Kabbage

February 21, 2017

Via electronic submission to: FederalRegisterComments@cfpb.gov

Monica Jackson
Office of the Executive Secretary
Consumer Financial Protection Bureau
1700 G Street NW
Washington, DC 20552

Re: Request for Information Regarding Consumer Access to Financial Records, CFPB–2016–0048

Dear Ms. Jackson:

Kabbage, Inc. ("Kabbage") welcomes the opportunity to comment on the Consumer Financial Protection Bureau's ("CFPB") request for information regarding consumer access to financial records ("RFI"). The RFI is a well-timed and important engagement with the financial services industry given the ongoing convergence of technologies that promote financial innovation and consumer access to information with legal and compliance frameworks that serve to protect consumer information. Kabbage appreciates the CFPB's efforts to rationalize these two important interests and in so doing to advance two CFPB objectives established by Congress in the Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank Act") -- providing consumers timely and understandable information to make financial decisions and facilitating access and innovation in markets for consumer financial products.[1]

We believe that access to customer information is the lifeblood of financial innovation and a necessary precursor for fair, transparent, and competitive markets for financial services. Kabbage strongly supports the core principles of customer empowerment and choice, both of which start with access to information. This decade has seen remarkable growth in the availability of accessible, real-time customer financial data and substantial technological advances used to aggregate such data. The convergence of these factors has allowed financial technology "FinTech" companies to produce a more holistic understanding of a customer and to analyze such data in order to identify trends and pattern resulting in significant benefits to consumers and small businesses. Kabbage has leveraged advanced machine learning technologies to analyze real-time information regarding small business loan applicants from verified third-party data sources, including transaction information from an applicant's bank account and other financial accounts, revenue and expense information from the applicant's accounting system, credit bureau information, payment processing information, shipping records from the applicant's inventory systems, along with numerous other data points. This analysis has produced

[1] *See* Dodd-Frank Act, § 1021.

Kabbage.com
855-278-7084 | info@kabbage.com | 730 Peachtree St., Suite 1100, Atlanta, GA 30308

unique insights that otherwise would be unavailable and that, when coupled with quick, automated, online underwriting, deliver an unparalleled user experience for small businesses. Kabbage's use of real-time data has also expanded access to credit for small businesses, enabling such businesses to focus on growth, hiring, and new opportunities.

Naturally, a customer's financial information is confidential, and numerous laws and regulations impose compliance requirements on those entities that collect, store, and transmit such information. However, compliance requirements do not, as some would suggest, preclude companies from making information available to customers in a safe and secure manner. Customers have an absolute right to their account information, to use it for the purposes they see fit, and to provide it to the third parties they trust. To conclude that customer information should not be freely transferable by the customer because of compliance requirements is to place the institution's interests above the customer's interests.

Kabbage's success in offering access to quality small business in a safe and secure manner and in compliance with laws and regulations demonstrates that innovation and customer access to information are fully consistent and indeed complementary of compliance requirements. Moreover, Congress recognized that customer access to information was sufficiently important – and fully reconcilable with these types of compliance requirements – when it included Section 1033 in the Dodd-Frank Act and vested rulemaking responsibility for the Section in the CFPB, which is in a position to harmonize customer data access and compliance requirements to the extent a conflict arises.

In furtherance of its mandate under Section 1033, Kabbage recommends that the CFPB (1) facilitate the creation and circulation of open banking application programming interfaces ("APIs") that enable third-party access to information and (2) develop principles-based standards for customer data access that foster innovation through the financial services ecosystem.

The CFPB should take action to facilitate the creation and circulation of open banking APIs that permit authorized third parties to access reliable information in a safe and secure manner that is tailored to a customer's needs. Open banking enables a customer to more easily make informed and reliable product comparisons, exercise mobility in moving from one financial services provider to another, and access custom financial products and services.[2] Open banking APIs in the context of small business credit reduce information barriers that exist between lenders and borrowers. Borrowers gain access to enhanced market information, thereby forcing lenders to compete on price, service, and availability, and lenders are better able to deliver products and services tailored to borrowers' needs. The reduction in information barriers also eases the path for new market entrants that seek to provide credit and financial services in innovative ways to borrowers and create jobs and opportunities in their local communities. APIs also have the capability to effectively deploy regulatory technologies ("RegTech") that connect government agency data systems with financial institution systems and

[2] In 2016, the United Kingdom's Competition & Markets Authority ("CMA") issued a policy guide favoring open banking and the adoption of API standards. *See* Competition & Markets Authority, Making banks work harder for you (Aug. 9, 2016), *available at* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/544942/overview-of-the-banking-retail-market.pdf. The guide identifies a number of deficiencies in the markets for consumer and small business financial services and calls for specific reforms such as the development and adoption of open banking APIs for the UK's largest banks, uniform service quality reporting for all banks, and APIs for switching retail bank account providers.

therefore streamline the reporting of financial and compliance information required under law and regulation. For these reasons, APIs stand to benefit all stakeholders in the FinTech industry, including financial account providers, permissioned parties, account aggregators, customers, and regulators.

Moreover, the CFPB should develop principles-based standards for customer data access, including open banking APIs, and not seek to promulgate rules that prescribe detailed requirements and limitations on such access. Principles-based standards for customer data access could include, for example, ensuring customers have access to all of their account data in a usable electronic form at no cost and encouraging the development of open banking APIs that use standardized data formats. These types of standards keep pace with the rapid evolution of technology in the FinTech industry and give the industry needed flexibility to satisfy market demands while remaining compliant with applicable laws and regulations.

In addition, principles-based standards are particularly appropriate for FinTech industry market participants, such as account aggregators, permissioned parties, and third-party platforms, that are rapidly innovating products and services, the benefits of which have yet to be fully realized in many cases. Technologies such as automated or insightful personal financial management, online lending and savings, investment automation, cash flow and budgeting analysis, alternative credit decisioning, and account security, fraud, and identity verification are poised to provide consumers and small businesses tremendous financial decision-making power and independence in the future but will be unduly stifled at their current stage of development if the CFPB promulgates overly-prescriptive rules on customer data access.

Principles-based standards are especially appropriate for account aggregators, which have the ability to connect the many diverse market participants in the FinTech industry, accelerate innovation among such participants, and channel the benefits of such innovation – including increased speed and depth of analysis of customer information and enhanced user experience – to consumers and small businesses. Account aggregators bring together online banking and financial service platforms, large and small financial institutions, and service providers, each with their own unique information technology systems. Principles-based standards are critical to preserving the flexibility that aggregators require to successfully navigate and integrate these systems.

Together, open banking APIs and principles-based standards for customer data access give customers greater control over the collection, use and sharing of their data – including with downstream parties. These standards are precisely what Congress had in mind when it enacted Section 1033 of the Dodd-Frank Act in order to require covered persons to make available information in a usable electronic form.[3]

Section I of this letter contains background information regarding Kabbage, and Section II contains responses to selected questions in the RFI.

[3] 12 U.S.C. § 5533(a). Section 1033 also requires the CFPB to promulgate standards applicable to covered persons to promote the development and use of standardized formats for information to be provided to consumers, and open banking APIs are best suited to the development of such standardized formats.

I. Background Information

Kabbage was formed to achieve a simple premise: leverage the power of real-time, persistently connected data to streamline the lending process for small businesses. This commitment to small businesses and enriching the lives of their owners, employees, and customers has fueled the company's rapid growth and many technological innovations.

Kabbage launched publicly in 2011 after spending several years developing the technology necessary to support an automated loan application, underwriting and servicing platform ("Platform") that could be used by small businesses to complete an application entirely online, generally receive a credit decision in less than ten minutes and, if approved, quickly access funds. Leveraging this Platform, in 2014, Kabbage partnered with Celtic Bank, a Federal Deposit Insurance Corporation ("FDIC")-insured, Utah-chartered industrial bank, to launch the Kabbage® Small Business Loan Program ("Program"), which provides access to lines of credit issued by Celtic Bank that currently range from $2,000 to $100,000. Since inception, the Program has spurred important industry innovations for small business credit access, such as point-of-sale access to funds, a clear and conspicuous mobile environment for credit, and fast debit network funds disbursement.

As a service provider to Celtic Bank, Kabbage is subject to a host of regulatory requirements by virtue of the Bank Service Company Act.[4] These requirements include, among many others, customer identification, anti-money laundering, fair lending, customer disclosures, information security, data protection, and privacy. Developing a compliance program for all of these requirements involves substantial resources, including a commitment to compliance from the company's board of directors, executive officers, and employees. The Program's compliance with these requirements is examined annually by the FDIC and Utah Department of Financial Institutions ("DFI").

Kabbage is a thought leader in the industry and has consistently advocated for transparency in small business lending. In October 2016, Kabbage unveiled the "Straightforward Metrics Around Rate and Total cost Box," or "SMART Box" disclosure in partnership with other industry lenders through the Innovative Lending Platform Association ("ILPA"). The primary goal in developing the disclosure was to increase transparency in the small business lending industry and empower small businesses to easily determine the cost of credit. The SMART Box was informed by an in-depth analysis of the small business marketplace including small business survey data and recent findings from an Electronic Transactions Association study,[5] which underscore small businesses' preferences and priorities with regard to pricing disclosures. The SMART Box disclosure provides transparency in fees and rate structure and enables a small business borrower to compare credit products offered by different lenders. The SMART Box is currently provided on the first page of the loan agreement for all Kabbage-branded Program products.

Recognizing the broader capabilities of the Platform, in 2015, Kabbage began licensing the Platform through a software as a service ("SaaS") model to financial institutions around the world interested in extending small business credit in order to deepen relationships with existing customers and to extend the reach of their services. Kabbage has successfully launched strategic partnerships with

[4] 12 U.S.C. § 1867(c).

[5] *See* Electronic Transactions Association, New ETA Survey Finds Online Lending an Important Tool for Small Business Owners (Apr. 13, 2016), *available at* http://www.electran.org/publication/transactiontrends/new-eta-survey-finds-online-lending-an-important-tool-for-small-business-owners/.

a number of the top 50 leading global financial institutions,[6] including ING Bank N.V. ("ING"), The Bank of Nova Scotia ("Scotiabank"), and Banco Santander ("Santander"). The Platform is fully customizable and can be adapted to fit each financial institution's underwriting criteria, credit risk appetite, loan terms, and data systems. Licensing the Platform under a SaaS model to global financial institutions gives Kabbage the opportunity to make available its proprietary data collection and analysis technologies on a scaled basis to customers around the world. Working with global institutions such as ING, Scotiabank, and Santander has required Kabbage to develop sophisticated Platform controls for data security, risk management, and compliance that satisfy the legal regimes in each of the countries where the institutions do business, and these controls in turn have enhanced the Program and benefitted small businesses in the United States. Kabbage's dual role as both a service provider for Celtic Bank and a SaaS provider of an online lending platform gives the company a unique vantage point with respect to the access and use of customer financial information.[7]

The Platform relies upon automated data access and secure open APIs to collect and aggregate data specific to loan applicants from a variety of verified third-party sources. Small business customers provide their permission for the Platform to retrieve this information. The data is securely stored and analyzed on an ongoing basis by the Platform's proprietary algorithms and machine learning technologies, including Artificial Intelligence ("AI")-driven solutions that are subject to continuous testing and phased implementation to ensure reliability. The analysis produces actionable credit information for either Celtic Bank or financial institutions that have licensed the Platform through the SaaS model. Access to robust and reliable small business customer information is paramount to the Platform. Without this access, the comprehensiveness and speed of the Platform's analyses may be inhibited, potentially reducing the many benefits the Platform currently, or could in the future, offer to small businesses.

II. Responses to Specific RFI Questions

Question 1 – What types of products and services are currently made available to consumers that rely, at least in part, on consumer-permissioned electronic access to consumer financial account data? What benefits do consumers realize as a result? This question covers the use of such data to deliver products or services or to assess eligibility for a given product or service.

Kabbage does not offer consumer financial products or services that rely in any way on consumer-permissioned electronic access to consumer financial account data.[8] Loans funded by Celtic Bank through the Program are for small businesses' commercial purposes only, and the agreement that borrowers enter into in connection with these loans appropriately limits use of the loan proceeds to commercial purposes.

---

[6] Ranked by asset size.

[7] The Program that Kabbage offers with Celtic Bank in the U.S. involves the extension of credit for commercial purposes and not for personal, family, or household purposes. Kabbage does not collect, maintain, or transmit information that would be considered information concerning a consumer financial product or service. Accordingly, Kabbage is not a "covered person" for purposes of Section 1002(6) of the Dodd-Frank Act, 12 U.S.C. § 5481(6), and would not be (1) required under Section 1033 of the Dodd-Frank Act to make available account or transaction information to its customers or (2) subject to any rules promulgated by the CFPB thereunder. Kabbage is commenting on the RFI in its capacity as a provider of a platform for small business credit that has experience with permissioned access to financial data.

[8] *See supra* n. 2.

In this small business credit context, the Platform uses APIs to facilitate the collection of a variety of data from small business loan applicants. After obtaining the small business's permission, the Platform collects real-time financial and non-financial information about the applicant, including, as applicable, information from its bank accounts, e-commerce platforms, accounting programs, shipping platforms, payment processors, and online review sites, among other data sources.

After completing the necessary compliance checks, Kabbage aggregates all of this data on the Platform, builds a proprietary representation of the small business's financial statements, conducts a detailed cash flow analysis, identifies fraud and identity verification risks, and performs a credit risk analysis of the small business based on the 5 C's of credit: character, capacity, capital, collateral, and conditions. Permissioned access to account information enables the Platform to examine traditional underwriting information with substantially mitigated risk of an accounting error, and the Platform's direct connections with the customers' data sources allow for confirmation of data against complementary, substitutional or combined sources of data. These data access points and controls create a highly reliable and multi-faceted underwriting environment that produces useful information about customers. For example, the analysis of bank account, accounting, and payment information offers a triangulated view of cash flows that is much more accurate than a traditional cash flow analysis.

The collection and analysis of this information provides direct benefits to small businesses. Principally, with robust and varied data, the Platform is able to create a deeper analysis of a customer's creditworthiness, establish loan terms and conditions better tailored to the customer, and provide insights into the customer not available from traditional underwriting processes. This, in turn, results in the extension of credit to markets and borrowers that may not historically have had access to credit. The availability of this data also contributes to enhanced identity verification and fraud monitoring controls with respect to the Platform because much of the data is verified by a third party that has an independent relationship with the customer and its own data security and integrity controls.

The Platform also contributes to a seamless and convenient user experience. It benefits customers by giving them the freedom to apply for credit at any time and from any location using a mobile phone, tablet, or computer. The owner of the small business is not required to take time out of his or her day to, for example, gather receipts, prepare documentation, or visit a loan officer. Furthermore, without human interactions that involve potential judgment and discretion in underwriting and pricing, such as a loan applicant's interactions with a loan officer, there is far less opportunity for discrimination on constitutionally-protected grounds.

Question 2 – How many consumers are using or seeking to use such products or services? What demographic or other aggregate information is available about these consumers?

Kabbage has extended credit to over 100,000 small and medium-size business customers since launch of the Program. Kabbage's Platform is used by a number of global financial institutions, including Scotiabank, ING, and Santander. These institutions have used the Platform to serve approximately 750,000 small business customers, and the potential exists to expand use of the Platform to serve over 20 million small business customers in the jurisdictions in which the institutions currently do business.

Question 3 – To provide or assess eligibility for these products and services, what kinds of consumer financial account data are being accessed, by what means, under what terms, and how often? How long is accessed data stored by permissioned parties or account aggregators?

Kabbage obtains access to the financial information described in greater detail above on a real-time basis through APIs. This information includes, but is not limited to, credit bureau information, identity information, sales channel information, accounting information, bank account information, and payment processor information.

The collection, use, and transmission of this information is governed by the privacy notices of the various entities involved, including as applicable Kabbage, the account aggregators, financial account providers, and global financial institutions.

Question 6 – In what ways, if any, do consumer products and services that rely, at least in part, on consumer-permissioned electronic access to consumer financial account data differ according to whether the offering company provides or does not provide transaction accounts to consumers? Do any such differences impact consumers? If so, how?

Financial institutions that hold transaction accounts for customers, such as banks and credit unions, have advantages over financial services providers that do not and need to rely on other institutions for account information. An account-holding institution may control access to the customer data it maintains and use this access to provide reliable, real-time information to its customers. On the other hand, these institutions may restrict third-party access to the data or compromise third-party data feeds and thereby disadvantage financial services providers that require access to the data to provide products or services. Subjecting the availability of their services to the whim of the account-holding institution can create major hurdles for financial service providers in not only providing their services but also in innovating with respect to such services.

Periodic and unpredictable interruptions or obstacles to data access are problematic for customers that rely on FinTech applications for personal financial management. Customers may attempt to spend money they do not have or make financial choices based on outdated or incomplete information. If an account-holding institution adopts terms of service that prohibit a customer from sharing its online credentials, a customer may refrain from using FinTech solutions that rely on account aggregation services and forego the unique benefits these solutions offer.

Question 8 – What incentives or disincentives exist for consumer financial account providers to facilitate or discourage consumer-permissioned access to the account data that they hold by permissioned parties or account aggregators? In what ways do consumer financial account providers directly or indirectly facilitate or restrict consumer-permissioned access to account data? What are the associated impacts to consumers and other market participants?

Financial account providers may be concerned that permissioned access to their customers' account data may somehow create enhanced cybersecurity risk or injure their competitive position and decide to restrict access to account data, with the unfortunate effect of preventing permissioned parties from offering their services to such customers. For parties that satisfy unmet demands for financial services, such as access to competitively priced small business credit,[9] access restrictions may affect entire markets for financial services.

[9] For example, as described in the Department of the Treasury's recent whitepaper on marketplace lending, according to a survey of small business credit published by the Federal Reserve Banks of Atlanta, Boston, Cleveland, New York, Philadelphia, Richmond and St. Louis in 2015, only half of small business loan applicants received the full amount of financing they requested. The Federal Reserve Bank of Atlanta, Boston, Cleveland,

A provider's decision to curtail access disregards a customer's right to his or her own account data and ignores the many benefits that such access produces for the customer as well as the provider. For example, if Kabbage cannot obtain permissioned access to certain financial data, the small business borrower may be forced to manually provide additional documentation verifying its identity or substantiating its financial resources. The borrower may not obtain credit or may obtain credit on less favorable terms (e.g., lower line amount or greater fees) than would otherwise be available. Real-time access to this information benefits customers by enabling Kabbage to adjust line amounts and fees based on the business's performance.

Facilitating customer-permissioned access may also be beneficial to the provider itself because it integrates the provider's data in other applications used by the customer, and many customers view this portability and ease of integration as important prerequisites for their financial products and services. If the provider refuses to grant access, the customer may seek an alternative provider. In addition, rather than straining the customer's relationship with the provider, integration of the provider's data in other customer applications serves to highlight the importance of the provider's data to the application (i.e., the application cannot provide its benefits without provider data) and its contribution in giving customers a holistic view of their financial profile.

Question 9 – What impediments, obstacles or risks do consumer financial account providers currently face in providing data to or allowing access to data by permissioned parties or account aggregators? Describe specific operational costs, risks, and actual or potential losses, and identify their specific causes.

As noted above, consumer financial account providers may perceive a number of risks in providing data access to permissioned parties or account aggregators, although these risks can be mitigated through due diligence, contractual protections, and other controls. Regulatory protections also exist for consumer financial products and services. For example, consumer financial account providers are required under the Gramm-Leach-Bliley Act ("GLBA") to comply with restrictions on the disclosure of customers' nonpublic personal information to nonaffiliated third parties. The provider must sort through whether disclosure of consumer information is consistent with GLBA and the privacy representations made to consumers.

Question 10 – What impediments, obstacles or risks do permissioned parties or account aggregators currently face in obtaining such data? Describe specific operational costs, risks, and actual or potential losses, and identify their specific causes.

As described above, financial account providers may restrict permissioned parties' and account aggregators' access to account data based on cybersecurity or competitiveness grounds. When permissioned parties and account aggregators lose access to account data, there may be interruptions or inaccuracies in the services they provide to customers, and customers – who directed the institution to grant such access to the party or aggregator in the first place – may be harmed or disadvantaged. Thus, access restrictions by financial account providers frustrate innovation and customers' use of their chosen financial products.

New York, Philadelphia, Richmond and St. Louis, *Small Business Credit Survey 2015* (Mar. 2016), *available at* https://www.newyorkfed.org/smallbusiness/joint-small-business-credit-survey-2014.html. Small businesses with less than $100,000 in annual revenue and start-ups with fewer than two years of operations had the most difficult time securing credit, with 63 percent and 58 percent, respectively, reporting a financing deficiency. *See id*.

In addition, the allocation of liability among various participants in a lending platform such as the Platform – including the customers, financial account providers, account aggregators, financial institutions licensing the Platform, and others – is based solely on heavily negotiated bilateral agreements. The negotiation process is time-intensive because multiple agreements must be negotiated instead of a single omnibus agreement. Each party is subject to differing risks and legal requirements, and each party is not in contractual privity with the other parties, causing friction as certain parties may be forced into conflicting positions that require them to absorb another party's liability.

Permissioned parties and account aggregators also may encounter difficulties in obtaining data via screen scraping. The legal and regulatory posture of screen scraping is evolving, and in the absence of guidance from the CFPB or another regulator, a financial account provider may block access to customer data based on the belief that screen scraping is impermissible. Screen scraping as a technique for collecting permissioned data is more crude than the use of APIs and tends to generate data that is less reliable and robust than the data transmitted through APIs. However, small businesses that have bank accounts with community banks that do not have the resources to invest in API development would miss out on the benefits of innovation without screen scraping. Screen scraping levels the playing field and gives underserved customers broader access to financial products and services.

Question 11 – What impediments, obstacles or risks do consumers currently face in obtaining—including permitting access to—such data?

As described above, customers may be subject to a number of impediments and obstacles to obtaining access to their data. For example, particular financial account providers may require customers to complete additional forms or give certifications in order to request their information. A customer may be forced to navigate cumbersome and confusing user interfaces that require the customer to specify the types of data for which it is requesting access and the format in which the data is being requested. Once requested, the data produced by the provider may not be in a standardized format that is usable by the customer, account aggregators, or permissioned parties and may not be a complete record of all data in the provider's possession.

Question 12 – What security and other risks do consumers incur if they permit access to their financial account data in order to obtain a particular product or service? What steps have consumer financial account providers, account aggregators, permissioned parties and other users of consumer-permissioned account data taken to mitigate such risks? What information do these parties communicate to consumers about associated risks?

The risks that customers face in permitting access to their financial account data are related to the risks faced by permissioned parties and providers. These risks include enhanced cybersecurity risk from granting access to account data to third parties, potential legal risk from bearing losses due to uncertainties in liability under the Electronic Fund Transfer Act for consumer accounts, and risk that a customer's privacy choices will not be honored or that its information will be shared in a manner inconsistent with law or representations made to the customer.[10]

[10] AI technologies may help mitigate the risk that a customer's privacy choices are not honored or that a customer's data is shared in a manner inconsistent with customer's preferences or representations made to the customer. For example, there are solutions in the market that compile the various privacy preferences of a customer over time, learn the scenarios in which the customer opts out or opts in, as appropriate, to certain

Financial account providers, account aggregators, and permissioned parties, including Kabbage, have implemented a number of controls to mitigate these risks. Financial account providers have developed robust third-party risk management programs in response to regulatory guidance from the federal banking agencies, and these programs require comprehensive due diligence and monitoring of third parties such as third-party platforms and account aggregators with whom the providers contract. Due to these programs and federal banking agency supervision under the Bank Service Company Act, many third-party platforms and account aggregators' effectiveness in mitigating the above risks is regularly evaluated, and if mitigation is deficient, the third-party platform or account aggregator may be subject to mandatory remedial efforts or enforcement actions. Separately, financial account providers, account aggregators, and permissioned parties may be subject to the Payment Card Industry Data Security Standard ("PCI-DSS") requirements in order to safeguard the sensitive payment card information they collect, store, and transmit.

Third-party platforms and permissioned parties also obtain customer consent before accessing any of the customer's data and provide detailed disclosures of the manner in which the data will be accessed, stored, and transmitted. These controls are designed to ensure the customer understands the various parties that will have access to its data and the parties' uses of such data.

Cybersecurity risk has been a focal point of the FinTech industry and consumer and commercial loan platforms. To mitigate this risk, third-party platforms and permissioned parties have explored use of tokenization to eliminate the need to store and transmit sensitive customer login credentials. Similarly, financial account providers and other parties have offered read-only access to customer data to mitigate cybersecurity risk.

Question 13 – In what ways, do account aggregators or permissioned parties use consumer-permissioned account data for purposes other than offering or facilitating the delivery of a specific product or service to the permissioning consumer? Do such companies continue to access or store data after the consumer ceases to use the product for which the permissioned data use was intended by the consumer? Do such companies share the data with other parties and, if so, under what terms and conditions? What are the associated impacts to consumers?

There is a broad range of practices among account aggregators and permissioned parties regarding uses of customer information for purposes other than providing the permissioned product or service. For example, account aggregators and permissioned parties may use aggregated or anonymized information (i.e., information that does not identify an individual customer) for risk management purposes, to enhance the customer experience, to improve their technologies, and to develop new offerings. Many companies are increasing their disclosure regarding uses of permissioned account data that do not relate to the permissioned product or service so that the customer is aware of all the ways the company will use and disclose the data.

In the context of consumer financial products and services, these practices are governed by the GLBA and other financial privacy statutes. If GLBA does not apply, the practices are generally bound by the

---

privacy practices such as data sharing, and ensure that these preferences are automatically communicated to providers of products and services.

representations made to customers in the privacy notice or similar terms and conditions of the permissioned party or account aggregator.[11]

Question 15 – To what extent are consumers able to control how data is used by permissioned parties or account aggregators that obtain that data via consumer-permissioned access? Are consumers able to control what data are accessed, how often they are accessed, for what purposes and for how long the data are used, and with which entities, if any, a permissioned party or account aggregator may share the data and on what terms and conditions? Are they able to request that permissioned parties, account aggregators, or other users delete such data? Is such data otherwise deleted and, if so, when and by what means? To what extent are consumers consenting to permissioned party and account aggregator practices with respect to access, use and sharing of consumer financial account data?

For a consumer financial product or service, data usage is subject to the re-use and re-disclosure restrictions in GLBA, which generally restrict a service provider to use and disclosure in furtherance of the service being provided.[12]

The most direct source of information explaining a permissioned party's or an account aggregator's use of customer data is its privacy notice, which typically is incorporated in the customer enrollment process and is consented to either explicitly or implicitly through the customer's use of the product or service. While privacy notices vary broadly, in general, the notice should explain the purposes for which the permissioned party or account aggregator obtains customer information, including purposes related to the underlying product or service (e.g., underwriting, servicing the customer's account) and unrelated to the product or service (e.g., internal analytics, marketing). The privacy notice also should describe the entities to whom the party or aggregator discloses customer information. The customer has control over the practices covered in the privacy notice insofar as it may decide not to use a product or service based on the entity's privacy practices or opt out of certain third-party sharing. Once the customer has consented to the privacy notice, the permissioned party or account aggregator may access the customer's data in any manner consistent with the notice.

As a practical matter, there also are features of data access that the customer may control that are outside the scope of the privacy notice. For example, a customer may be able to control which of its data is accessed by a permissioned party or account aggregator. However, the extent of this control may depend on the data source and whether the source is capable of segregating its data into discrete data points that the customer may select or de-select for access. Newer data sources such as social networking information tend to offer customers such granular control over their data but traditional data sources such as banks and credit bureaus do not and often provide all information about the customer in the system. In general, customers do not control going forward how often or for how long their data is accessed by a party or aggregator once permission is provided.

Permissioned parties and account aggregators generally will delete customer data upon request unless doing so would violate recordkeeping requirements under applicable laws and regulations or

[11] The representations made in these notices are enforceable against the party or aggregator. For example, the CFPB brought an enforcement action against Dwolla due to misrepresentations made to customers regarding the company's information security practices under the prohibition in the Dodd-Frank Act on unfair, deceptive, or abusive acts or practices. *See* 12 U.S.C. §5531(a); *see, e.g.*, *In the Matter of Dwolla, Inc.*, Administrative Proceeding File No. 2016-CFPB-0007 (Mar. 2, 2016).

[12] *See* 12 C.F.R. § 1016.11.

create contractual liability. The implementation period for deleting data and the manner in which it will be carried out depend on the party or aggregator.

Question 16 – Do consumer financial account providers vet account aggregators or permissioned parties before providing data to them? Do consumer financial account providers perform any ongoing vetting of account aggregators or permissioned parties? If so, for what purposes and using what procedures? What are the associated impacts to consumers and to other parties?

Financial account providers that are regulated banks are required to have robust third-party risk management programs that satisfy supervisory guidance issued by the federal banking agencies.[13] These programs are required to include, among other controls, risk-based due diligence on service providers and other third parties, mandatory contractual provisions in service provider agreements that preserve certain rights for the regulated bank, and ongoing monitoring of the service provider relationship. However, not all financial account providers will be subject to this guidance, and the providers that are subject to this guidance may not be in a position to apply their third-party risk management programs to all aggregators and permissioned parties, particularly those aggregators and permissioned parties that access the provider's customer data using means such as screen scraping that do not necessitate an agreement, or even notice, between the parties.

Question 17 – What industry standards currently exist, in development or otherwise, to enable consumer-permissioned access to financial account data?

There are currently a number of industry processes that participants may use to facilitate customer-permissioned access to financial account data, including OAuth, screen scraping, Screenless Data Collection, Open Financial Exchange, and the Durable Data API. Nevertheless, Kabbage supports the creation of generally agreed upon principles and standards for open banking that are aligned with comparable efforts in other jurisdictions. For example, open banking standards currently are being explored in the United Kingdom by the Open Banking Working Group ("OBWG"), which was formed in 2015 by HM Treasury. The OBWG published a manual, *The Open Banking Standard*, which describes how financial data should be created and shared and how access to financial data should be provided.[14] A comparable body of standards for data access in the United States would provide much-needed clarity to financial account providers, permissioned parties, account aggregators, customers, and other stakeholders with respect to the collection, storage, and processing of account data.

Question 20 – Are "industry standard" practices that provide consumers with data access comparable to that envisioned by section 1033 of the Dodd-Frank Act likely to be broadly adopted by consumer financial account providers, permissioned parties and account aggregators in the absence of regulatory action? If not, how will "industry standard" practices be insufficient? What marketplace considerations are likely to bear on such developments? Generally, how will the advent of standard practices for consumer-

[13] *See, e.g.*, Board of Governors of the Federal Reserve System, Guidance on Managing Outsourcing Risk (Dec. 5, 2013); Office of the Comptroller of the Currency, OCC Bulletin 2013-29, Third-Party Relationships (Oct. 30, 2013); Federal Deposit Insurance Corporation, FIL-44-2008, Guidance for Managing Third-Party Risk (June 6, 2008); Consumer Financial Protection Bureau, Compliance Bulletin and Policy Guidance 2016-02, Service Providers (Oct. 31, 2016).

[14] *See* The Open Banking Standard: Unlocking the potential of open banking to improve competition, efficiency and stimulate innovation, *available at* https://theodi.org/open-banking-standard.

permissioned access to consumer financial account data affect competition and innovation in various consumer financial service markets?

Kabbage fully supports the creation of broad-based and flexible industry principles to facilitate customers accessing and using the data they are generating. For example, Kabbage supports the following principles: (i) customer account data should be readily available to customers in a usable electronic form and at no cost, (ii) open banking APIs should use standardized data formats and include access to certain minimum data fields (subject to customer consent) that are required by permissioned parties to provide their services, (iii) objective criteria such as compliance with legal, privacy, and information security requirements should be used to vet potential permissioned parties and data should be made available to those parties that satisfy the criteria, and (iv) providers should not selectively deny access to particular types of permissioned parties in a manner that's anti-competitive or violates other public policy goals.

While these types of industry principles would be helpful in bringing more structure to permissioned access to customer data, there is a risk as there is with all such principles that industry participants will not adopt the standards or fail to adhere to them once adopted. Moreover, financial account providers, permissioned parties, and account aggregators, although technically part of a broader industry for FinTech, generally reside in different industries, thus reaching a consensus on standards may be difficult.

In determining whether to take regulatory action under Section 1033 of the Dodd-Frank Act or otherwise, the CFPB should be mindful of the global nature of the issue. Access to customer data implicates customers of U.S. and non-U.S. financial institutions around the world, so overly prescriptive rules regarding access to customer data would place U.S. companies at a disadvantage vis-à-vis their competitors in other jurisdictions, create a fractured regulatory framework to the extent the rules diverge substantially from international access rules or conventions, and/or stifle innovation by precluding third-party platforms and other FinTech companies from accessing customer data or scaling internationally. Any regulatory action to facilitate access to customer data should be subject to public comment so that a measured and workable approach is developed to the benefit of all interested parties.

* * *

Again, we appreciate the opportunity to comment on the CFPB's request for information and look forward to additional dialogue with the CFPB on data access standards and Kabbage's role more specifically.

Sincerely,

L. Scott Askins

Scott Askins
General Counsel
Kabbage, Inc.