Symposium on Consumer Access to Financial Records
February 26, 2020

Written Statement of Natalie R. Williams
Managing Director & Associate General Counsel, Responsible Banking, Data & Privacy
JPMorgan Chase & Co.

Submitted to the Consumer Financial Protection Bureau

Thank you for the opportunity to serve as a panelist at the Consumer Financial Protection Bureau's (CFPB) Data Aggregation Symposium.

I. Data Aggregation Presents Both Benefits and Risks

Financial data aggregation has grown dramatically in recent years and has yielded consumer benefits. Among other things, it has facilitated the creation of an array of innovative products and services that can help consumers better understand and manage their financial lives.

However, data aggregation should be undertaken in the best interest of consumers. It therefore must be executed with appropriate measures to ensure data safety and security and informed consumer consent. Most aggregators require consumers to provide financial account login credentials so that they can "screen scrape" the consumer's financial information. Through this practice of "screen scraping," aggregators have the ability to collect all of the consumer's financial information, even if the financial application the customer desires to use doesn't need it. That information can include account numbers, payees, and contact information as well as details on mortgage, investment and credit card accounts, joint accounts, and children's accounts. Aggregators also generally store account login credentials and scraped customer data, creating highly attractive targets for hackers and malicious insiders. Moreover, current data aggregation practices often are insufficiently transparent regarding the use and sharing of consumer financial data. This, in turn, limits the control that consumers have over their own financial information, placing data privacy and data security at risk.

Under these circumstances, banks face heightened risk given: (1) the potential for incidents involving data aggregators where consumer financial information is compromised, facilitating fraud, identity theft, and other negative consequences; and (2) the fact that consumers likely will

turn to their banks to make them whole in the case of any unauthorized transactions. In "screen scraping" scenarios, some banks may not even be able to determine whether a data aggregator breach has affected its customer base because they may not be able to distinguish between the customer and the data aggregator or determine which types of data a given aggregator has collected.

II. Chase's Data Aggregation Approach Balances These Benefits and Risks

Because of these risks, we have developed a data aggregation approach based on application programming interfaces (APIs) that leverages tokens (OAuth) rather than customer credentials; this approach provides a more secure method for data aggregation than screen scraping. In 2017, we entered into a groundbreaking data access agreement with Intuit. Since then, we have entered into a number of bilateral agreements that together comprise over 95 percent of the aggregator traffic coming through Chase. Our agreements follow three core principles: (1) safe and secure access to customer data through APIs; (2) customer transparency and control around what data is being accessed and downstream use of customer data by those receiving it; and (3) aggregator responsibility for risks they introduce.

We also want to make sure our customers understand what data they are sharing and who they are sharing it with. Recognizing that it's very easy for consumers to click "I agree" to terms they have not read or understood, we created the AccountSafe portal on our chase.com website. AccountSafe provides customers with an easy way to see the financial applications that are accessing their accounts through our secure API, the specific accounts being accessed, the specific account information being accessed, and the last time it was accessed. It also enables customers to turn off account access for particular applications or entirely – affording them both control and the information required to exercise it.

III. The CFPB Principles Have Sparked Collaborative Market-Driven Innovations in the Data Aggregation Ecosystem

Our approach aligns with the CFPB's 2017 Data Access Principles (the "CFPB Principles"). After issuing a Request for Information on consumer data access and examining the burgeoning, fast-changing market and the consumer protection issues it created, the CFPB declined to pursue prescriptive rulemaking in this space. Instead, the CFPB provided market participants with flexible yet clear and comprehensive principles in 2017 that "reflected the agency's vision for realizing an innovative market that gives consumers protection and value." The CFPB Principles address the key rights, challenges, and risks in this market: they cover data access, data scope and usability, control of the data and informed consent, payment authorization, data security, transparency on data access, data accuracy, accountability for access and use, and disputes and resolution for unauthorized access.

The CFPB Principles have provided market participants with the necessary flexibility to create technologies, tools and other measures to provide consumers with safe, robust data access and greater control over their data and how it is being used. With those principles as a guide, Chase and other banks, aggregators, and fintech companies have made substantial progress in improving and strengthening the data aggregation ecosystem. This progress is reflected in a number of positive developments:

- *Increase in Bilateral Data Access Agreements.* Following the release of the CFPB Principles, financial institutions, aggregators, and fintech companies have negotiated several bilateral data access agreements that reflect the agency's principles. These principles have accelerated efforts by market participants to contractually resolve consumer data access issues in ways that work for consumers and other key stakeholders.

- *Financial Data Exchange (FDX).* As a cross-industry group of leading aggregators, financial institutions, fintech companies, trade groups, and consumer advocates, FDX is dedicated to unifying the financial industry around a common, interoperable standard to facilitate secure access to consumer financial data and accelerate innovation while giving consumers greater control over their data and better awareness of how it is being used. FDX is creating an industry standard API (FDX API), a framework for security and certification, and user experience guidelines. FDX's membership has grown considerably since its launch and now includes 82 organizations. FDX committees and working groups meet regularly to advance the following objectives: (1) define use case profiles, (2) adopt and improve data-sharing standards, (3) adopt and improve secure authentication standards, (4) develop a certification program, (5) develop user experience and consent guidelines best practices, and (6) seek broad adoption of the FDX API standard.

- *Model Data Access Agreement.* With extensive input from member banks, non-bank financial institutions, and aggregators, the Clearing House developed a template data access agreement that is consistent with the CFPB Principles. Banks, data aggregators, and fintech companies can use the Model Agreement as a reference to facilitate the development of API-related data sharing agreements. The Model Agreement, which is voluntary, provides a foundation of common, generally-accepted terms that parties can reference to accelerate the process of reaching agreements.

- *Due Diligence Assessment Utility.* The Clearing House, member banks, and a leading aggregator have partnered to pilot a common process to evaluate the safety and security of third party apps, which will help ensure banks and their customers can trust the apps that have access to the customer's data. The intent is to help streamline and expedite the required compliance process by alleviating duplicative efforts by each financial

institution to assess the security and controls practices of each third party fintech company individually.

These efforts, in which we have been actively engaged, illustrate that the CFPB's principles-based approach has yielded significant benefits and is facilitating the continuing improvement and maturation of the data aggregation ecosystem. The CFPB's approach is working well and should continue, particularly given the pace of technological innovation and business model evolution likely to emerge in this space. Extensive, prescriptive rules, such as Europe's Payment Services Directive 2, are unnecessary given the substantial progress being made and ill-advised since any such potential rulemaking would likely chill and potentially freeze innovation and market-driven solutions to the detriment of consumers and the ecosystem more generally.

IV. The CFPB Should Consider Clarifying Guidance and Regulatory Action in Two Targeted Areas

There are, however, two targeted areas where clarifying guidance and regulatory action would facilitate the continuing improvement and development of the data aggregation ecosystem.

First, the CFPB should affirm that GLBA's privacy and safeguard provisions apply to data aggregators and subject leading data aggregators to supervision and regular examination given the consumer protection risks their activities create

Traditionally, only regulated financial institutions and their contractual vendors, both of which are subject to GLBA and are either directly or indirectly supervised by regulators, had access to consumer financial data. Congress recognized, when enacting the Safeguards provisions of GLBA, that "each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."[1] In turn, GLBA also imposed stringent third-party risk management requirements on financial institutions to help ensure that each contractual vendor was meeting the data security requirements imposed by GLBA, creating a secure financial system.

Banks also are subject to rigorous examination on nearly all aspects of their information security practices, which are informed by extensive information security guidelines for financial institutions published by the Federal Financial Institutions Examining Council. These include guidelines regarding secure software development, third-party oversight, technology vendor management, business continuity planning, and cybersecurity threat awareness. Rigorous supervision requires not only adherence to the data protection principles outlined in GLBA, but also to specific information security standards, such as multifactor authentication and encryption,

[1] 15 U.S.C. § 6801(a).

which are reasonably contemplated in anticipation of the cybersecurity threats posed to both consumers and financial institutions today.

Data aggregators, who often collect and store more of any particular consumer's financial data than a single financial institution, present challenges to the existing regulatory model. Data aggregators that use screen-scraping, the least secure but often the most convenient method of data access, require consumers to provide (and may need to store) login credentials for routine access to the consumer's financial information. The same, identical set of login credentials would then be used by both the consumer and the aggregator to access the consumer's financial accounts, thereby increasing the risk of unauthorized transactions. Screen scraping threatens the careful balance that the CFPB Principles have struck between facilitating convenient customer-permissioned access and the need to protect consumers from fraud and identity theft because baseline security controls are not necessarily in place. The current bilateral agreement approach better accommodates both needs by providing access through secure APIs and contractually requiring aggregators to meet certain minimum information security requirements and to exercise oversight over their clients. That said, contractual oversight is not a perfect mechanism for ensuring consistent, robust practices regarding information security and privacy. Supervision by a federal regulator such as the CFPB would help enhance the ecosystem's overall safety.

Many consumers do not appreciate that different regulatory frameworks could potentially apply to banks and non-bank entities, and that there could be more risk when they share personal financial data and account credentials with an aggregator. Recent cybersecurity events with wide-ranging consumer impacts (like the Equifax breach) demonstrate that large data aggregators could be attractive targets for cyberattacks for both state and non-state actors due to the wealth of consumer information they possess. For consumers who use multiple financial institutions, a compromise of a data aggregator's system could provide a hacker with a comprehensive picture of the consumer's financial profile, not to mention multiple login credentials. This provides an avenue for myriad unauthorized transactions, fraud, identity theft, and other potential consumer harm that may be difficult, if not impossible, for any particular financial institution to mitigate.

Any compromise of an aggregator's data systems, or any transactional fraud, error, or abuse on the part of the aggregator, also creates challenges for financial institutions in the form of unauthorized transactions under Regulations E and Z. Although the extent of an institution's liability for unauthorized transactions under Regulations E and Z will turn on the facts and circumstances of the particular situation, the reality is that bank customers will look to banks to make them whole if they experience losses or otherwise suffer harm. Additionally, financial institutions may have to incur costs for breach notifications, credit monitoring services, and issuance of replacement accounts. The increasing growth of aggregator activity magnifies the potential exposure for financial institutions in this space.

In order to address the challenges to consumer financial privacy and data security presented by the activities of data aggregators, the CFPB should make clear GLBA's applicability to data aggregators and strongly consider exercising its larger participant rulemaking authority to assert supervisory jurisdiction over larger participants in the aggregation market.

First, consistent with the FTC's position, it should reinforce the applicability of GLBA's privacy and safeguard provisions to data aggregators because: (1) aggregators fall within the expansive definition of "financial institution" under the statute; (2) they maintain as much, if not more, financial data as compared to financial institutions regulated under GLBA; (3) they are in the best position to control and manage information security risks relating to the information in their possession; and (4) they have a legal and ethical obligation to protect consumer privacy and safeguard consumer information. The CFPB should reinforce GLBA applicability by issuing guidance on this matter.

In addition, at present, there is a lack of holistic, regulatory supervision over data aggregators, leaving a critical gap in consumer protection. Specifically, while federal regulators have enforcement jurisdiction, they generally lack the supervisory jurisdiction that would allow for examinations and other ongoing oversight. Moreover, any supervision that might occur at the state level would not necessarily be uniform or comprehensive. Without ongoing federal supervision, there will be circumstances where it may be impossible to detect or correct deficiencies in privacy and data security protocols until there has been an incident in which consumer data has been compromised. Moreover, given consumer expectations and regulatory uncertainty regarding the application of Regulation E and Z in the data aggregation context, even if an aggregator experiences a data breach, it is likely that the bank, as the data owner, will suffer significant financial consequences due to the lax security practices of the data aggregator. As a result, data aggregators may have little incentive to adhere to strong information security and privacy practices or employ robust data minimization and data retention practices until a data breach or a cybersecurity event occurs – which poses a serious risk to consumers and the market generally.

In order to address this risk, the CFPB should consider utilizing its larger participant rulemaking authority to bring data aggregators within the ambit of the agency's supervisory jurisdiction. Such authority has been used in the past in order to enable CFPB to supervise activities that pose heightened risk relating to consumer financial services.

Although the CFPB would not be able to directly enforce or examine GLBA-required security standards, it could evaluate data aggregators' compliance with UDAAP, focusing in particular on information security issues, and with Regulation P. The CFPB's focus might include determining whether aggregators' security practices are consistent with their representations and

assurances. The CFPB could also coordinate with the FTC to ensure that data aggregators are subject to the FTC Safeguards Rule.

Fulsome regulatory supervision will better ensure that data aggregators are vigilant in developing and maintaining risk-based information security programs and that these programs are consistently updated based on emerging cybersecurity threats, as they often represent to consumers. For example, if a data aggregator represents to consumers that it utilizes "bank-grade security," then it should have in place the basic elements critical to that level of security, such as strong encryption for consumer information, robust incident response plans (including communications to customers and financial institutions) and purge requirements should a consumer cease using an underlying application. Supervision can go a long way in this regard, ensuring that a data aggregator's representations regarding privacy and data security practices are consistent with what the consumer actually gets on a consistent basis.

Second, the CFPB should provide guidance on obtaining informed and effective consent from consumers on uses of data unrelated to the products and services they have requested from fintech applications

The CFPB Principles state that "authorized terms of access, storage, use, and disposal [should be] fully and effectively disclosed to the consumer, understood by the consumer, not overly broad, and consistent with the consumer's reasonable expectations in light of the product(s) or service(s) selected by the consumer." Consistent with the Principles, market participants agree that consumer data should be accessed and used only as consented to by the customer. The challenge, however, is ensuring that such consent is both informed and effective.

In our experience, aggregators have faced challenges trying to establish consistent consent frameworks with their fintech application customers given the diversity of their client base in terms of size, maturity, and other factors. They often feel compelled to revert to the lowest common denominator in terms of consent, even if this does not provide consumers with informed and effective consent. Further, broad consents are generally the rule, not the exception. Only rarely are downstream data uses restricted to activities that are "consistent with the consumer's reasonable expectations" or designed to provide a benefit to the consumer. Additionally, we have observed that aggregators on behalf of their clients may continue to screen scrape a customer's data long after a customer has stopped using the applicable fintech applications. This continued access is very likely not well understood by customers so there is an opportunity for more effective consent through better disclosure of access and purge practices.

Establishing robust and consistent consent frameworks would provide significant consumer benefits, enabling informed consent and protecting consumer privacy. The bilateral arrangements between aggregators and financial institutions are not effective vehicles for achieving this

consistency, particularly when the parties often obtaining consent are the aggregators' fintech customers. As such, it would be extremely useful for the CFPB to develop model forms and provide more specific guidance on what informed and effective consent looks like in this context, including guidance on prominence and placement of different elements of the consent in the customer experience/journey.