January 26, 2021

Dave Uejio,
Bureau of Consumer Financial Protection,
1700 G Street NW,
Washington, DC 20552.

Dear Mr. Uejio,

On behalf of the Center for Data Innovation (datainnovation.org), we are pleased to submit comments in response to the Consumer Financial Protection Bureau's ("the Bureau's") request for comment on its Advance Notice of Proposed Rulemaking (ANPR) on developing regulations to implement section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act, which provides for consumer access to financial records.[1]

The Center for Data Innovation is the leading think tank studying the intersection of data, technology, and public policy. With staff in Washington, D.C., and Brussels, the Center formulates and promotes pragmatic public policies designed to maximize the benefits of data-driven innovation in the public and private sectors. It educates policymakers and the public about the opportunities and challenges associated with data, as well as important data-related technology trends. The Center is a non-profit, non-partisan research institute affiliated with the Information Technology and Innovation Foundation.

SUMMARY

Some traditional financial institutions, such as banks and brokerage firms, limit consumers from allowing authorized third parties to access their account information online without any legitimate business justification, restricting competition, reducing market transparency, and harming consumers.

Many of these data holders resist sharing due to a fear that third parties (defined by the Bureau as 'data users') will disrupt and circumvent their relationship with their customers, such as by notifying customers of opportunities to reduce bank fees by using an alternative financial institution. Restrictions on third-party access to the online services or application programming interfaces (APIs) of traditional financial institutions undermines the development and adoption of emerging financial technology (fintech) services that provide

[1] "Advance Notice of Proposed Rulemaking: Consumer Access to Financial Records", Federal Register, November 06, 2020, https://www.federalregister.gov/documents/2020/11/06/2020-23723/consumer-access-to-financial-records.

innovative new financial services for a wide range of consumers, including low-income ones who are underserved by traditional financial institutions. This has led to a fragmented banking landscape, with some Americans having access to the innovative financial services third parties offer, and others blocked from doing so by their banks.

One way the Bureau can ensure all Americans have access to these emerging fintech services is by requiring regulated financial institutions to maintain open APIs that provide access to consumer account information. In particular, the Bureau should require data holders make any data a consumer can access directly through their portal available to authorized third parties through APIs.

The Bureau is uniquely positioned to strike the right balance to ensure that open API rules protect the legitimate interests of banks, such as not imposing undue costs, creating unnecessarily complex technical requirements, or exposing financial systems to significant security threats, while also ensuring open APIs are a pathway for the type of technological innovation that will unlock more value for consumers.

Please find our responses to the relevant questions in the attached document

Sincerely,

Daniel Castro
Director
Center for Data Innovation
dcastro@datainnovation.org

Hodan Omaar
Policy Analyst
Center for Data Innovation
homaar@datainnovation.org

A. BENEFITS AND COSTS OF CONSUMER DATA ACCESS

1. What are the benefits to consumers from authorized data access? What are the benefits to consumers from direct access? What specific regulatory steps by the Bureau would enhance those impacts and how would they do so?

The benefits from these services have led to the sharp growth of fintech companies—businesses using innovative technology to improve financial services. For example, mobile banking (such as using a banking app) was the primary method consumers used to access their bank accounts in 2019—more popular than telephone banking, online banking (using a computer or tablet), visiting a bank teller, and using an ATM or bank kiosk. Indeed, mobile banking has grown popular quickly with 34 percent of Americans accessed their bank accounts using mobile banking in 2019, compared to only 9 percent of Americans accessed their bank accounts using mobile banking in 2015.[2]

While many consumers use mobile banking apps from their financial institutions, many others prefer to use third parties to manage their financial accounts for a variety of reasons. First, customers can manage multiple bank accounts through a single application, and thereby gain a single solution to view their finances.[3] Second, bank customers can use third-party apps to more easily move funds between savings and checking accounts, to avoid overdraft fees, or to take advantage of higher interest rates. Third, customers can use this data to compare financial services based on their own usage patterns and get more personalized financial advice. Fourth, customers can forecast their cash flow (and again avoid overdraft charges). Fifth, consumers and businesses can allow lenders to review their transaction history to assess their credit worthiness.

To ensure that consumers can continue to gain access to these third-party tools, the Bureau should require that financial institutions not limit access to any customer account data that a consumer can access directly. In essence, a consumer should be able to authorize access for a third party to any of their account data that they themselves are able to access directly. As discussed in more detail later, this requirement should exclude the financial institution's proprietary data or data it has acquired from third parties.

---

[2] Federal Deposit Insurance Corporation (FDIC), *How America Banks: Household Use of Banking and Financial Services, 2019 FDIC Survey* (Washington DC, October 2020), 4, https://www.fdic.gov/analysis/household-survey/2019report.pdf.

[3] Daniel Castro and Michael Steinberg, "Blocked: Why Some Companies Restrict Data Access to Reduce Competition and How Open APIs Can Help" (Center for Data Innovation, November 2017), https://www2.datainnovation.org/2017-open-apis.pdf.

2. How does authorized data access facilitate competition and innovation in the provision of consumer financial services? What are the impacts of direct access on such competition and innovation? What specific regulatory steps by the Bureau would enhance that impact and how would they do so?

When financial institutions block third parties from accessing authorized financial data on behalf of a customer, they reduce competition and opportunities for innovation.

Blocking third-party tools reduces competition because not only do third parties help customers better understand their budgets and spending patterns, but they also identify opportunities for their users to reduce their fees for financial services by using alternative products—the reason some financial institutions may choose to block these services.[4] Additionally, if users are spending more time on these third-party sites and apps, there are fewer opportunities for traditional financial institutions to engage their customers to promote additional services. Indeed, according to a 2020 survey of leaders from 543 unique banks nationwide, 76 percent of financial institutions believe that they are losing revenue to emerging fintech companies.[5] When fintech companies threaten both banks' margins and, for some, even their long-term viability, it is understandable why some banks are resisting this disruption, even though it would ultimately benefit consumers.

Blocking third-party tools also limits data-driven innovation, reducing the number and quality of services available to consumers. For example, several fintech companies are using customer data and machine learning to develop new services that improve decision-making in finance. Fintech company Deserve, for example, is using machine learning to assess users' credit worthiness based on their potential future earnings rather than on traditional metrics that look at credit history, such as a FICO score.[6] This gives consumers that might not have a credit history, such as students or new immigrants, or those who want to rebuild their credit a chance to build their financial power. By requiring financial institutions to provide consumers the same level of access to their financial data whether they choose to access their information directly or through an authorized third-party, the Bureau can ensure there is a level playing field for all market participants. This will increase competition and innovation that benefits consumers.

---

[4] Daniel Castro and Michael Steinberg, "Blocked: Why Some Companies Restrict Data Access to Reduce Competition and How Open APIs Can Help" (Center for Data Innovation, November 2017), https://www2.datainnovation.org/2017-open-apis.pdf.

[5] Mark Jacobsen, "Bank Executive Business Outlook Survey 2019 Q4" (Promontory Interfinancial Network, 2019), https://www.promnetwork.com/media/250839/promontory-network-bank-executive-outlook-survey-q4-2019.pdf.

[6] Deserve company website, accessed January 20, 2021, https://www.deserve.com/about-us/.

3. What costs to consumers flow from authorized data access? What costs result from direct access? What specific regulatory steps by the Bureau would reduce any such impacts and how would they do so?

Both direct and authorized access carry security and privacy risks. But there is no more security risk in customers sharing online credentials with third-party tools than when these customers share this same information with personal assistants or family members.[7] In fact, unlike the average personal assistant or family member, most third-party tools use advanced security measures and customer login information to detect and prevent unauthorized use.

Indeed, the most prominent consumer financial data aggregators, such as Yodlee, Plaid, and Finicity, which supply data to many third-party tools, have robust security programs.[8] Some even undergo reviews by federal regulators, including the Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency (OCC), and the Federal Reserve.

Moreover, when financial institutions provide authorized third-parties access to customer data they can do so using stronger data security measures, such as by using token-based authentication which allows consumers to provide access to their online accounts without sharing their usernames and passwords.

Because the risks stemming from authorized access are commensurate with the risks to direct access, it is only right that financial institutions that leverage authorized access for their services be subject to the same privacy and data security requirements that those who leverage direct access are. In particular, the Bureau should expand the applicability of the Gramm-Leach-Bliley Act, which requires companies to explain their information-sharing practices to their customers and to safeguard sensitive data, to include fintech companies that obtain authorized access to consumer data from traditional financial institutions.[9]

---

[7] Daniel Castro and Michael Steinberg, "Blocked: Why Some Companies Restrict Data Access to Reduce Competition and How Open APIs Can Help" (Center for Data Innovation, November 2017) https://www2.datainnovation.org/2017-open-apis.pdf.
[8] "Financial Data Security," Envestnet Yodlee, https://www.yodlee.com/legal/yodlee-security/; "Security," Plaid, https://plaid.com/security/; "Security Leadership," Finicity, https://www.finicity.com/security/.
[9] Gramm-Leach-Bliley Act of 1999, S.900, 106th Cong. (1999).

4. What should the Bureau learn about the costs and benefits of authorized data access from regulatory experience in State jurisdictions or in jurisdictions outside the United States? What should it learn from such sources with respect to direct access? How should this inform the Bureau's consideration of specific regulatory steps that it might take to implement section 1033?

The opening up of the banking market—by regulators on one hand and market standards on the other—has already extended to more than 50 countries.[10] The United Kingdom, in particular, has implemented one of the most comprehensive open banking initiatives that is instructive for the United States.

In 2018, the UK's Competition and Markets Authority (CMA) committed the nine largest UK banks (CMA9) to implement pre-defined open APIs to drive competitive and innovation pressure in the financial sector. The CMA-initiated Open Banking Implementation Entity (OBIE) worked with banks, fintech companies, third party providers, and consumer groups, to create software standards and industry guidelines that drive competition and innovation in UK retail banking.[11] As a result of its efforts, the UK has been able to further cement itself as having one of the most intense banking markets in the world, with strong competition between a range of financial service providers and high levels of innovation.[12]

If the Bureau seeks to emulate the UK's results, it too should adopt comprehensive open banking initiatives through APIs. However, the Bureau should also be cognizant of the differences between the U.S. banking landscape and that of the UK. The CMA9's combined market share accounts for over 90 percent of the UK's consumer and small business bank accounts.[13] In the United States, the banking landscape is more diverse with many more smaller and medium-sized financial institutions serving a large percentage of the population. Indeed, according to the latest World Bank data, the banking concentration in the United States, defined as the assets of three largest commercial banks as a share of total commercial banking assets, was approximately 35 percent in 2017.[14] Overcoming the

[10] Alice Prahmann, Franziska Zangl, Oliver Dlugosch, Stefanie Milcke, "Open Banking APIs Worldwide", (ndigit, September 2019), https://www.openbankingexpo.com/wp-content/uploads/2019/09/ndgit-Open-Banking-APIs-worldwide-Whitepaper.pdf.
[11] UK Open Banking website, accessed January 21, 2020, https://www.openbanking.org.uk/about-us/.
[12] Alice Prahmann, Franziska Zangl, Oliver Dlugosch, Stefanie Milcke, "Open Banking APIs Worldwide", (ndigit, September 2019), https://www.openbankingexpo.com/wp-content/uploads/2019/09/ndgit-Open-Banking-APIs-worldwide-Whitepaper.pdf.
[13] "Who are the participating banks," accessed January 26, 2021, https://www.openwrks.com/what-is-open-banking/participating-banks.
[14] The World Bank, Global Financial Development Database, (bank concentration; accessed January 19, 2021), https://www.worldbank.org/en/publication/gfdr/data/global-financial-development-database.

challenges these banks would face in adopting new APIs, such as the fact that they are more likely to use legacy systems based on monolithic architecture and bespoke interfaces that would not support such API-integrations, will require a clear strategy at the federal level.

Like the UK's OBIE, the Bureau should establish an industry-led organization tasked with working with different stakeholders in the banking sector to design API specifications and support all banks to adopt these standards.

B. COMPETITIVE INCENTIVES AND AUTHORIZED DATA ACCESS

5. What reasons are there to believe that competitive incentives will facilitate or undermine authorized data access? What responsive actions should the Bureau take and why?

There are several examples of financial institutions limiting third parties from accessing customer data on behalf of their users that demonstrate the fragile partnership between financial institutions and third-party organizations. In 2015, for example, a number of leading U.S. banks briefly blocked financial data aggregators from accessing customer data, during which time customers of these banks were unable to use many third-party tools.[15] This limitation was quickly removed due to consumer backlash.[16] In 2017, Barclays bank acknowledged it was blocking some third-party apps and services, citing security concerns.[17] In 2019, PNC Financial Services Group blocked Plaid, a data aggregator that connects Venmo and thousands of other apps to financial institutions, from accessing customers' account and routing numbers.[18] PNC suggested that customers instead switch to Zelle, a payment app that it and other major banks operate jointly and that competes with Venmo.

These instances demonstrate the fear that many financial institutions have that fintech competitors will disrupt their relationship with their customers, as well as the distrust fintech companies have that large financial institutions may arbitrarily restrict their access. Without regulator intervention, these institutions may resist creating open APIs, limit the utility of the ones they create, or implement other technical or administrative hurdles to securely

[15] Daniel Huang and Peter Rudegeair, "Bank of America Cut Off Finance Sites From Its Data," *The Wall Street Journal*, November 9, 2015, https://www.wsj.com/articles/bank-of-america-cut-off-finance-sites-fromits-data-1447115089?mod=WSJ_TechWSJD_NeedToKnow%20Whoever.
[16] Brian J. Hurh et al. "Consumer Financial Data Aggregation and the Potential for Regulatory Intervention," *Paymentlawadvisor.com*. June 7, 2017, http://www.paymentlawadvisor.com/2017/06/07/consumerfinancial-data-aggregation-the-potential-for-regulatory-intervention/#_ftn5.
[17] Ethan Wolff-Mann, "A banking war over access to your data is stifling innovation," *Yahoo Finance*, September 28, 2017, https://finance.yahoo.com/news/banking-war-access-data-stiflinginnovation-143439973.html.
[18] Yuka Hayashi, "Venmo Glitch Opens Window on War Between Banks, Fintech Firms", The Wall Street Journal, https://www.wsj.com/articles/venmo-glitch-opens-window-on-war-between-banks-fintech-firms-11576319402.

accessing customer data. The Bureau is best positioned to address these issues by requiring banks implement open APIs and providing oversight of the implementation process.

6. Should the Bureau expect access-related agreements between data holders and other participants in the authorized data access ecosystem to impact competition and innovation favorably or unfavorably? How should the Bureau take account of such impacts in implementing section 1033?

Some financial institutions have begun to share data with third parties. They do so to leverage these companies' technologies and services to benefit their customers, while retaining opportunities to study overarching consumer spending patterns and sell their own financial products such as loans and wealth management services.[19] For example, in early 2017, JPMorgan Chase announced a partnership with Intuit, the company behind Mint, QuickBooks, and TurboTax, to allow Intuit to synchronize bank customers' personal banking data with Intuit apps through an API.[20] The API allows Intuit's developers to create apps and software that are compatible with the bank's systems, and that enables the two companies to securely and seamlessly transfer data. The partnership has also allowed the two companies to establish certain use and data sharing guidelines that protect consumers from unwanted marketers.[21] Other large banks, including Bank of America, Wells Fargo, and Capital One, have implemented similar agreements to allow third parties, such as tech companies and data aggregators, access to banks' APIs.

But with more than 10,000 banks and credit unions in the United States, there are still many financial institutions that do not effectively share access to customer data, and negotiating access on a one-to-one basis between different financial providers and fintech companies is unnecessarily costly and inefficient.[22] The Bureau should implement open API rules to ensure all Americans can benefit from innovative products and services.

---

[19] "Here's why U.S. banks are sharing data with fintechs." Business Insider, February 7, 2017, http://www.businessinsider.com/heres-why-us-banksare-sharing-data-with-fintechs-2017-2.
[20] Daniel Castro and Michael Steinberg, "Blocked: Why Some Companies Restrict Data Access to Reduce Competition and How Open APIs Can Help" (Center for Data Innovation, November 2017) https://www2.datainnovation.org/2017-open-apis.pdf.
[21] "Press Release: Chase, Intuit to Gove Customers Greater Control of Their Information," Intuit, January 25, 2017, https://www.intuit.com/company/press-room/pressreleases/2017/Chase-Intuit-to-Give-Customers-Greater-Control-of-TheirInformation/.
[22] Kurt Badenhausen, "The Best Banks And Credit Unions In Every State 2019", *Forbes*, June 25, 2019, https://www.forbes.com/sites/kurtbadenhausen/2019/06/25/the-top-banks-and-credit-unions-in-every-state-2019/?sh=6dd99a257f78.

C. STANDARD SETTING

7. Should the Bureau seek to encourage broad-based standard setting work by authorized data access ecosystem participants? If so, how should it do so?

To ensure API adoption is not fragmented across different geographies and there are not duplicative development efforts across different businesses, the Bureau should encourage market-led standards for open APIs.

In the EU, for example, the second Payment Service Directive (PSD2) has been successful because it has built upon the API framework of the industry-led Berlin Group, a pan-European payments interoperability standards and harmonisation initiative.[23] The Berlin Group has participation from major players in the payments industry in 21 different European countries. This consortium has developed an API framework, called the NextGenPSD2 Framework, that has become the leading standard for PSD2 and which, according to the European Banking Association, is now used by 78 percent of EU banks.[24]

The United States already has an equivalent non-profit consortium, called the Financial Data Exchange (FDX), which aims to unify the financial industry around a common and interoperable standard for APIs. FDX includes 168 members, including major U.S. banks, such as the Bank of America, Chase, and Wells Fargo, and leading fintech companies such as Plaid, Intuit, and Finicity.[25] The latest API framework was updated in 2020 to meet industry standards and older versions have been adopted by industry players that cater to almost 12 million U.S. consumers.[26] The Bureau should work closely with FDX in the design of an open banking ecosystem.

D. ACCESS SCOPE

8. How might the Bureau protect against the exposure of confidential commercial information, information that must be kept confidential by law, or information collected for the purpose of preventing fraud or other illegal conduct while at the same time protecting

---

[23] The Berlin Group website, accessed January 21, 2020, https://www.berlin-group.org/.
[24] Hakan Eroglu, "Berlin Group and the way to PSD3", *MoneyToday.ch*, December 5, 2018, https://www.moneytoday.ch/news/berlin-group-und-der-weg-zur-psd3/.
[25] "Members", accessed January 21, 2020, https://financialdataexchange.org/FDX/The%20Consortium/FDX/The-Consortium/Members.aspx?hkey=362ecd23-b752-48aa-b104-a99e916276c8.
[26] "The Financial Data Exchange Releases First Major Update to FDX API, Makes Fourth Version Available," last modified March 19, 2020, https://financialdataexchange.org/FDX/News/Announcements/financial-data-exchange-releases-first-major-update-to-fdx-api-makes-fourth-version.aspx?WebsiteKey=deae9d6d-1a7a-457b-a678-8a5517f8a474.

the access rights provided in section 1033? Should the Bureau's approach differ depending on whether data is accessed by authorized third parties or directly?

There will be no additional risk of exposing confidential or commercial information if the Bureau only requires financial institutions to share the customer account data that consumers already have direct access to through their bank's online portal. Financial institutions should not have to share any computed information—proprietary information that the financial institution infers about the customer based on its own computations, such as an internal credit risk score, even if it displays some of this information to its consumers. Similarly, financial institutions should not have to share any third-party data it has acquired about its customers, again, even if it displays this information to its customers. This way, all participants in the banking market will have the same opportunity to innovate with the same customer data, while ensuring organizations do not have to give up ownership of sensitive data or data they have added value to.

E. CONSUMER CONTROL AND PRIVACY

9. Should the Bureau propose to address any of the following, and if so, how and why: (i) Data users providing authorized data to entities other than in connection with the primary purpose or purposes for which the consumer authorized data access; or (ii) data users retaining consumer data other than in connection with the primary purpose or purposes for which the consumer authorized data access?

The Gramm–Leach–Bliley Act (GLBA) rightly does not require organizations to disclose how they will use data before they collect it, or require them to use it for a specified purpose only. Nor does it have a data retention requirement for financial records.[27] It is right not to do so to provide financial institutions with opportunities to innovate. The Bureau should not impose any additional purpose specification or data retention requirements to data holders, regardless of whether they are data users or authorized third parties.

Purpose specification limits organizations from reusing data for new purposes—and by definition, limits innovation.[28] It is often not possible to anticipate the insights analytics might reveal from a large data set, and applications of the data set may only become apparent over time. Third parties that collect and use financial data, such as Venmo, Plaid,

[27] Gramm-Leach-Bliley Act of 1999, S.900, 106th Cong. (1999).
[28] Alan McQuinn and Daniel Castro, "A Grand Bargain on Data Privacy Legislation for America", (Information Technology and Innovation Foundation, January 2019), https://itif.org/publications/2019/01/14/grand-bargain-data-privacy-legislation-america.

and Finicity, already have privacy policies that explain how they use data.[29] As long as their activities fall within the scope of their privacy policies, third parties should be able to reuse data, just as other data holders are allowed to.

Data retention limitations reduce the amount of usable data available to organizations. While one rationale for data retention limitations is that it limits the potential privacy risks for individuals because there is less data that can be misused or exposed in a data breach, these restrictions come at a steep price because they limit organizations from retaining historical data for new and interesting purposes that may ultimately benefits consumers. For example, to build better fraud detection tools, financial institutions need to have a wealth of historical transaction data to analyze. Data retention limitations will not only inhibit these third parties from innovating, the asymmetry of these rules will have a negative impact on competition within the market.

10. How, if at all, should a Bureau rule implementing section 1033 seek to limit authorized access to the minimum amount of consumer data necessary to effect the purpose of authorizing access as reasonably understood by the authorizing consumer? What are the benefits and risks to consumers, to competition, and to innovation in consumer financial services of such steps? What are the benefits and risks to consumers, to competition, and to innovation if such steps are not taken?

The GLBA rightly does not impose data minimization requirements on financial institutions. The Bureau should avoid amending these rules to impose such requirements on data holders or authorized third parties.[30]

Data minimization limits organizations from collecting more data than they need for specific tasks (e.g., processing a payment). Some critics favor data minimization because it fundamentally limits the amount of personal data organizations can collect and therefore reduces privacy risk.[31] Companies that do not have or use extensive data sources may support this provision, as it reduces the advantage competitors with more data have.

However, this restriction significantly limits companies from exploring new data sets that may lead to new or improved products and services. Data minimization negatively impacts

[29] "Privacy Policy," Venmo, https://venmo.com/legal/us-privacy-policy/;"Privacy," Plaid, https://plaid.com/overview-privacy/; "Privacy Policy," Finicity, https://www.finicity.com/privacy/.
[30] Gramm-Leach-Bliley Act of 1999, S.900, 106th Cong. (1999).
[31] Alan McQuinn and Daniel Castro, "A Grand Bargain on Data Privacy Legislation for America", (Information Technology and Innovation Foundation, January 2019), https://itif.org/publications/2019/01/14/grand-bargain-data-privacy-legislation-america.

start-ups that, at the outset, do not know what data will be most valuable for their business model or yield the best predictive insights. Data minimization can also hurt existing businesses by limiting their ability to conduct post hoc analyses to develop new types of products and services based on what they learn from the data—even if these organizations use this data in a way that protects individual privacy. And it impacts businesses' future flexibility by limiting those that want to pivot to different business models based on data.

The Bureau should not require data minimization as a benchmark for privacy because it overlooks the potential overall impact on consumer welfare. Instead, the Bureau should look at risk-mitigating strategies for protecting personal privacy, such as through the GLBA's security requirements.