



February 13, 2020

William Wade-Gery
Assistant Director
Consumer Financial Protection Bureau
Office of Card, Payment and Deposit Markets
1700 G St NW
Washington, DC 20552
William.Wade-Gery@cfpb.gov

Gary Stein
Deputy Assistant Director
Consumer Financial Protection Bureau
Office of Consumer Credit, Payment, and Deposit Markets
1700 G St NW
Washington, DC 20552
Gary.Stein@cfpb.gov

Re: The Symposium on Consumer Access to Financial Records (the “*Consumer Financial Access Symposium*”) presented by the Consumer Financial Protection Bureau (the “CFPB”)

Dear Messrs. Wade-Gery and Stein:

As requested, in connection with the CFPB’s Consumer Financial Access Symposium later this month, I am submitting this letter relating to Section 1033 of the Dodd-Frank Act and the various challenges currently presented by the financial data aggregation service marketplace.

Section 1033

As you know, Section 1033 of the Dodd-Frank Act requires a covered financial institution to provide information to a consumer regarding the financial products and services the institution provides to the consumer, as well as transactional, cost and usage information related to those products and services. That information must be made available in an electronic form.

Consumer banks generally provide the above information to consumers in a readily accessible electronic format through online banking sites and mobile applications. Wells Fargo maintains online banking sites and mobile applications that a consumer can use to review their balances, check their transactional history (e.g., recent deposits, withdrawals and credit transactions) and review the costs and fees associated with their accounts. Additionally, such sites and applications provide other tools that allow a consumer a wide measure of control of their accounts – such as the ability to schedule recurring payments, “turn off” credit cards, report fraud and manage security settings (among other things). We also provide ready electronic access to various privacy, regulatory and other account related disclosures at our sites or through our apps. These electronic

channels are accessible through methods that are designed to ensure that a consumer can securely access their financial information.

While Wells Fargo and other financial institutions are already providing consumers direct electronic access to the information required to be made available by Section 1033, we understand consumers may choose to use third party financial applications and services to manage their financial information, which of course is the customer's choice. We are committed to providing our customers the ability to control and share their financial information in a secure and transparent manner, consistent with legal and regulatory expectations.

Current Challenges

Of course, there are challenges associated with a consumer using applications and services provided by financial data aggregators ("**Aggregators**") and other service providers accessing and relying on financial account information maintained at financial institutions ("**Account Data Users**"). Examples of some of these concerns include:

- ***Security Issues.***
 - Consumer banks supervised by federal banking regulators are generally subject to extensive regulatory requirements with regards to the protection of consumer financial data, such as the Interagency Guidelines Establishing Information Security Standards. Aggregators and Account Data Users are generally not subject to the same type of comprehensive data security rules under which regulated financial institutions operate.
 - Until recently, if Aggregators or Account Data Users obtained access to a consumer's financial account information maintained at a financial institution, that information had to be "screen scraped" from the institution's websites. Screen scraping requires the consumer to share their sensitive personal information (like usernames and passwords) to third party Aggregators or Account Data users. Sharing such sensitive personal information presents inherent risk to the consumer and the financial system overall, and also creates liability exposure to financial institutions under Regulation E.
- ***Transparency, Access and Control Issues.***
 - Regulation P requires covered financial institutions to provide disclosures regarding their privacy and information sharing policies and practices. Not all Aggregators or Account Data Users would be subject to the disclosure requirements of Regulation P.
 - When seeking to obtain a consumer's access credentials for a particular financial institution, some Aggregators and Account Data Users use interfaces that include names, logos or other content that may cause confusion for the customer who may believe that they are logging into their bank, when in reality they are logging into the Aggregator or Data Account User who is screen scraping to access their financial data.
 - Account Data Users often rely on an Aggregator to screen scrape a consumer's account information from a financial institution's website. In many cases, consumers using the services of an Account Data User will have no knowledge of the existence of such Aggregator, nor the ability to limit the Aggregator's access to the consumer's financial information.
- ***Operational and Cost Issues.*** Financial institutions such as Wells Fargo incur significant costs to ensure reliable access to their online banking sites. Screen scraping from those sites imposes significant

costs on the financial institution and can potentially impact the response times and availability of those sites.

Industry/Marketplace Approaches & Shortcomings

Wells Fargo and other financial institutions are taking a combination of approaches to address these challenges.

- ***Bilateral Agreements.*** Many financial institutions (including Wells Fargo) have successfully negotiated bilateral agreements with Aggregators relating to the access, use and sharing of consumer financial account information. These agreements (and the operational processes relating to the implementation of these agreements) are generally designed to address:
 - ***Security.*** A consumer's financial account data will be shared through secure means and subject to security commitments by the applicable Aggregator and downstream Account Data Users. Screen scraping will ultimately be eliminated in favor of more secure methods of data access such as application program interfaces.
 - ***Consent/Control/Access.*** The access and use of a consumer's financial account data by the applicable Aggregator or Account Data User will be subject to the consumer's consent (and the consumer's ability to revoke such consent).
 - ***Transparency.*** A consumer will have ongoing access to information regarding (a) the categories of financial data it chose to make available to third parties and (b) the identity of the relevant parties with whom it directed that information to be shared.
 - ***Liability Allocation.*** In order to meet applicable safety and soundness regulations and guidance, when a bank shares financial information with an Aggregator under a bilateral agreement, the Aggregator would agree to assume certain responsibilities and liabilities in connection with their access and use of that financial information.
- ***Industry Standards.*** Various Aggregators, Account Data Users and financial institutions (including Wells Fargo) have been actively working through industry consortiums, such as the Financial Data Exchange ("FDX"), to develop a common set of principles and technical standards for the sharing and use of consumer financial account information. These industry approaches complement (but do not fully replace) bilateral agreements.

Bilateral agreements and industry standards are empowering customer choice and allowing for sharing consumer financial data in a more secure and transparent manner. However, while more financial institutions, Aggregators and Account Data Users are using bilateral agreements and industry standards, adoption is not complete across the industry. There is also inconsistency in how these contractual and industry approaches are implemented by different market participants.

Potential Solutions & Regulatory Involvement

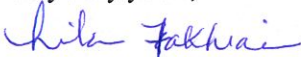
Wells Fargo remains committed to using bilateral agreements, and working with industry bodies such as FDX, to ensure that consumers can control their data sharing preferences in a secure and transparent manner. We believe these two approaches can continue to yield steady progress in addressing the issues currently facing the financial data aggregation service marketplace.

We understand there may be a desire for the CFPB to promulgate more formal regulations or guidance to better protect consumers. In analyzing whether regulations or additional guidance should be provided, consideration should be given to the following:

- **Ensuring Continued Progress.** Any regulations or guidance should not overlook the progress that financial institutions, Aggregators and Account Data Users have made in reaching consensus over the key principles associated with data sharing (*i.e.*, consumer consent and control, security of data access, transparency of data access).
- **Consent/Control/Verification.** Consumers need to have the ability to determine the identity of the Aggregators and Account Data Users with whom their available financial account information, including any account access credential, is shared and the purposes for which such data is being shared. However, financial institutions should be able to implement reasonable processes to verify and authenticate the identity of a consumer who is electing to share his or her account information with such third parties.
- **Security.** Financial institutions are subject to wide-ranging regulations designed to ensure the security of customer data. Aggregators and Account Data Users that access the same categories of consumer financial account data as regulated financial institutions should be subject to similar data protection duties and obligations.
- **Liability Allocation.** Financial institutions should not be required to bear the costs and liability associated with security failures of Aggregators and Account Data Users. If an Aggregator or Account Data User fails to implement reasonable security controls with regards to the account data in its possession, a financial institution should not incur the liability associated with such failure – whether that liability arises from breach notification costs, unauthorized financial transactions, fines or legal claims.
- **Regulatory Consistency.** To the extent any regulations are promulgated with respect to customer-permissioned financial data sharing arrangements, such regulations should take into account the existing safety/soundness, privacy and data security regulatory frameworks under which financial institutions operate.

Much progress has made in recent years to address issues in the financial data aggregation services marketplace. Wells Fargo remains committed to working with both regulators and the wider industry to continue to improve the consumer's ability to control and share their financial account data in a secure and transparent manner.

Very truly yours,



Lila Fakhraie
Senior Vice President
Wells Fargo Bank, N.A.