TECHNET
THE VOICE OF THE
INNOVATION ECONOMY

1420 New York Avenue NW, Suite 825
Washington, D.C. 20005
www.technet.org | @TechNetUpdate

November 7, 2023

Via electronic delivery to: CFPB_consumerreporting_rulemaking@cfpb.gov

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

Re: TechNet response to the Consumer Financial Protection Bureau's Outline of Proposals and Alternatives Under Consideration for Consumer Reporting Rulemaking

To whom it may concern:

TechNet appreciates the opportunity to comment on the Consumer Financial Protection Bureau's (CFPB or the Bureau) outline of proposals regarding consumer reporting (the Outline). We are concerned that rules promulgated in alignment with the Outline will have significant and negative consequences across a wide array of financial, commercial, and technological sectors, potentially impacting consumers and small businesses. Specifically, the suggested scope of activity that would be subject to the *Fair Credit and Reporting Act* (FCRA) significantly exceeds the extent of the statute and would be disruptive to the innovation economy.

TechNet is the national, bipartisan network of technology CEOs and senior executives that promotes the growth of the innovation economy by advocating a targeted policy agenda at the federal and 50-state level. TechNet's diverse membership includes dynamic American businesses ranging from startups to the most iconic companies on the planet and represents over 4.2 million employees and countless customers in the fields of information technology, e-commerce, the sharing and gig economies, advanced energy, cybersecurity, venture capital, and finance.

Consumers must be confident that their data and privacy are protected no matter where they live, and businesses across industries need regulatory certainty about consumer data to thrive in the innovation economy. We agree that transparency on the impact of data brokers is important for marketplaces and consumers. However, we are concerned that the proposed policy changes in the Outline would ultimately cause confusion and uncertainty for businesses and consumers alike.

The CFPB's broad conception of data brokers and credit reporting agencies greatly exceeds the intent of the FCRA. For example, the CFPB proposes to label as "data

brokers" those "that interact with consumers directly."[1] However, the CFPB also acknowledges that the FCRA's text excludes from the definition of "consumer report" the information that relates to "transactions or experiences" between consumers and the entity compiling that information.[2] In light of its conflicting comments concerning the rule's coverage of first-party data brokers, the CFPB should clarify that, in fact, first parties who share only this "transaction or experience information" would not be considered and regulated as "data brokers" because of the FCRA's statutory exception.

Additionally, by attempting to generally label data brokers as credit reporting agencies, the CFPB would embrace an approach that no other federal or state institution has sought to use in regulating data brokers. Both federal and state legislation on this subject has routinely pursued a narrower, targeted, and consensus-based definition of data broker that focuses on the elements of selling and licensing data and excludes more marginal transactions – providing clear awareness and guidance to consumers and companies alike. Congress has taken a carefully targeted approach of focusing on the specific types of sensitive data that it seeks to protect and the relationship that selling entities may have with respect to the consumer whose data they are sharing. For example, Congressional attention has been either on the sale of data relating to specific sensitive matters like personal location or health or on the lack of a direct connection between consumers and the entities selling or licensing consumer data.[3]

States have taken a similar path. For example, California, Vermont, Oregon, and Texas have enacted legislation that defines a data broker, in essence, as a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship.[4] Furthermore, in other draft bills on data brokers, multiple states have pursued definitions that directly align with this narrowed approach, including, but not limited to, Delaware, Massachusetts, and Washington.[5] The Bureau's expanded concept of

---

[1] Consumer Financial Protection Bureau, "Small Business Advisory Review Panel for Consumer Reporting Rulemaking Outline of Proposals and Alternatives Under Consideration," September 2023. *See* page 7, note 19.

[2] *Id.*, compare page 7, note 19 (defining "data brokers" to include those "that interact with consumers directly") with page 8, note 20 (explaining the "transactions or experiences" exception in the FCRA).

[3] *See e.g.*, *Health and Location Data Protection Act of 2022* (S.4408); *Data Broker List Act of 2021* (S.2290).

[4] Specifically, California defines a data broker as "a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship." Cal. Civ. Code § 1798.99.80. Vermont, which uses a slightly broader definition, defines a data broker as "a business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship." 9 V.S.A. § 2430(4). Oregon has adopted a similar definition, defining a data broker as "a business entity or part of a business entity that collects and sells or licenses brokered personal data to another person." Oregon House Bill 2052 § 1(1)(c)(A) (2023 Reg. Sess.). *See also* Tex. Bus. & Com. § 509.001(4).

[5] *See e.g.*, Delaware House Bill 262 (2021) § 12D-101(4), Massachusetts Information Privacy and Security Act, Senate Bill 227 (2023) § 93M(2), and Washington Senate Bill 5813 (2022) 42.56 RCW § 201(8).

data brokers is also broader than what Congress has considered in its own efforts to address data brokers.

Accordingly, TechNet would encourage the CFPB to reconsider this unconventional approach so as to avoid contributing to the existing regulatory patchwork problems impacting consumer privacy issues and, instead, work to develop proposals that harmonize with the more uniform and targeted approach taken by state and federal legislators across the country. In particular, TechNet would encourage the CFPB to consider a definition of data brokers that focuses on such entities that (1) knowingly collect and (2) sell or license the covered personal information to third parties. Additionally, the CFPB's definition of a data broker should exclude entities processing data that are already covered by the *Gramm-Leach-Bliley Act*, as most of the states already regulating data brokers have done.

Further, current application of the FCRA, which is based on a long-established statutory framework, would fundamentally change under the regulatory proposals contemplated by the outline. We are troubled by the expanded use of credit header data, which falls outside the statutory definition of data contained in a consumer report as defined by the FCRA and Congress. Additionally, the CFPB has not made clear that the sharing of certain types of data is necessary to achieve its aim of protecting consumers; specifically, aggregated and anonymized data should not be subject to the FCRA due to the nature of the activity. Privacy and other data protection restrictions also typically do not apply to data transfers that are specifically directed by the customer (e.g., data necessary to process a payment that a customer has specifically directed) so that the consumer can, in fact, receive the requested services. Adding written instructions or consumer consents and revocations, such as the Outline suggests, would add additional and unnecessary complexity here.

Data transfers that are designed to help identify and mitigate fraud and other conduct by bad actors are also critical use cases, and restrictions on those uses will detrimentally impact consumers. In these pro-consumer situations, the businesses that send or receive data for these purposes should not be captured by requirements directed to actual "data brokers." Additionally, data aggregators that are acting as a pass-through should not be considered data brokers if the third-party access they are enabling is not associated with a permissible purpose under the FCRA.

Standard customer-facing firms that interact with data to support their customers and users, engage in lawful advertising, and work to improve their services, and that do not sell customer data to third parties should also not be captured by proposals stemming from the Outline. Similarly, the CFPB should continue supporting data activities that provide meaningful consumer benefits and pose little to no risk to consumers. For example, first parties' collection and processing of accurate information can enrich the consumer experience with financial products and services. The use of consumer financial information for internal operations or

lawful advertising can also help companies improve their service and product offerings, resulting in greater customer satisfaction without creating privacy risks for consumers. Also, any proposal that imposes restrictions on the use of credit header data should include exceptions for important healthcare services and fraud prevention purposes.[6]

Instead, we encourage the CFPB to focus its attention on addressing high-risk data practices such as the sale of consumer financial data without the proper diligence of purchasers, the sale of financial data used to deny consumers of important services or economic opportunities, and the sale of consumer financial data for purposes outside the terms by which it was originally collected and in ways that have substantial impacts on consumers, to the extent those data activities fall within the CFPB's jurisdiction.

Private sector efforts are empowering consumers to better manage their financial lives and enjoy new, safe, secure, inclusive, and reliable financial tools. TechNet supports rulemaking that would allow consumers the right to access and share their financial records and securely request that their financial information be accessed and shared with approved third parties by aligning data definitions, rights, and responsibilities with general principles of privacy and data protection laws. To that end, we look forward to engaging on the CFPB's rulemaking on consumer data privacy. However, we are concerned that the CFPB's efforts to regulate consumer reporting, as explained in the Outline, could undermine these efforts and create avoidable confusion. We urge the CFPB to provide clarity about the process for consumer financial data and consumer reporting rulemaking as soon as possible.

The current landscape of state privacy laws is already creating a conflicting patchwork of privacy rules that confuse consumers and hurt our nation's innovators, particularly small and medium-sized businesses. Congressional action, rather than a CFPB rule, is the best approach to crafting federal privacy protections, as Congress can expressly preempt state laws and ensure that the enforcement of clearly delineated national privacy rules is conducted by authorities with relevant expertise. According to a recent study by ITIF, if Congress does not pass a federal privacy law, it could result in costs of over $1 trillion to our economy over ten years, with small businesses bearing $200 billion of that cost.[7] We are concerned that a potentially overly broad rulemaking from the CFPB, pursuant to the FCRA, could undermine innovation across the U.S. by adding to the existing patchwork of privacy laws rather than creating a single, coherent consumer data use framework. Instead, concerns about insufficient preemption are warranted considering the CFPB's issuance of an interpretative rule, which seeks to clarify that the "FCRA's express preemption provisions have a narrow and targeted scope" and that states

[6] For example, credit header data may be used to identify patients, identifying underserved populations for personalized and preventative care, patient matching, and contact tracing and emergency prevention.
[7] Information Technology & Innovation Foundation, "The Looming Cost of a Patchwork of State Laws," January 2022.

"retain substantial flexibility" to enact additional rules and regulations beyond the bounds of the FCRA.[8]

Congress and federal agencies should update outdated laws and rules in order to utilize modern financial technologies and meet consumer and business demand for innovative financial products. While TechNet appreciates the CFPB's interest in consumer data protection, we urge the Bureau to refrain from overly broad rulemaking that would ultimately harm consumers and create market uncertainty. We are deeply concerned that the proposals in the Outline would likely have the opposite effect of its intended purpose by leaving consumers in a greater state of uncertainty as to who is collecting and using their information and why.

Thank you for your attention to our views on this matter.

Sincerely,

Carl Holshouser

Carl Holshouser
Senior Vice President

[8] 12 CFR Part 1022, "The Fair Credit Reporting Act's Limited Preemption of State Laws."