November 6, 2023

Comment Intake
Consumer Financial Protection Bureau
1700 G Street NW
Washington, D.C. 20552

SENT VIA ELECTRONIC MAIL TO CFPB_consumerreporting_rulemaking@cfpb.gov

Re: Small Business Advisory Review Panel for Consumer Reporting Rulemaking; Outline of Proposals and Alternatives Under Consideration

Method Financial ("Method") was pleased to have had the opportunity to participate as a Small Entity Representative ("SER") in the Consumer Financial Protection Bureau's ("CFPB" or "the Bureau") Small Business Regulatory Enforcement Fairness Act ("SBREFA") panel, which was convened to provide perspective regarding the implications for small businesses of the Bureau's potential rulemaking pertaining to consumer reporting. As I shared throughout my participation in the SBREFA process, while Method is absolutely committed to ensuring consumers may access and share access to their financial data with full transparency, control, and safety, we:

1. Urge the Bureau to recognize a bright line distinction between "data brokers," who maintain and sell their warehoused consumer data (a product), and data aggregators or data access platforms (collectively "data access platforms"), who facilitate consumer-permissioned data access (a service) where the data is obtained directly from the data provider in real-time and is used only once for the purpose consented to by the consumer. Data access platforms should not be considered "data brokers";
2. Urge the Bureau—to the extent that it proposes a Fair Credit Reporting Act ("FCRA") rulemaking—to carve out such data access platforms from the definition of a "consumer reporting agency" under the FCRA; and
3. Believe that application of the FCRA to consumer-permissioned data access platforms is impracticable, counterproductive, adds unnecessary complexity, and would lead to confusion among stakeholders including consumers. Further, the resulting burdens and negative impacts to all stakeholders far outweigh any consumer protection benefit.

I appreciate this opportunity to submit a more detailed written summary of these views.

About Method

Method is a business-to-business software-as-a-service ("SaaS") provider to entities such as banks, credit unions, and financial technology companies (collectively, "Partners") that provide financial products and services to their end users ("consumers"). Our services are driven by our mission to facilitate efficient consumer debt management. Through Method's secure consumer authentication and account connection flow, our Partners can obtain consumer-permissioned, real-time data on their consumers' liability accounts including credit cards, student loans, personal, auto, mortgage, and other loans using elements of their personally identifiable information ("PII") so that they can provide use cases that provide their consumers with safe, secure, and convenient debt management and repayment solutions.

Through our required consumer-facing disclosures and contractual prohibitions, our Partners can use this data for the single and sole purpose for which that data was accessed and that the consumer authorized: namely, to provide the financial product or service their consumer requested, such as personal financial management, bill pay, refinancing, debt consolidation loans, or balance transfers, among other use cases. Importantly, while Method retains the data in an SSL encrypted datastore that meets or exceeds SOC 2/Type 2 and PCI DSS requirements, it only does so for record retention purposes. Method never re-discloses or reuses data for commercial purposes; not even internally.

Method authenticates consumers using their PII through a process that is already commonly used by financial institutions to satisfy their KYC/CIP requirements. Namely, Method integrates with vendors including mobile network operators ("MNOs") and the major credit bureaus to authenticate the consumer using those organizations' existing, regulated consumer authentication processes. Further, Method's integration with the MNOs also bolsters authentication and fraud mitigation with one-time-passcodes, SIM swap checks, and silent verification. This authentication process has provided hundreds of thousands of consumers with the ability to share their liability data to obtain valuable debt management products and services.

Importantly, Method's authentication and account connection processes do not require any consumer credentials or implementation by the data provider of new authentication tools, such as OAuth or other token-based technologies. Our tools demonstrate that existing technology solutions can enable safe and secure consumer authentication and eliminate the need for data providers to invest in significant technology enhancements.

Method is not a "Data Broker"

In its SBREFA memo, the CFPB suggests it may include consumer-permissioned data access platforms including Method to fall under its definition of "data brokers." As I shared during the SBREFA panels, we strongly reject this categorization.

Informed consumer consent is the basic principle around which all of Method's products and processes are based. Method does not relay any consumer's data without the consumer's knowledge and meaningful, informed consent through clear and conspicuous disclosures. Any data that we relay is obtained directly from the data provider in real-time when the consumer permissions and directs it. And the data can be used only for the strict use case that the consumer authorized at that time.

Unlike a data broker, Method never provides data from its own "files." We never sell, market, assemble, evaluate, or maintain consumer data. The data is never redisclosed or reused. Method merely operates as a conduit or a "dumb pipe" to relay real-time, consumer-permissioned data directly from a data provider to the data recipient that the consumer has selected to help them service their debt.[1]

To illustrate: Imagine that John Doe seeks a financial service from our credit union Partner and provides consent to access and share his liability account information with the credit union Partner for purposes of obtaining that requested service. One hour later, John Doe then seeks a financial service from our bank Partner and provides consent to access and share his liability account information with the bank Partner for purposes of obtaining that requested service. The data relayed to the credit union Partner is not later shared with the bank Partner. There would be two distinct and separate "pulls" from John Doe's liability accounts, based on two separate authorizations.

Method would keep the data from both "pulls" in the previously-described, encrypted datastore for record retention purposes only. As stated before, the data from either "pull" is never re-disclosed or reused.

Finally, I would once again emphasize, as I expressed during the SBREFA panels, that Method's agreements with our Partners require express written consent with affirmative acknowledgement,

[1] Method's interaction with the consumer-permissioned data is limited to the mechanical tasks of standardizing the data into a readable format. Given that the typical transaction and experiential data fields obtained from data providers is largely standard, Method's accuracy rate is 99.9999%.

from a consumer prior to conducting *any* activity on their behalf in connection with our services or data we relay. Our agreements also mandate that our Partners can only use the data as authorized by the consumer when the data is accessed, and present disclosures, notifications, and communications as required by applicable law in a clear, conspicuous, easily understood manner.

We strongly believe that the sum of these factors creates a robust consumer protection regime that materially distinguishes the consumer-centric role we play from how "data brokers" operate.

Applying the FCRA to Data Access Platforms is Counterproductive, Impracticable, and Confusing

As the CFPB notes in its SBREFA memo, Congress enacted the FCRA in 1970 to provide consumers with more transparency and control into the data maintained and disclosed by credit reporting agencies that is used for credit decisions (and later, other permissible purposes). To underscore several material points about Method's and other similar consumer-permissioned data access platforms' business model:

- the data that Method accesses and relays is always accessed at the express direction and consent of the consumer;
- the data that Method accesses and relays always comes directly from the data provider in real-time when the consumer permissions it—Method does not "maintain" files that it discloses to any third-parties or uses for internal purposes;
- the data that Method relays is consumer transactional and experiential ("T&E") data, which consumers can access at any time from their account-holding institution; and
- unlike credit reporting agencies prior to the enactment of the FCRA, or data brokers today, there already exist regulatorily-prescribed dispute and error resolution channels for that T&E data that consumers commonly use including, for example, through Regulations E and Z, and chargeback processes.

Extending the FCRA to Method and similar data access platforms is simply unwarranted and would add substantial complexity and confusion to a framework that already provides comprehensive consumer transparency and control with little, if any, consumer benefit. For example as summarized below: if data access platforms were considered to be consumer reporting agencies ("CRAs"), the platforms' compliance with the FCRA's error dispute resolution requirements would lead to confusing and absurd results for all stakeholders.

Data Access Platforms as CRAs

Section 1681i of the FCRA requires CRAs to investigate consumer disputes and correct inaccurate data in their files. But foisting this requirement on data access platforms like Method is an exercise in futility given that Method does not maintain "files," and the disputed data never sees the light of day again. As noted previously, the data is never re-disclosed or reused for any reason. The duty to investigate and correct would thus serve no purpose whatsoever and add no consumer benefit.[2]

Rather, applying those duties to data access platforms would be unreasonable given the lack of consumer benefit and the extremely high costs of compliance, which are discussed later in this comment. And it would have the unintended, adverse consequence of creating differences in the parallel consumer records retained by the data access platform and as compared to the consumer's account-holding institution. As noted in the John Doe illustration above, Method relays real-time, consumer-permissioned data directly from the data provider with each consumer authorization, and retains the data from each of those "pulls" for record retention purposes. If John Doe in the illustration above disputed the data from one "pull" but not the other, an error correction would create differences in what should otherwise be identical, parallel records.[3]

Under § 1681i(a)(2)(A) of the FCRA, a CRA is also required to notify a furnisher of disputed information "at the address and in the manner established with the [furnisher]." But data access platforms like Method operating under Section 1033 of the Dodd-Frank Act would not have an agreed-on address and manner of notification, making compliance confusing and difficult. And given that there are tens of thousands of data providers in the Section 1033 marketplace that would be "furnishers" under a potential FCRA rulemaking, requiring data access platforms to establish an agreed-on notification address and manner with each would be remarkably burdensome, and especially so for small businesses.

---

[2] If a potential rulemaking considers data access platforms to be a CRA, it is unclear whether the Bureau would seek to resolve the futility issue by requiring an data access platform to respond to consumer disputes with a frivolous and irrelevant notice under § 1681i(a)(3). This would be insufficient for at least three reasons: (1) it could cause consumer confusion and potentially discourage them from disputing the issue directly with the data provider (furnisher) through well known, existing channels; (2) it does not resolve the underlying futility of considering data access platforms as CRAs; and (3) it still imposes extreme hardship and undue burdens on data access platforms, particularly smaller platforms.

[3] A potential rulemaking could also cause a divergent parallel record issue, and resulting consumer confusion, between a financial institution and a data aggregator, as noted in FN 5.

Consumers

As established during the SBREFA panel meetings, the law is complex and confusing even to sophisticated business parties. Average consumers cannot be expected to be familiar with the FCRA or its intricacies. They are likewise unfamiliar with the various types of entities—and the material differences among them—that are or may be subject to the FCRA as CRAs or furnishers. The vast majority of consumers may only have a vague notion that furnishers regularly provide information to CRAs who regularly provide that information to third parties.

A potential rulemaking that results in data access platforms like Method being a CRA would substantially increase that complexity and confusion, and cause potential harm to consumers under existing provisions of the FCRA. Section 1681g requires CRAs to provide certain disclosures to consumers such as: (1) a summary of rights, including the right to dispute information in the CRA's "file" and the CRA's duty to correct; and (2) all the information in the "file" itself.

The summary of rights disclosure could cause a mistaken belief in consumers that a dispute leading to a correction of information in the data access platform's "files" would be beneficial. But, as noted earlier, that data is never re-disclosed or reused. The data access platform's duty to correct would thus serve no purpose and add no consumer benefit. consumers may also be confused into thinking, to their detriment, that disputing the data with a data access platform is the only or the best way of filing a dispute when, in fact, better avenues exist.[4]

Second, the potential that a correction could lead to a data access platform having divergent parallel consumer records with different T&E data could confuse consumers who request their "file" under § 1681g. Consumers could be confused about what T&E data was actually provided to a data recipient (or a "user" under the FCRA) and what information was corrected. They could

[4] While a correction by the data access platform could mean that the financial institution (furnisher) had corrected their data, the process under the FCRA is indirect, lengthier, less effective, and potentially detrimental to consumers relative to existing processes (e.g., Regulations E and Z) for consumers to correct errors with their financial institutions. Moreover, in the Section 1033 context, data access platforms are typically relaying T&E data. For credit and debit cards, there already exists a commonly used, effective, and regulatorily required dispute and chargeback process that involves back-and-forth communications among the financial institution, consumer, and merchant. The dispute procedures in the FCRA are simply not designed to handle such T&E disputes. And given the punitive liability regime under the FCRA—through enforcement and private right of actions with fee shifting provisions and statutory damages with no showing of harm—financial institutions that could potentially be considered furnishers under a rulemaking would likely just "correct" the transaction rather than face a potential lawsuit, which would lead to losses (to both the FI and the merchant) and increase first-party fraud.

be further confused into thinking that the inconsistent parallel files might all be disclosed in future requests.[5]

Section 1033 "Covered Persons" as Furnishers

Furnishing is voluntary under the FCRA. Entities that choose to be furnishers are subject to complying with myriad requirements under the law. A potential rulemaking would substantively change this framework under the FCRA by forcing "covered persons" who comply with their requirement to provide financial data under Section1033 of the Dodd-Frank Act to be involuntary furnishers of that data under the FCRA. They would then be subject to the duties of furnishers, which, of course, they did not bargain for.[6]

Compliance with those requirements is burdensome, demanding a significant outlay of time, money, and other resources as described more fully later in this comment. The burdens are particularly onerous to smaller entities like community banks and credit unions for whom the outlay may be existentially prohibitive. Worse still, because they would be involuntary furnishers under a potential rulemaking, these data providers may not even be aware of their FCRA obligations, leaving them susceptible to enforcement actions and private litigation.

The points above highlight just some of the concerns, difficulties, and confusion that would stem from a proposed FCRA rulemaking in this space. What's more, these points only focus on disputes, which represents just a sliver of the FCRA's obligations. I would also once again point out, as we discussed during the SBREFA panels, that the application of a credit reporting rulemaking to real-time, one-time use consumer-permissioned data access platforms like Method will have other adverse and counterproductive consequences. To the extent that Method is

[5] Again, Method does not re-disclose or reuse any data. The larger point is that a potential rulemaking that encompasses data access platforms is inconsistent with the FCRA and consumers' understanding of it. A consumer could be further confused if they successfully disputed an error directly with their financial institution and then later requested their "file" under FCRA § 1681g from a data access platform that contained pre-dispute T&E data from that institution. If the institution did not know they were a furnisher under the FCRA and that the data access platform was a CRA, then they may not have communicated the correction to the platform (and even if they did, the requirement would be unnecessarily burdensome and absurd as to companies like Method who never re-disclose or reuse that data). The consumer could then have diverging parallel transaction records.

[6] In turn, this may cause them to seek ways to avoid providing this data to the detriment of consumers who authorized the release of the data—undermining the very purpose of the Bureau's efforts to implement Section 1033 of the Dodd-Frank Act—which consumers require to obtain products and services.

deemed a nationwide credit reporting agency under a future rulemaking, such a rule could actually require our company to collect *more* consumer data than we do today. As the Bureau noted in its SBREFA memo, nationwide consumer reporting agencies have certain obligations in circumstances in which they believe systemic issues are resulting in inaccurate data being reported about multiple consumers.[7] By definition, complying with this requirement would require Method to collect enough data to identify and notify any potentially impacted consumers in such an event. Similarly, if consumer-permissioned data platforms like Method will be required under the FCRA to correct consumer files when a consumer files a dispute, we will be mandated under statute to maintain that consumer's file for a significantly longer period of time than Method typically retains consumer data today. Both unnecessarily create risk of consumer harm due to a cyber event or privacy breach and convey no consumer benefit.

The Undue Burdens on Impacted Stakeholders will Acutely Impact Small Businesses

The proposals under consideration for this potential rulemaking would, if implemented, represent a significant and disproportionate compliance burden for smaller market entities without any meaningful gains to consumer benefits or protections. As one SER stated on the SBREFA panel, it would be "back breaking" for his company. Several other SERs agreed that a potential rulemaking could cause their business and many others to close their doors or consolidate to survive, threatening competition in the marketplace.

If data access platforms like Method were to become CRAs under a potential rulemaking, we would be required to: (1) hire staff with FCRA compliance expertise, including compliance and dispute resolution professionals with subject matter expertise; (2) provide ongoing FCRA training; (3) build operational processes; (4) build controls and ongoing monitoring, testing, and auditing to ensure compliance; and (5) as noted earlier, build and maintain the technical resources required to gather and store additional consumer data.

While Method does not have corresponding cost estimates, the resources required to implement these would be massive. For an early-stage, small business start up like ourselves, it would be extremely difficult to meet core business needs and to grow the company given the allocation of substantial resources to satisfy these burdens.

[7] For Method, such an event would be exceedingly rare. As noted before, Method has a formatting success rate of 99.9999%.

The CFPB Should Exclude Data Access Platforms from any Future FCRA Rulemaking

Method urges the CFPB to mitigate the potential adverse impacts outlined above and shared during the SBREFA panels by carving out from any potential FCRA rulemaking entities that: are consumer-permissioned data access platforms that simply serve conduit functions in obtaining and relaying real-time data directly from a data provider to be used for the sole purpose authorized by consumers, and who do not re-disclose or reuse consumer data or maintain consumer "files" for the purpose of doing so.

There exists a wide range of regulatory precedent supporting this approach. The Federal Trade Commission's ("FTC") 2011 report, *40 Years of Experience with the Fair Credit Reporting Act*, specifically asserts that "[a]n entity that performs only mechanical tasks in connection with transmitting consumer information is not a CRA because it does not assemble or evaluate information."[8] This so-called "conduit function" exclusion from the FCRA has for the last two decades allowed, by the CFPB's own estimations, more than 100 million consumers to electronically share access to their financial data in order to receive the benefit of a more competitive financial product, service, or tool. Further, the 2011 Report advises that a software provider that allows companies to obtain credit report information "is not a CRA" because it itself is not assembling or evaluating any information; though the company using the software may be. Such is the case with a software provider like Method.[9-10]

Most critically, the CFPB proposed in late October a sweeping rule implementing Section 1033 of the Dodd-Frank Act that would create a legally binding consumer financial data access right in the United States. Method is a strong supporter of the Bureau's efforts to implement Section 1033 of the Dodd-Frank Act and notes that rule will, once finalized, require consumer-permissioned data access platforms like Method as well as consumer-permissioned third parties, like our Partners who use our platform service, to comply with a litany of consumer consent, disclosure, data privacy, and data security standards, including elements of the Gramm-Leach-Bliley Act and the FTC's Safeguards Rule. Having only had a short period of

[8] *See* Fed. Trade Comm'n, *40 Years of Experience with the Fair Credit Reporting Act: An FTC Staff Report with Summary of Interpretations*, at 29 (2011).

[9] *Id.* This provides more support for the distinction between data access platforms like Method, on the one hand, and data brokers on the other. Method provides a service to its Partners to facilitate access to real-time data directly from the data provider, whereas data brokers themselves assemble the data to create and maintain a consumer file and sell that file as a product.

[10] Moreover, the T&E data accessed through Method's platform is not a "consumer report" under the FCRA's exception for a "report containing information solely as to transactions or experiences between the consumer and the person making the report." § 1681a(d)(2)(i).

time to review the Bureau's Section 1033 proposed rule, it is impossible to analyze how that rule and the credit reporting rulemaking contemplated by the CFPB in its SBREFA memo would interact, though it seems clear that the consumer protections the Bureau is seeking in the consumer-permissioned data access space are more appropriately effectuated under Section 1033 than under a potential FCRA rulemaking.

Conclusion

Once again, Method greatly appreciated the CFPB's invitation to participate as a SER in its credit reporting SBREFA panels. I hope that our feedback during this process has been beneficial to the Bureau in distinguishing between the characteristics of entities, like Method, that operate with full consumer consent and control, that do not assemble consumer records nor evaluate them, and do not sell, market, or maintain consumer data for the purpose of furnishing or using that data outside of the strict use case for which the consumer has provided their authorization.

While we are strongly aligned with the Bureau's desire to ensure that consumers have control over and transparency into their data when permissioning access to their data for credit decisioning use cases or other permissible purposes, we do not believe that requiring consumer-permissioned data access platforms like Method to become credit reporting agencies will provide the consumer benefits the CFPB is seeking. On the contrary, such a decision would create significant consumer and stakeholder confusion, add substantial market complexity, and meaningfully over-burden smaller entities. Instead, the CFPB should exempt consumer-permissioned data access platforms like Method from any future FCRA rulemaking.

Thank you for your consideration of our perspectives. We welcome any opportunity to discuss these issues further.

Sincerely,

/s/ *Phil Chang*
Phil Chang
General Counsel