

December 29, 2023

Rohit Chopra  
Director  
Consumer Financial Protection Bureau  
1700 G Street NW  
Washington, District of Columbia 20552

**RE: Comments of ACT | The App Association on the Consumer Financial Protection Bureau's Required Rulemaking on Personal Financial Data Rights (Docket No. CFPB-2023-0052; 88 FR 74796)**

Dear Director Chopra:

ACT | The App Association (the App Association) appreciates the opportunity to provide input to the Consumer Financial Protection Bureau (CFPB or Bureau) in response to its proposal to implement personal financial data rights under the Consumer Financial Protection Act of 2010 (CFPA) by request for comments on consumer access to financial account and account-related data in usable electronic form, including access by entities acting with consumer permission, in connection with the provision of products or services that make use of that information.<sup>1</sup>

## **I. Statement of Interest & General Comments**

In general, the App Association supports a Bureau rulemaking that would promote and effectuate stronger consumer access rights and choice regarding how and where consumers can leverage their own financial data. With this rulemaking, the Bureau has an incredibly important opportunity to ensure that data that consumers generate about themselves through their financial transactions and other activities is accessible and portable, instead of hidden behind walled gardens erected by legacy financial institutions. The Bureau should enable a more competitive financial services marketplace through the use of open application programming interfaces (APIs) that allow consumers to more effortlessly tap into the deep reservoir of beneficial use cases offered by innovative financial technology companies and non-traditional financial institutions.

The App Association is a global trade association for small and medium-sized technology companies. We work with and for our members to promote a policy environment that rewards and inspires innovation while providing resources that help them raise capital, create jobs, and continue to build incredible technology. Today, the value of the ecosystem the App Association represents—which we call the app economy—is approximately \$1.7 trillion and is responsible for 5.9 million American jobs.<sup>2</sup> As the world has quickly embraced mobile technology, our member companies have been creating innovative solutions that power the growth of the internet of things (IoT) across modalities and segments of the economy.

---

<sup>1</sup> 88 FR 74796.

<sup>2</sup> <https://actonline.org/2022/09/30/act-the-app-association-report-reveals-apps-contributed-e210-billion-to-the-eu-economy-in-2021/>.

The App Association fought for greater consumer access to data over the last few years, a battle that has carried us across numerous policy spheres as data became a touchpoint of numerous consumer industries. For example, the App Association’s Connected Health Initiative has played a key role in shaping and supporting the Centers for Medicare & Medicaid Services’ (CMS)<sup>3</sup> and Office of the National Coordinator for Health Information Technology’s (ONC)<sup>4</sup> past rulemakings on patient data interoperability and information blocking, which raise numerous parallel issues to those the CFPB now confronts. In the health context, traditional healthcare providers operate similarly to banks in the financial sector, historically creating a bottleneck for patient healthcare data that prevents timely and informed care coordination and decision-making. As a result, the App Association supported the creation of APIs that, informed by transparency in data usage, allow the sharing of patient-generated health data between and amongst providers and patients, as well as between other important stakeholders who have a role in improving care coordination and decision-making. We advocate for a similar solution here.

## **II. App Association Recommendations for Implementation of Section 1033, and for Making Financial Information Available to Consumers**

### *A. Benefits to Consumers from Authorized Access to Their Data*

As a principle, the App Association believes that seamless consumer access to data, both direct and authorized, is necessary. Consumers generate data every day that outlines the intimate experiences and transactions that constitute their lives. Consumers ought to be able to access, control, and transport such data that they generate from simply existing in and interacting with the world. We believe that principle is consistent with the Bureau’s statutory mandate under Section 1033.

On a practical level, improved consumer access to data would allow users to make informed decisions and to more easily access the great diversity of products and services in the financial technology marketplace that offer novel solutions to evolving consumer banking needs in the digital age. The opportunities for consumers in the open market are enormous. Financial technology applications can improve consumer access to credit using data points that traditional lenders overlook<sup>5</sup>; they can allow consumers to budget and receive personalized tips in real time<sup>6</sup>; and they can send consumers sophisticated analytics tailored specifically to them and their goals.<sup>7</sup> Moreover, while the use-cases that already exist in a semi-restricted marketplace are incredibly promising, and there is no telling what new types of beneficial use-cases would be developed as more data is made available.

---

<sup>3</sup> *Connected Health Initiative, Comments to CMS on Docket No. CMS-9115-P. Submitted June 3, 2019.* <https://static1.squarespace.com/static/57ed48b4f5e23125aa094623/t/5cf57ba1dc8dc60001aa2d9e/1559591845651/CHI+Comments+re+CMS+Interop+Rule+%28final%29+%28060319%29.pdf>

<sup>4</sup> *Connected Health Initiative, Comments to ONC on Docket No. CMS-9115-P. Submitted June 3, 2019.* <https://static1.squarespace.com/static/57ed48b4f5e23125aa094623/t/5cf57c627c6a3e00016b6f61/1559592037688/CHI+Comment+Cover+Ltr+re+ONC+Info+Blocking+Rule+%28final%29+%28060319%29.pdf>

<sup>5</sup> *Aite, “Alternative Data Across the Loan Life Cycle: How FinTech and Other Lenders Use It and Why.” 2018.* [https://www.experian.com/assets/consumerinformation/reports/Experian\\_Aite\\_AltDataReport\\_Final\\_120418.pdf?eqlqTrackId=7714eff9f5204e7ca8517e8966438157&elqaid=3910&elqat=2](https://www.experian.com/assets/consumerinformation/reports/Experian_Aite_AltDataReport_Final_120418.pdf?eqlqTrackId=7714eff9f5204e7ca8517e8966438157&elqaid=3910&elqat=2)

<sup>6</sup> *PwC, Global FinTech Report 2019: “Crossing the lines - How fintech is propelling FS and TMT firms out of their lanes.” 2019.* <https://www.pwc.com/gx/en/industries/financial-services/assets/pwc-global-fintech-report-2019.pdf>

<sup>7</sup> *Ibid.*

To effectuate greater consumer access to data, the Bureau could use its Section 1033 rulemaking authority to require data holders to make any data a consumer can access directly available to authorized third parties through open APIs, a variation of a scheme already successfully implemented in the United Kingdom.<sup>8</sup> This would help avoid a continuation of the status quo, whereby third parties must negotiate tokenized access individually with every data holder, who enjoy virtually all of the leverage in such negotiations. In a relatively decentralized financial services sector that includes nearly 4,500 federally-insured depository institutions, such negotiations are incredibly laborious and are almost certain to leave large portions of the public unable to benefit from data access.

Of course, smaller financial institutions, such as community banks and credit unions, may struggle to update their legacy software and databases to accommodate an open API straight away. For this reason, the App Association would suggest that the Bureau contemplate alternatives to open API participation in the interim for these smaller institutions, including permitting a certified credentials-based access regime or another access model.

### *B. Access to Consumer Data's Impact on Competition and Innovation*

As the Bureau is aware, the current data access regime involves a mixture of informal credentials-based access agreements and formalized, token-based access agreements. This system is complicated to navigate for both consumers and third parties and often allows traditional financial institutions to impose their will regardless of consumer welfare.

Indeed, some stakeholders, such as banks and brokerage firms, have chosen to prevent consumers from authorizing third parties to access their account information, severing their customers from their preferred services. For example, beginning in 2019, PNC prevented customers from connecting their bank accounts to the peer-to-peer payment platform Venmo, instead directing their users to a competing platform, Zelle, which is owned by a consortium of large banks, including PNC.<sup>9</sup> This type of self-preferential behavior reduces competition, while at the same time offering consumers an illusory choice to leverage third-party service providers that in reality only operate on the banks' terms. Consumers ultimately lose out.

Moreover, the complexity of the current scheme preferences large data aggregators over smaller data users. As the Bureau notes in its outline, individual consumers and third-party data users that seek to negotiate data access to a large number of data holders in lieu of individually negotiating each agreement often turn to large aggregators to provide that service. Smaller data users often do not possess the means or legal expertise to negotiate bilateral agreements on their own and may be more reliant on large data aggregators than others. An open API would ease this burden and reduce smaller firms' reliance on intermediary players in the space.

---

<sup>8</sup> Alice Prahmann, Franziska Zangl, Oliver Dlugosch, Stefanie Milcke, "Open Banking APIs Worldwide". September 2019. <https://www.openbankingexpo.com/wp-content/uploads/2019/09/ndgjit-Open-Banking-APIs-worldwide-Whitepaper.pdf>

<sup>9</sup> Yuka Hayashi, "Venmo Glitch Opens Window on War Between Banks, Fintech Firms", Wall Street Journal. December 14, 2019. <https://www.wsj.com/articles/venmo-glitch-opens-window-on-war-between-banks-fintech-firms-11576319402>.

### C. *Extent to Which Access to Consumer Data Pursuant to Section 1033 Raises Privacy Concerns*

To the extent that the Bureau opts to increase access to consumer financial data with this rulemaking, there is the unfortunate potential for unscrupulous actors to use apps to profit from an individual's information in ways that the individual did not authorize or understand. App Association members include leading consumer financial app developers who build transparency and privacy concepts into their innovations "by design" as a matter of principle and ethics. Our members condemn the unethical or illegal sharing of sensitive financial information with third parties, particularly when it is done without the knowledge and consent of an individual. If consumers access their and their family's financial data—some of which are likely sensitive—through a smartphone, users should have a clear understanding of the potential uses of that data by developers. Otherwise, most users will not be aware of who has access to their information, how and why they received it, and how it is being used. The downstream consequences of using data in this way may ultimately erode a user's privacy and willingness to disclose information to his or her financial services provider. The App Association believes that it is in the best interest of the consumer/user to understand how their data is being used.

At the same time, the small business developer community the App Association represents already practices responsible and efficient data usage to solve problems identified across consumer and enterprise use cases. Since the inception of the General Data Protection Regulation (GDPR) in Europe, the California Consumer Privacy Act (CCPA), and the subsequent adoption of similar measures around the country and the world, our members have responded to evolving consumer expectations and enhanced market competition by meeting and, in many cases, exceeding relevant legal requirements. These efforts include the utilization of cutting-edge privacy-by-design approaches from the earliest phases of product development and the most advanced tools and methodologies available, such as differential privacy techniques.<sup>10</sup> We welcome such regulation, as complying with GDPR and CCPA has given some of our members a competitive advantage over competitors who are not compliant and typically creates new opportunities through a thorough review of organizational processes. The App Association appreciates and shares the Bureau's interest in protecting user privacy. Consumers around the world rely on our members' products and services, with the expectation that our members will keep their valuable data safe and secure. Despite the protestations of traditional financial institutions attempting to retain their ironclad grip over consumer financial data, our members' commitment to privacy and security is robust, as evidenced above.

Like ONC<sup>11</sup> and CMS<sup>12</sup> have, the Bureau should establish a framework outlining high-level data privacy and security guardrails that addresses individual access; data collection, uses and disclosures; consent and authorization; breach mitigation procedures and consumer notice; and security practices. Such requirements should be based on demonstrated risks to consumers, with technology-neutral measures, scaled to the levels of risk presented, as means for compliance. Such guardrails should ensure that consumers are oriented to the risks of sharing their financial data with third parties that are not financial

---

<sup>10</sup> *Differential Privacy*, HARVARD UNIVERSITY PRIVACY TOOLS PROJECT. <https://privacytools.seas.harvard.edu/differential-privacy> (last visited 17 February 2023).

<sup>11</sup> *Office of the National Coordinator for Health Information Technology, Information Blocking and the ONC Health IT Certification Program: Extension of Compliance Dates and Timeframes in Response to the COVID-19 Public Health Emergency*. October 2020. <https://www.federalregister.gov/documents/2020/11/04/2020-24376/information-blocking-and-the-onc-health-it-certification-program-extension-of-compliance-dates-and>

<sup>12</sup> *Centers for Medicare & Medicaid Services, "Patient Privacy and Security Resources – Supporting Payers Educating their Patients."* December 2020. <https://www.cms.gov/files/document/patient-privacy-and-security-resources.pdf>

institutions and better equip the Federal Trade Commission to hold third parties to sound privacy and security practices.

The App Association also notes that if a company is selling and/or sharing user data, that company should clearly explain why and how that data is being shared (in plain language, as opposed to unnecessarily long and complicated end-user license agreements), and how it will be used so that the consumer can make an informed decision and provide affirmative consent mechanisms for certain uses.

### **III. Conclusion**

We thank the CFPB in advance for its consideration of our views. We are committed to helping the Bureau actualize the benefits that will flow from consumers enjoying strong access rights and choice regarding their financial data. We look forward to engaging further in the future.

Sincerely,



Brian Scarpelli  
Senior Global Policy Counsel

**ACT | The App Association**  
1401 K St NW (Ste 501)  
Washington, DC 20005