complete.

Consumers need to be able to trust that their data are up-to-date, accurate and complete in whatever third-party application they choose to use, if the data are to be useful for decision-making. They must also have an accessible and easy-to-use method to resolve errors if the data are inaccurate or incomplete.

The diversity of business models, application functionality and technical methods within the data-sharing ecosystem makes ensuring consistency in the timing, volume and content of data transfers challenging. This variability can lead to suboptimal results for both consumers and providers, such as delays in accessing real-time information for consumer-decision making, unanticipated loads on financial institutions' systems, and the transfer and storage of excess information, which can increase risk in the event of a data breach.

To improve results for all parties, financial institutions, data aggregators and third-party application providers should collaborate to create shared expectations around the timing and content of data

transfers across application functionalities, and to build out bilateral, or if possible, industry-wide systems that consumers can use to resolve errors.

Recommended Practices

- Financial institutions, data aggregators and third-party application providers collaborate to determine what data will be shared to achieve application functionality.
- Financial institutions, data aggregators and third-party application providers establish a known timing and volume of data transfers to provide optimal functionality for the consumer.
- Financial institutions do not disrupt the flow of data unless there is significant and demonstrable security or system integrity risk to the business or a security risk for the consumer.
    - If data flow needs to be interrupted by a financial institution, data aggregators and third-party application providers are notified at the earliest possible juncture as to the cause of the interruption and the timeline for resolution.
    - If data flow is interrupted, the consumer-facing application provider notifies consumers at the earliest possible juncture.
- Data aggregators inform financial institutions of any suspicious attempts to access data and/or systems.
- Consumers are provided with clear, easy-to-use means to resolve data reporting errors.

Consent

Consumers provide explicit consent for access to and use of their data. Consumers can easily view, modify and revoke consent for data sharing.

Consumers must be able to understand and control which third parties have access to their financial data and for what purposes those data may be used.

While third-party application providers routinely ask consumers for consent to access data from financial institutions on their behalf, the ways in which those consent prompts and the corresponding terms of service disclosures are presented can vary significantly from application to application. Additionally, there is varying information and functionality provided to consumers regarding their ability to view or modify previously-permissioned consent.

All parties have a role in ensuring that consumers are aware of, and actively consenting to, the opportunities and risks associated with sharing their financial data, and that they have ongoing agency to renew, revoke and change their consent.

Recommended Practices

- Third-party application providers seek consumer permission for the specific data access necessary to enable application functionality at the time of enrollment.
    - Data aggregators notify financial institutions when data access consent has been obtained for relevant consumer accounts.
- Consumers maintain their consent, either through a readily-available and clear revocation option or by renewing permission on an established timeline.
    - If consumer consent is revoked, or not renewed, no new data are collected.
    - If a consumer leaves an application dormant for a reasonable length of time, consent is considered to be revoked.

- The ability to clearly view and revoke previously-permissioned data access is available at any time through the third-party application.
- Financial institutions and data aggregators may collaborate to develop dashboards, either via the financial institutions' websites or a third-party site, which provide the consumer with the ability to view, modify and/or revoke consent for all of the third-party applications to which consent has been provided.

Security

All entities follow applicable laws and industry best practices with regard to data privacy and security.

Consumers must have confidence that their data are adequately protected by all applications, systems and providers that have access to them.

Other industry-led initiatives such as the U.K.'s Open Banking Working Group and the Open Financial Exchange Consortium (OFX) have made recommendations regarding security practices such as the use of the OAuth protocol and tokenization for authenticating consumer consent and accounts, as well as the use of APIs for data transfer.

While CFSI supports the adoption of industry-wide technical protocols, we understand that those listed above are not the only secure options available today and that technology will continue to evolve over time. In order to fully achieve the principle of Security, a shared set of standards is needed that can be applied and updated on an ongoing basis.

Recommended Practices

- Financial institutions, data aggregators and third-party application providers collaborate to define industry-wide standards and protocols for consumer data sharing.
    - Entities may collaborate to identify or develop an independent body to administer and maintain the standards over time.
- All entities that participate in the generation, collection, transfer and storage of consumer financial data follow applicable laws and industry best practices regarding data privacy and security.
    - Best practices contain tiers of rigor commensurate with the type and amount of data sharing entities engage in, so as to not unduly limit innovation or competition.

Minimization

Only the minimum amount of data required for application functionality are collected, and the data are stored only for the minimum amount of time needed.

Limiting the amount of data stored, the number of locations in which they are stored, and the length of time during which they are stored can help protect consumers from risks in the event of a breach or misuse of their data.

The recent proliferation of data functionality for consumers, as well as for internal business analytics and other revenue-generating activities, combined with the lack of coordination among entities, have contributed to the use of broad and recurring data pulls that may not always be necessary. There is also

a lack of clarity about optimal data storage timelines, potentially resulting in a large amount of old and unnecessary data in the ecosystem.

Financial institutions, data aggregators and third-party application providers should thus jointly create incentives to limit data storage and reduce the amount of unnecessary data in the ecosystem.

Recommended Practices

- Financial institutions, aggregators and third-party application providers agree on the minimum amount of data necessary to achieve application functionality.
- Financial institutions, aggregators and third-party application providers agree on the maximum storage time to achieve application functionality.
    - Transfer timing and volume schedules are structured to reduce or eliminate the need for data storage by third-party application providers.
    - The amount of time for which data will be stored is transparent and easily-understood within consumer consent prompts and terms of service or privacy policies.
- Data that are no longer required for the application functionality or for legal compliance are destroyed.

Ongoing Challenges

These principles provide a framework to address many of the tensions in the data sharing ecosystem, yet there is still significant work to be done to ensure that they can be applied across the industry.

There are three primary challenges that cut across all of the principles:

- How to fully and securely include small financial institutions and third-party application providers in the data sharing ecosystem.

Consumers benefit from the variety and reach of U.S. financial services providers, but many of the practices recommended in this framework – for instance, establishing and managing to mutually agreed-upon terms for data sharing – may be challenging to implement for resource-constrained small businesses, such as regional financial institutions, credit unions, and early-stage application developers. An industry-wide solution is needed to enable consumers to choose small institutions without losing access to secure and reliable channels for data sharing.

- How to adapt complex legacy system infrastructure to technological advances.

The practices recommended within this framework will likely require changes to existing systems within financial institutions, and in some cases, may even require new industry-wide infrastructure. Many financial institutions and important infrastructure players rely on older computing systems that limit their ability to implement and manage new technology such as APIs or consumer-facing dashboards. Solving for these challenges will likely take time and significant investment on behalf of many industry participants.

- How to develop functional and flexible technical implementation details amidst competing business interests.

The principles outlined here are aspirational for the industry and can serve as general guidelines today, but many of the practices that support these goals cannot be implemented until there are more detailed technical standards and industry best practices in place. Additional details are needed across all of the principles, from what should be included in audit and security standards to how and when consumer consent should be obtained. Developing these more detailed standards will require significant time, resources and buy-in from across the industry.

Potential Solutions

While the challenges noted above are significant, multiple options are available today, and still more options may be developed in the future, to ensure inclusive and secure data access for consumers. Many of these potential long-term solutions would require significant coordination and infrastructure development beyond that already called for in this brief. For example:

- Industry-wide API or other technical standards

All entities in this market could benefit from a common set of data-sharing standards, implementation guidelines and technical infrastructure solutions. However, many financial institutions are now developing bespoke relationships with aggregators and third-party application providers. Previous efforts such as the OFX Consortium and the U.K.'s Open Banking Working Group provide informative precedents for the creation of industry-wide API or other technical standards. This approach would require a coordinated effort by the industry to develop common standards and investment in new financial institution technology infrastructure. Because not all financial institutions can support this depth of investment, there may be an important role for the providers of core banking services to play in making such technology available to the entire ecosystem.

- Cooperative development among financial institutions

Financial institutions have come together in the past to develop jointly-owned and -operated entities that, in turn, provide services to the broader marketplace, such as the ClearXChange network for faster payments. A similar model could work for data sharing. Additionally, the use of common processors by many smaller financial institutions may enable wider adoption of technology and data management standards across many financial institutions. This approach would help maintain standards, build infrastructure and provide off-the-shelf solutions, with each entity still maintaining control over implementation.

- The "credit bureau" model

Another path to ongoing coordination could be to leverage a trusted, transparent and accessible intermediary to hold responsibility for collecting, monitoring, storing and sharing data; providing a centralized error-resolution process; and vetting new market entrants. Examples of this kind of model already exist in the form of credit bureaus, which perform some of these functions for lending data, and the Vendor Security Alliance, an initiative recently launched by Uber, Square, Dropbox, Airbnb and other prominent technology companies to verify the cybersecurity practices of their third-party vendors. Data aggregators could take a leadership role in the formation of such an entity, as they already perform

many of these tasks today, such as auditing third-party application providers and monitoring data quality. While a transition to this solution may not be immediate, it is a compelling option for the future.

- Complete consumer data ownership

A model of complete financial data ownership by consumers has few existing systems in place to leverage and limited examples to use as references, but it has the potential to fully disrupt the concept of data sharing. While consumers may "own" their data in theory, they remain a largely intangible and widely-dispersed resource that is difficult to control or manage. Some groups have begun to establish models for consumer data ownership, such as the Personal Data Project, which leverages technology to compile and secure personal data and enables users to direct their use. Another example is Handshake, which connects consumers directly to providers seeking data, and enables them to monetize that demand. Even the World Economic Forum has asserted that consumer data will become a unique asset class, and enabling consumers to directly leverage them can spur innovation and value. While the idea of complete consumer data ownership is still in nascent stages, the concept would enable not only access and control for consumers, but additional monetary and service benefits yet to be defined.

- Government regulation

Finally, the CFPB has the authority to craft regulation around the issue of consumer data access, and could mandate standards and coordination for the industry. Regulation would create a level playing field for all actors and help protect consumers' interests, but may limit the power of businesses to shape their ongoing role in data sharing. As they study this issue and consider potential regulatory actions, the CFPB and other agencies should weigh carefully the tradeoffs between regulatory certainty and the flexibility the industry needs to continue to innovate. Providers, for their part, should continue to engage proactively with regulators to help them better understand the challenges and opportunities involved in data sharing.

Conclusion

The data sharing ecosystem has the potential to strengthen and contribute to the cycle of financial service provision, consumer financial health and provider success. It is essential that the financial services industry work together to ensure that the ecosystem is secure for all involved and provides benefit into the future. Through CFSI's research, stakeholder conversations and working group sessions, we have discovered significant alignment around the guiding principles that should underlie future solutions. We hope that this framework will support greater collaboration among the parties as they develop data-sharing solutions that provide security and control for consumers, are inclusive of small institutions, and generate trust among all participants. In the months to come, CFSI will continue to engage with stakeholders to discuss how best to support application of this framework across the industry.

Glossary of Terms

API: Application Program Interface, which is a set of routines, protocols, and tools for building software applications. APIs enable software programs to effectively and securely communicate with each other.

Application functionality: The specific service that the consumer is asking the third-party application to perform.

Authentication: The process of identifying a consumer, and confirming their relationship to held financial accounts.

Data aggregator: An entity that retrieves information from a financial institution and makes that information available to consumer-facing third-party applications via an API. Data aggregators may also be providers of direct consumer-facing applications.

Dodd-Frank Wall Street Reform and Consumer Protection Act - SEC. 1033. Consumer Rights to Access Information (a): Subject to rules prescribed by the Consumer Financial Protection Bureau, a covered person shall make available to a consumer, upon request, information in the control or possession of the covered person concerning the consumer financial product or service that the consumer obtained from such covered person, including information relating to any transaction, series of transactions, or to the account including costs, charges and usage data. The information shall be made available in an electronic form usable by consumers.

Financial institution: An entity that holds consumer accounts and provides services through which transactions flow, generating new financial data. This is the information source for data aggregators and third-party applications.

OAuth: A widely-used standard that provides a simple and secure mechanism for users to authenticate themselves and authorize how their data can be shared. It allows a user to initiate the sharing of his or her personal data between different organizations without sharing login credentials.

Third-party application provider: An entity that provides a consumer-facing application that delivers a financial product or service, using aggregated data obtained from a data aggregator or through direct connections with financial institutions.

Tokenized authentication: Tokenization substitutes sensitive credentials with a unique, non-sensitive identifier, or 'token' that cannot be reversed back to the original data. Tokenized authentication enables access to consumer accounts using such tokens instead of log-in credentials.