FINANCIAL HEALTH NETWORK

Seven Pain-Points in the Consumer Financial Data Ecosystem:

Priorities for the CFPB's Rulemaking Under §1033 of the Dodd-Frank Act

Consumer's ability to access and electronically share their financial data has already demonstrated considerable financial health benefits. But our research among consumers, their financial app providers and data aggregators reveals seven "pain points" impeding data access and preventing consumers from sending their data where it can do them the greatest good. The Bureau's pending rulemaking under Section 1033 of Dodd Frank can best serve financial health by incorporating a few basic principles that will enshrine consumers' data access rights. The most important of these is to accord consumers the ability to share data from their financial service providers with their third party agents on the same terms—timeliness, frequency, and scope—as they are able to obtain it directly from paper statements and online banking services.

Introduction

Over the last two decades, the emergence of an ecosystem of consumer financial data portability in the US financial services market has enhanced competition for consumer credit, payments, and deposits; fostered product and service innovation; and helped increase access to services among underserved communities. Through our organizational lens of consumer financial health, allowing consumers to access and share their financial data has enabled them "to see, and manage to, a more complete picture of their financial lives."[1]

The data ecosystem has developed in the shadow of Section 1033 of the Dodd-Frank Act (DFA) which was enacted over a decade ago and declares that "subject to rules prescribed by the Consumer Financial Protection Bureau" (CFPB), consumers have the right to obtain from their financial services providers data about their accounts including "charges and

[1] https://cfsi-innovation-files-2018.s3.amazonaws.com/wp-content/uploads/2016/10/23184445/2016_Data-Sharing-Principles.pdf at 2

usage data." Until recently, however, the Bureau eschewed rulemaking in favor of a set of "Consumer Protection Principles" that it issued in 2017 and that arguably helped accelerate data portability's evolution, while allowing industry to tackle many of the technical details involved.

The results of this "light touch" regulatory approach have been mixed: On the one hand, the US financial services market provides consumers with a greater degree data portability—and as a result, more consumer-benefitting innovation—than in many markets where such portability has been more formally mandated. On the other, the absence of a binding rule left "white space" that at least some financial institutions have sought to exploit to their benefit.

Almost two years ago the CFPB signaled its intent to start down the rulemaking path, by issuing an Advance Notice of Proposed Rulemaking (ANPR) in October 2020. Rohit Chopra, the CFPB Director, recently has made clear that this rulemaking is now a top priority[2] That is a welcome effort: clearer rules of the road for data holders, data intermediaries (data aggregators), and data users will assure continued innovation to the benefit of consumers.

Scaffolding the data-sharing ecosystem with a durable regulatory framework will require striking balances between assuring that consumers can move their data where they want it to go while protecting their privacy and preventing harm from data falling into unauthorized hands. Add to that the diversity of financial services providers, the myriad ways in which they employ information technology to manage and move their customers' data, and the need to migrate from screen-scraping and credential sharing (to better assure data reliability and security, respectively). And finally, and as both the Financial Health Network[3] and the CFPB's own ANPR have acknowledged, questions of consumers' rights relating to their financial data implicate established regulatory regimes, including those pertaining to consumer reporting (Fair Credit Reporting Act and Reg V), payments (including Electronic Fund Transfer Act and Reg E), fair lending (Equal Credit Opportunity Act and Reg B), and privacy (Gramm-Leach-Bliley Act and Reg P).

---

[2] For example, see Rohit Chopra: Written Testimony Before the Senate Committee on Housing, Banking and Urban Affairs, April 26, 2022, available at https://www.banking.senate.gov/imo/media/doc/Chopra%20Testimony%204-26-22.pdf.

[3] Consumer Financial Data: Legal and Regulatory Landscape, https://cfsi-innovation-files-2018.s3.amazonaws.com/wp-content/uploads/2020/10/14142025/Financial-Data-White-Paper-_-1013_fin.pdf

As the CFPB's rulemaking team grapples with these complexities, it shouldn't lose sight of Dodd-Frank's core intent of assuring data access and portability. Its priorities should be to bolster those aspects of the consumer financial data ecosystem that are enabling consumers to access and share their data today and to remove ambiguities (most importantly about the roles and responsibilities of data holders, intermediaries, and users) that are preventing consumers from fully enjoying these rights. This means paying at least as much attention to how the eco-system currently benefits consumers and competition and how it can further those goals as is paid to the risks to both consumers and other market stakeholders from enabling data to move more freely.

In short, the Bureau can and should set its rulemaking priorities by first asking: "What are the ways in which consumer-permissioned data sharing can help consumers better lead their financial lives? And what are the ways in which the financial data ecosystem is preventing consumers from fully enjoying these benefits?"

In most cases the answers to these questions can be distilled down to a few basic principles: Consumers should have the ability to share data from their financial service providers with their third party agents on the same terms—timeliness, frequency, and scope—as they are able to obtain it directly from paper statements and online banking services. In turn, the third parties and their data aggregators should collect only what they reasonably need to provide the service or advice consumers have requested of them; and they should retain this consumer-permissioned data only as long as their relationship with the consumer persists or as the law requires. Focusing on these core principles will enable the CFPB to avoid what Director Chopra has rightly labeled the "highly complicated rules that have long been a staple of consumer financial regulation"[4] and the complex, time-consuming process required to write such rules.

Financial Data Sharing Through a Financial Health Lens

For many Americans, a core challenge in their financial lives is managing their many accounts across multiple providers, including their checking account, credit card accounts, mortgage, student loans, auto loans, retirement savings, and other investments. Beginning

[4] Rethinking the Approach to Regulations, https://www.consumerfinance.gov/about-us/blog/rethinking-the-approach-to-regulations/

in the mid 2000's personal financial management (PFM) applications like Mint.com enabled consumers to assemble a more complete picture their finances for the first time. These services relied on data aggregation—the ability to pull in data from multiple accounts at different providers—to enable consumers to view multiple aspects of their financial lives on something like a single dashboard, thereby enhancing their ability to optimize their finances.

For too many other Americans the challenges they face are more basic: juggling income and expenses, keeping track on when bills come due, finding ways to obtain affordable credit when they need it, and reducing the amount they spend on everyday financial services. For them a wide range of apps has emerged which use data aggregation in some way to access data from their transaction and credit accounts. Here are some of the most important examples:

- A consumer who has had little exposure to credit and doesn't have a credit score or whose credit score is not reflecting of their current financial situation can give a prospective lender (or a consumer reporting agency) access to their recent cash flows—earning and spending—that can be used to underwrite loans in the absence of or in lieu of a traditional credit history.

- A consumer who has difficulty making ends meet and risks overdrafting their account at the end of the month can sign up for a low-cost 3rd party service that is authorized to monitor the consumer's checking account and deposit extra funds into their account automatically when balances are low, thereby saving overdraft fees.

- A consumer who carries balances on several credit cards can enable a PFM app to assemble a consolidated picture of their debts, set a plan to pay them down, and impose spending limits on their cards so that they can't rack up further debts.

- A consumer seeking to build an emergency savings cushion can sign up to have an app monitor their checking account so that small amounts are automatically debited from their checking or prepaid account when cash flows permit and deposited in a separate institution.

- A consumer owing student loans with multiple servicers can enable an app to assemble a complete picture of their educational debts, assess their eligibility for certain forbearance or forgiveness programs, and assemble the optimal repayment plan for which they qualify.

- A consumer who uses public benefits can sign up for a service that accesses benefits data to track how much benefit funds or credits they have in their government accounts, helps budgets how to spend them, and assesses the consumer's eligibility for additional benefits.

- A consumer seeking to open a low-cost, non-overdrafting account with a challenger bank can share access to their existing checking account information to permit online account opening and rapid funding of the new account.
- A consumer seeking to build credit can allow an app to identify from checking account data the consumer's rent payments or other recurring bill payments and report those payments to consumer reporting agencies.

These are examples of just some of the services that use access to information about a consumer's financial situation (obtained from their personal deposit and credit accounts) to provide advice or take actions to their benefit. There also are examples of new entrants in the money services and money transfer businesses who, by obtaining real-time access to account data, are able to provide more convenient and less costly options for consumers.

Competition from such new services has arguably helped pressure the largest banks to soften their overdraft programs, increased access to credit (especially personal installment loans) and helped reduce the share of US consumers who are unbanked. Many of these services have been introduced by "fintechs" that didn't exist a decade ago and that owe their existence to the data-sharing eco-system.[5]

Seven Pain Points in the Data-Sharing Ecosystem

Despite this progress, considerable ambiguity remains regarding consumers' right to access and share their financial data. As a result, some consumers' ability to share their data is

[5] The Financial Health Network has formally supported dozens of these companies during their early stages through its efforts as advisor, as peer network facilitator, and—in full disclosure—as an investor through its Financial Solutions Lab.

constrained in ways that limit their access to certain helpful services and the scope and useability of what data they are able to share. We identified these particular "pain points" in the consumer data-sharing eco-system through interviews with data users and intermediaries (aggregators). It should be the rulemaking's top priority to fix them by articulating clear principles that can be formulated in an efficient rulemaking process.

1. **Access by third parties isn't universal across financial institutions.** Data users and aggregators report that they are unable to access consumers' data from some financial institutions and that lack of access is most prevalent among the smallest institutions. Some institutions simply do not offer online banking, so have no means to respond to electronic data queries. But others are simply not permitting log-ins from servers that they do not recognize, even when (as a result of consumer permissioning) aggregators or users are using the consumer's log-in credentials.

   Some institutions are simply not recognizing their obligation to share data with consumers' third party agents. Comments in response to the CFPB's ANPR from some trade groups representing community financial institutions indicate they and their constituencies do not interpret DFA §1033 as according to consumers the right to share data about their financial accounts and transactions with third parties.

   Even institutions that do not affirmatively block aggregators from accessing data have been reluctant to invest in API connections. Absent an API the only way aggregators can obtain data on the consumer's behalf is through screen-scraping using the consumer's online banking log-in credentials; this requires that consumers remember their user ID and password, share it, and update the information if their password changes. To date only a very small portion of consumer financial institutions below the top 25 by assets have implemented APIs or adopted the API specifications developed through the Financial Data Exchange. [Placeholder for reference to Jack Henry's offer of free API installations?].

   Thus, one of the most important objectives of the CFPB's rulemaking should be simply to confirm the right of consumers to share data derived through their relationship with a financial services provider with the third parties of their choosing and confirm the obligation of data holders to facilitate such sharing. Providing clarity on this central point will accelerate the migration of today's

data-sharing ecosystem away from the use of log-in credentials and screen scraping. Clarity regarding third party access will also strengthen the hand of data aggregators and third party service providers to negotiate access agreements via APIs that will, in turn, make the market for data aggregation services more competitive.

At the same time, small financial services providers face disproportionate costs when enabling their customers to share financial data. Banks and credit unions whose customers rely on screen-scraping by data aggregators to share their financial data are themselves reliant on their core platform providers or other third party vendors to host their online banking services. Some of them incur incremental costs from data-sharing to the extent that their vendor contracts are priced per log-in or per page-refresh. Similarly, small entities will incur proportionately higher costs of implementing APIs and tokenized permissioning to the extent such implementations must be customized for each institution.

Thus, the Bureau should consider delaying small institutions' deadlines for complying with the 1033 rule and more thoroughly assess the cost challenges that the consumer data ecosystem imposes on them. For example, the Bureau could exempt small institutions (e.g. those with fewer than XXX accounts or with assets under $1B) from deadlines to take affirmative steps to facilitate data access for X years and instead permit such institutions to comply during that interim period by simply allowing screen-scraping.

2. **Many financial services providers are not aware that they are covered by Section 1033 and as a result do not take steps to make the data available** DFA's language is quite broad and on its face includes all "covered persons" under the Act, including both depositories and non-depository providers of "consumer financial products and services," a phrase that the DFA defines through a lengthy enumeration of activities. Clarity is needed as to the scope of some of those enumerations in order for the financial health benefits of Section 1033 to be fully realized.

   For example, many consumers rely on providers of various types of prepaid instruments and payment processing services that enable them to access certain

employee benefits such as health savings and flexible spending accounts that represent funds consumers can tap; these consumers would stand to benefit from tools that access their data to help them use their benefits fully and effectively. Likewise, some of the most financially vulnerable consumers rely on providers of prepaid instruments and other payment processing services that enable them to access certain public benefits such as SNAP benefits and Supplemental Security Income. Clarifying the application of 1033 to the providers of these instruments and services would enable consumers to benefit by authorizing apps to help them track and manage these benefits.

Thus, the rule should explicitly define the types of entities (data holders) that are covered by the obligation to facilitate financial data sharing at least for those cases where there is known uncertainty and a tangible benefit from resolving that uncertainty. We recognize that it may not be feasible in a single rulemaking to resolve all of the marginal boundary cases involving the DFA's enumeration of consumer financial products and services. At a minimum, however, the Bureau should explicitly include among covered data holders government entities and their contractors when they provide prepaid instruments or payment processing services for the purpose of enabling consumers to access public benefits on a sustained basis or when they service government loans, such as student loans. Likewise, providers of similar instruments and services used to access employee benefits should be covered. And the same is true with respect to third party loan servicers who process payments from consumers to their lenders and maintain information about the loan balances, including government loans such as federal student loans.

3. **Even among institutions that permit consumers to share their data, not all data is available.** Financial health application providers and data aggregators indicate that some financial institutions withhold data such as the interest rate on a loan or credit card, or the number and amount of penalty fees a consumer has been charged. Despite the fact that this is the sort of information that must appear on a consumer's monthly credit card or checking statement, some institutions are not sharing it on the grounds that it is proprietary. As a result, some apps that help consumers manage their cash flows, assets, and liabilities are unable to provide their customers with a full picture of their finances. Notably, these data limitations

are most evident among large institutions that have implemented APIs as the means of responding to data queries from data aggregators (as opposed to those from whom data is obtained via screen-scraping).

Notably, some institutions withhold personally identifying information such as, address, SSN ,or date-of-birth that the consumer supplied to the data holder themselves; others withhold account number and routing codes that can be used to initiate payments or inter-account transfers. Withholding those fields can make it more difficult for data aggregators to verify that the authorization they have received is legitimate and thus may stand in the way of maintaining data security. Moreover, account numbers and routing numbers are necessary to allow an authorized data user to transfer funds from an account (as in the case of funding a new checking or savings account) or initiate a balance transfer into an account (as in the case of a credit card account). Thus, withholding the information has anti-competitive consequences.

To assure availability, the rulemaking should confirm that a consumer can obtain and share any data that they would normally be able to see themselves in the course of their relationship with the data holder. As a general principle, the scope of data a consumer can request to share should be the same as what they already are able to see themselves via paper statements or via their online banking user experience. Pricing data -- information about fees and interest rates that constitute the cost of a financial service -- are critical for apps that help consumers better manage their financial lives, and also for apps that help consumers compare the cost of their incumbent service provider with the costs they would experience by switching to a competitor. Likewise, identifying information supplied by the consumer and account information that would appear in the consumer's online account profile information would be covered when the consumer requests that it be provided to a third party.

4. **Many of the largest institutions that have entered into direct negotiated agreements with data aggregators have imposed limits regarding the number of data calls an aggregator can make per day, the number of accounts an aggregator can query per day, and/or the number of times per day an aggregator can obtain a response to a data call about a particular account.**

Among the most financially vulnerable consumers are those whose earnings can barely match their spending, and/or whose earnings' volatility and unpredictability frequently cause their incomes to fall short of expenses. For these consumers, tracking and managing funds flows at the end of their pay periods when funds get low, and at the beginning of the month when rent and other bills come due, can be an hour-by-hour affair. Some of these consumers rely on third party applications that warn them when funds are low, that a particular debit transaction may put their checking account into overdraft, or automatically replenish their account with an emergency advance on their wages. Such apps rely in turn on timely data. Apps that help consumers plan and manage their cash flow often need to check available balances and pending deposits and debits several times per day.

The rulemaking should make it clear that data holders cannot unreasonably restrict the frequency with which a consumer or their agents can access data about their accounts. That is not to say that responding to individual data inquiries doesn't impose costs, especially for small institutions as discussed above. Rather, it is to say that a data user should be able to obtain data with the same frequency, on average, that the most information-hungry consumer might seek and obtain it themselves. Based on conversations with data users and aggregators regarding consumers' appetite for data, the aggregator should reasonably have the ability to make data calls up to 4 times in a day to a particular account—and whenever the consumer initiates a query themselves directly through their agent data user.

5. **Some institutions appear to be using the consumer permissioning process to discourage access.** The US data-sharing ecosystem has evolved sufficiently that more than two-thirds of consumers have had the opportunity to give permission to one or more third parties to obtain and use data from one or more of their financial accounts.[6] As APIs emerge, the process of obtaining consent is migrating from data aggregators – who used to obtain log-in credentials to enable screen scraping -- to the financial institutions whose APIs require the aggregators to direct the consumer to a site managed by the consumer's financial institution. Aggregators and data users report that among the banks that have implemented such permissioning interfaces, completion rates vary considerably. This suggests that some financial

[6] Murphy, Silberman, and Arves: "Financial Data: The Consumer Perspective." https://finhealthnetwork.org/wp-content/uploads/2021/04/Consumer-Data-Rights-Report_FINAL.pdf

institutions have structured processes that, by design or otherwise, are sufficiently complex as to cause consumers to abandon the process midstream. **Thus the Bureau should make it clear that institutions should not overstate the risks--or otherwise unreasonably discourage consumers--from sharing their data.**

6. **"Breakage" is a continuing problem.** Data users and aggregators report that a high proportion of account linkages expire within a short period after they have received consumer permission to access them. For example, one data-user reports that two years after receiving consumers' permission to link their accounts, more than half of those linkages are no longer working.

   To some extent this "breakage" necessarily accompanies the use of consumers' log-in credentials as the means of access, as online financial services providers may encourage consumers to change their passwords frequently. But some breakage is now occurring in instances where the data holder has provided an API and user-specific tokens for access. In some cases the tokens are programmed to expire within short periods, requiring the consumer to re-permission access by the data users. Such time restrictions cannot be justified on security grounds.

   The Bureau should require data holders to not unreasonably limit the duration of consumer-permissioned access. The Bureau could allow access to be limited to a single use when the consumer is granting data access for a limited-duration purposes such as to provide income verification for a loan application or to transfer account- and routing-number information to a merchant for a one-time payment. The Bureau should, however, require longer-term durations for consent when the consumer is providing information to a service with whom they have an ongoing relationship such as a PFM orP2P payment service). And in use-cases that require ongoing account access, the Bureau could specify that permissions have some minimum term (e.g. one year) that would be disclosed to the consumer but would not preclude rescission of the consumer's right to revoke permission at any time.

7. **Aggregators' scope of data collection and retention exceeds consumers' expectations.** Most consumers who have consented to share their financial data

with a third party are not aware of the role that data aggregators play in the process. The survey we conducted in 2020 indicates the vast majority either don't remember using an aggregator or don't believe they interacted with an aggregator when permissioning access to their account data. Moreover, most consumers expect that when they link their account data to a fintech application that the application will only take the data it needs to perform the service the consumer signed up for. They are unaware that the fintech, or the data aggregator that serves it, may be pulling more data than they need or all of the data that is available (as may be likely in the aggregator's case).

The largest aggregators that access consumers' financial data generally package and price the data they resell by use case. Data users thus have an incentive only to purchase the data they need (although there is little incentive to destroy data once it is no longer needed given the nominal cost of data storage). But this data minimization incentive does not apply to the aggregators themselves. Aggregators are likely to collect more than they need because of the insights that full-scope data (e.g. all of the data available from a linked account) can provide (e.g. for further product development) and because some resell anonymized, aggregated data for app developers' use and other market analysis purposes. And while aggregators may delete consumers' personal information when a consumer ends their relationship with the data user that has obtained access to it, it isn't clear that the aggregator doesn't retain the data on an anonymized basis (or the ability to re-identify it).

It is further likely, as more consumers link more of their accounts through different service providers, that an aggregator will collect data on more than one account of a consumer even for consumers who are not using an app designed to bring multiple accounts together into a single dashboard. For example, they may collect data on the consumer's checking account for one data user, one or more investment accounts for another data user, and one or more of their credit cards and/or student loan accounts for yet another data-user. If the aggregator were able link these accounts (i.e. by matching personally identifying information that they have collected) it would obtain a level of insight into a consumer's financial life and behavior that no other entity in the consumer data ecosystem would possess and certainly not intended by the consumer.

To be sure, there are potential benefits to consumers and the consumer financial market from a vigorous and competitive data aggregation industry. But the unique scope of data that aggregators are able to collect and retain on individual consumers –aside from compounding exposure that could result from data breaches-- permits the aggregator to develop (and potentially sell) inferences about the consumer that the consumer had not intended anyone to develop. Finally, and perhaps most importantly from a consumer financial health perspective, the scope of aggregator's data collection and retention has the potential to undermine consumers' trust in their trusted agents (i.e. when an agent assures the consumer that it is collecting only the data it needs but its aggregator is not) and in the financial data ecosystem more broadly.

Section 1033 in terms speaks about the duties of financial institutions to share data and the correlative right of consumers to obtain data but does not speak to the obligations of data aggregators. Moreover, while private entities, most notably the Financial Data Exchange, have sought to define use cases for data access and the data elements needed to facilitate each use case, these are not issues that are easily handled through prescriptive and difficult-to-change regulations.

Thus the Bureau, as an initial step, should establish its supervisory jurisdiction over data aggregators by engaging in a rulemaking to define data aggregation as a discrete market and to identify larger participants in that market. Pending the completion of such a rulemaking, the Bureau should exercise its authority to engage in risk-based supervision to examine the leading aggregators to assess risks to consumers and determine how best to assure that aggregators act in a manner consistent with consumers' expectations, their safety, and that of their financial services providers.

Conclusion

The ecosystem of consumer-permissioned data sharing that has evolved over the last two decades has demonstrated great benefits to consumers, competition, and innovators seeking to advance consumers' financial health. We look forward to the Bureau's issuance

of a proposed rule under Section 1033 that both enshrines consumers rights to share their financial data with trusted third parties and the corresponding obligations of data holders, data users, and data intermediaries (i.e. aggregators) in this ecosystem.

We have highlighted here the "pain-points" that are most impeding consumers (and their financial health) from enjoying the benefits of data portability in order to encourage the Bureau's rule-writing effort to prioritize the fundamental purpose of Section 1033. That is not to say that issues of data security, fraud risk minimization and risk allocation, costs to small institutions, and overlaps with consumer reporting and fair lending law can be dismissed. But these complexities, which Director Chopra has amply identified, needn't all be fully resolved before fully enshrining consumers' right to access their financial data.

Further, addressing these pain points needn't involve an overly prescriptive approach or complex language. Establishing a few clear principles—and building on those principles regarding data aggregation services that the Bureau first issued in 2017—will go a long way toward clarifying the rules of the road for all parties:

The Financial Health Network gratefully acknowledges the support of Flourish Venture Services for our work advancing financial health through the free and secure flow of consumer-permissioned data.