Value and Benefit of Model Data Access Agreement

Why is there a need to transition to APIs?

Many fintech applications currently provide products and services to consumers by requesting that consumers provide their banking platform usernames and passwords to the fintech applications to be used to access the consumer's bank accounts and take financial data through an automated process called "screen-scraping". This process requires consumers to give their banking platform credentials to third parties. It can also be opaque because it may not be clear to the consumer what parties are involved, and what the consumer is giving consent to. The Clearing House Payments Company (TCH) Connected Banking Initiative is focused on facilitating direct connections (application programming interface or "APIs") between the banks and the providers of data services. A transition to APIs may accelerate enhanced safety and security of customer account data, facilitate a consumer consent model focused on clarity and transparency of the data sharing process and enable future fintech innovation.

What is the anticipated value and benefit of the Model Agreement?

The fact that banks and data aggregators get to the point where a legal agreement is contemplated demonstrates a shared desire to migrate to API's. However, legal agreements between banks and data aggregators can take 12 months or more to develop and finalize and have become a bottleneck to the development of API relationships for those interested in reaching them. To alleviate that friction, TCH has developed a Model Agreement that banks[1] and data aggregators [2] can use as a reference to facilitate the development of terms and conditions enabling banks to share customer permissioned account information with data aggregators on behalf of financial apps[3] through a secure API, streamlining the potential switch to secure API technology. Use of the Model Agreement is entirely voluntary and the agreement is intended to be modified as circumstances may warrant. Further, the Model Agreement avoids taking any positions on commercial terms, which will need to be negotiated strictly between the parties. The

[1] Financial services entities, including banks and other financial institutions, are referred to in the Model Contract as "**FSEs**."
[2] Data access platform providers, including data aggregators, are referred to in the Model Contract as "**Data Providers**."
[3] Fourth parties with which data aggregators have a direct relationship, such as application developers, are referred to in the Model Contract as "**Data Provider Clients**."

Model Agreement does, however, provide a potential foundation of common, generally accepted terms that individual banks and data aggregators can use as a reference; reducing, if they choose, the need to define and negotiate the same terms each time they enter into a bilateral data access agreement.

How is TCH ensuring that the Model Agreement appropriately focuses on consumer control, data security, and accountability for impact on the ecosystem?

To ensure that the Model Agreement appropriately focuses on consumer control, data security and accountability for impact on the ecosystem, the Model Agreement has been specifically constructed to be consistent with the CFPB's *Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation* (Oct. 18, 2017), as noted in the table below. These CFPB principles are foundational to TCH's Connected Banking initiative, and the Model Agreement specifically.

The following table maps relevant Model Agreement terms to the CFPB's principles, and highlights the benefits of the Model Agreement for customers and for the integrity of data access practices generally.

Relevant CFPB Principles	**Relevant Model Agreement Terms**
A number of Principles support greater informed **consumer control** over access to and use of account information, *e.g.*: • Principle No. 1: Consumers should be able to access and define the use of their data through trusted third parties. • Principle No. 2: Information should be available in forms that are readily usable to consumers and authorized third parties. • Principle No. 3: Terms for accessing, storing, and using customer data should be disclosed and not be overly broad. • Principle No. 6: Consumers should be informed and able to readily ascertain the authorized third parties	The Model Agreement addresses these objectives through a number of provisions, *e.g.*,: • Art. 1.1(b) expressly states that a purpose of the Model Agreement is to allow customer information to be accessed, used, shared, and analyzed through a unified platform. • In Art. 2, Account Information is a defined term that includes the account related data of a customer, and is only to be shared through the express consent of a customer. There are multiple provisions requiring controlled access to and safekeeping of Account Information • Art. 3.3(c) provides that a Data Provider will access customer data only once it provides all necessary and appropriate disclosures and obtains all necessary consents from the customer.

Relevant CFPB Principles	**Relevant Model Agreement Terms**
accessing and using their account information. • Principle No. 8: Consumers should have reasonable and practical means to resolve disputes arising from unauthorized data sharing, unauthorized payments, and failures to comply with other obligations.	• Art. 4.1 provides that a FSE will provide access to Data Providers to customer data through a secure method. • Art. 4.3(a) limits access to the secure method for data access to only authorized users. • Art. 4.5(a) limits the scope of access and retention of customer information permitted Data Providers to only that information which is authorized by the customer, and is reasonably necessary to provide the customer with the services to which it consented. • Arts. 4.5(c), 4.10, and 8.6(a) provide that customer-related Data Provider obligations will "flow down" to Data Provider Clients. • Art. 5.1 provides that Data Providers and Data Provider Clients will provide clear and conspicuous disclosures to customers regarding how data will be collected, accessed, stored and used. • Art. 5.2 provides that a Data Provider will ensure that formal Agreements will reflect relevant terms that are accepted by customers. • Art. 5.5 addresses customer complaints and disputes.
Safety and security of consumer data is a primary focus of the CFPB principles, *e.g.*: • Principle No. 1: "Access does not require consumers to share their account credentials with third parties." • Principle No. 5: "Consumer data [should be] accessed, stored, used and distributed securely."	The Model Agreement addresses this objective through a number of provisions, *e.g.*: • Art. 3.3 affirmatively states that a key objective of the Model Agreement is to facilitate secure access to data without reliance on the sharing of account credentials with third parties and their use in screen scraping. Accordingly, Art. 3.3(b) provides that a Data Provider will cease using, and not use, screen scraping to obtain account data, and will only use APIs or data feeds provided by or on behalf of the FSE, for as long as access to Account Information is made

Relevant CFPB Principles	Relevant Model Agreement Terms
	available through the applicable API or other applicable data access method. • Arts. 6.5 and 6.6 contemplate audits at least annually that would include security reviews and assessments, and certifications that Data Providers maintain proper controls and procedures. • Art. 7.1 provides that Data Providers will develop quality assurance and internal controls "to ensure that Account Information is accessed in a secure manner." • Art. 13.6 provides that Data Providers will ensure that adequate risk assessment processes and "use of strong industry standard encryption" are in place to maintain control over confidential information. • Art. 13.7 provides for data safeguards, including "FSE Security Requirements" that will be set forth in Exhibit 2 to the Model Agreement (13.7(a)); and the express provision that a Data Provider will transfer account data beyond its internal firewalls "in a secure and confidential manner," and at a minimum in an encrypted format (13.7(g)).
Accountability for risks, harms, and costs introduced to consumers by the access of account information is addressed in Principle No. 9, which provides that the commercial participant that introduces such risks, harms or costs should be responsible for them.	Art. 14 addresses this issue by allocating risks to the responsible parties based on defined indemnification rights. The allocation of liability framework set forth in the Model Agreement is intended to incent the party that is in the best position to protect consumer information to do so, and to be responsible for inadequate levels of protection in the event that the privacy and security of consumer data is compromised.

In sum, the Model Agreement is intended to provide banks and data aggregators with a tool that can ease their contracting efforts and facilitate the development of direct relationships between banks and data aggregators.