Connected Banking:
Enabling innovation and customer control through a more secure exchange of financial data

M A R C H  2 0 2 0
Overview

Americans increasingly manage their money digitally, with over half (54%) of U.S. banking customers using mobile financial apps to navigate mobile payments, budgeting, sending and receiving money, accessing loans, investing in stocks and purchasing insurance.

These services provide consumers significant benefits that will continue to expand as financial apps and traditional banks identify new ways to use data to customize their offerings and better serve customers. However, protections and controls around the use of bank-held data have not kept pace with the dramatic growth of financial apps.

- Bank-held data is usually collected by financial apps through a process called “screen scraping,” whereby the apps log in using customer-supplied bank account credentials to gain unrestricted access to customers’ personal and financial information.

- Financial apps and other data aggregators often store consumers’ bank account login credentials and sensitive account information, courting serious harm in the event of a data breach. Because logins use customer-supplied usernames and passwords, banks have a hard time distinguishing between screen-scraping “bots,” malicious bots and actual customers. The 24 owner banks of The Clearing House (TCH) estimate that up to 45% of their bank website log-ins come from data aggregators.

Research conducted by TCH in 2019 shows that most consumers are unaware of financial data collection practices and want more control and transparency when sharing their data. For instance, most financial app users (70%) are confident that their information is both private and secure. However, consumers have limited knowledge about what data is collected, and how data is stored and shared. This is likely because this information is contained within the apps’ terms and conditions, which a majority of financial app users (79%) did not read. Terms and conditions are also not standardized across apps and many today allow the app to use all available data in customers’ bank accounts, resell the data to third parties, or even grant power of attorney to initiate transactions.

Most financial app users (80%) are also not fully aware that the apps or third parties may store their bank account username and password. Once they realize this, 68% are uncomfortable with the apps’ level of access. Similarly, a majority of financial app users do not know how their data is being used and shared by the apps. Less than 20% of users are aware that the apps may use third parties to access consumers’ personal and financial information, with nearly 65% expressing discomfort with these arrangements.

With the lack of awareness about which parties can access data, what data they can access, and what they can do with the data, consumers are not in control of their data. We need a new ecosystem that puts consumer control and safety at the forefront.

While there is widespread support among stakeholders for migration to direct application programming interface (API)-based connections, the question is how to make the change. To that end, TCH is currently working with our member banks and other stakeholders to develop standards and tools that will enable the ecosystem to collaboratively create a consumer-focused financial data sharing system with the security and transparency that people expect from their financial institutions. This system, known as Connected Banking, will enable sustained innovation in financial services by making the exchange of consumer financial data safer and more secure, while giving consumers greater control over how their data is used and by whom.
In the European Union, the Revised Payment Service Directive (PSD2) is enabling open banking. Enacted in November 2015 and rolling out in stages, PSD2 phased out screen scraping in 2019 and is requiring banks to grant third parties access to customer data via dedicated interfaces. PSD2 further stipulates that these interfaces may only be used in rendering the specific services the third party provides to the consumer. These regulations, in addition to the implementation of the General Data Protection Regulation on May 25, 2018, mandate a future in which EU consumers are provided explicit, transparent disclosures of third party access, collection and use of their data. The U.K. is implementing its own version of open banking, which took effect on January 13, 2018. The U.K.’s Open Banking Initiative requires banks to open their data to third parties but takes PSD2 one step further by requiring that they do so in a standard format.

These early attempts at managing the issue were well-intentioned and employed several promising solutions. However, this type of prescriptive approach, created by parties that don’t live and breathe these issues every day, and are not required to live with the results, often produces suboptimal solutions and unintended consequences. For example, while moving from screen scraping to APIs is advisable, PSD2 mandated the move without addressing any API standards. As a result,
banks ended up creating their own individual APIs, which didn’t integrate with other banks’ APIs. This required third parties and data aggregators to create separate API builds for each bank, significantly slowing adoption.

U.S. financial regulators, in contrast, have taken a more market-oriented regulatory stance. In 2017, the Consumer Financial Protection Bureau (CFPB) issued a principles-based approach for consumer data privacy and security, which addressed the topics of data access, payment authorization, data security, and consent, among other things. As a result, the CFPB made its intentions clear and left implementation in the hands of the operational experts.

So far, we are seeing early promise. For example, the CFPB’s approach has encouraged collaboration between stakeholders across the many areas required to build a sustainable ecosystem, including the launch of the Financial Data Exchange (FDX), an industry-wide consortium focused on creating a common API standard for data sharing, as well as several deals between banks and data aggregators to share data through APIs.

With thousands of banks, data aggregators and third party financial apps, it is critical to standardize technology, vendor management processes and consumer protections to achieve sustainable growth.

<table>
<thead>
<tr>
<th>Dimension</th>
<th>CFPB Principles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
<td>Authorization; no requirement to share credentials</td>
</tr>
<tr>
<td>Data Scope and Usability</td>
<td>Access only to necessary data</td>
</tr>
<tr>
<td>Control / Informed Consent</td>
<td>Fully-disclosed terms; data revocation rights</td>
</tr>
<tr>
<td>Authorizing Payments</td>
<td>Payment initiation requires ‘separate and distinct authorization’</td>
</tr>
<tr>
<td>Security</td>
<td>Secure access, storage, use and distribution of data</td>
</tr>
<tr>
<td>Access Transparency</td>
<td>Consumers know the purpose, frequency and type of data accessed</td>
</tr>
<tr>
<td>Accuracy</td>
<td>Data is accurate and current</td>
</tr>
<tr>
<td>Unauthorized Access</td>
<td>Consumers can dispute / resolve unauthorized access; unauthorized parties are held responsible</td>
</tr>
<tr>
<td>Accountability Mechanism</td>
<td>Parties’ goals / incentives are aligned to enable safe consumer access and deter misuse</td>
</tr>
</tbody>
</table>
The TCH Approach – Connected Banking

*Enabling innovation and customer control through a more secure exchange of financial data*

We believe that a collaborative approach between regulators and key stakeholders, led by the private sector, will ultimately result in a more sustainable ecosystem, where core elements are addressed upfront and flexibility remains to quickly address early mistakes. With this approach, the U.S. can create a system that achieves the same overarching goals of open banking without facing some of the obstacles that have limited its potential in other parts of the world.

The system also must be principles-based to allow it to keep pace with rapidly advancing technology that is fueling innovation in financial services. A collaborative, market-led approach will enable the ecosystem to resolve issues and unintended consequences more quickly because it doesn’t require legal or policy changes. On the other hand, a prescriptive, regulatory approach would force stakeholders to quickly adapt to the letter of the law rather than to build out comprehensive solutions.

---

### We believe that this system must be guided by three core values:

<table>
<thead>
<tr>
<th>Acting in the best interest of the consumer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guidelines and actions are in the best interest of customers and help them better manage their finances whilst protecting their privacy and security</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Protecting and enhancing the stability and safety of the financial industry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guidelines and actions help foster a safe and sound financial system that reduces overall risks and creates resilience</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Fostering efficiency and collaboration within the financial industry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guidelines and actions should help all parties interact and share data more efficiently, providing value to all parties involved</td>
</tr>
</tbody>
</table>

---

### CONNECTED BANKING vs OPEN BANKING

<table>
<thead>
<tr>
<th>OPEN BANKING</th>
<th>CONNECTED BANKING</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prescriptive regulatory approach</td>
<td>Follows CFPB principles</td>
</tr>
<tr>
<td>Lack of standardized APIs in some markets</td>
<td>Designed by those who live and breathe it every day</td>
</tr>
<tr>
<td>Banks, data aggregators operate independently</td>
<td>Agile, market-oriented approach</td>
</tr>
<tr>
<td>Unintended consequences</td>
<td>Standardized through APIs, by FDX</td>
</tr>
</tbody>
</table>

- Enables evolution from screen scraping to more secure API access
- Allows data access to be right-sized based on consumer consent and third party data needs
- Goal is to promote consumer control and consent
- Encourages collaboration among industry stakeholders to drive adoption

Building on the key tenets outlined above, TCH is advocating for a solution — called Connected Banking — that combines the best features of Open Banking and a more market-based approach that for the first time will put consumers in control of their data, ensure the safety of critical financial information and the banking system, and build an ecosystem that’s collaborative and positioned for long-term growth and sustained innovation.
What Fundamental Changes Are Required?

With Connected Banking, the industry will move from an environment where there was previously no direct relationship between banks, data aggregators or third parties to one where all parties are focused on serving a mutual customer. These relationships require agreements on technology, legal contracts, bank and third party risk-management and consumer permissions. Streamlining these standards and practices are essential to scaling migration from screen scraping.

The key characteristics of Connected Banking are:

- Standards for API-based technology
- Principles for required contracts between banks and third parties
- Tools for centralizing and sharing third party risk management
- Centralized network infrastructure to accelerate and scale APIs and consumer consent

API-based Technology Standards:

API and token-based technology are a natural choice to replace screen scraping as the tool to share bank-held data and enable customer control of data access. APIs allow third parties to offer a wide variety of services while empowering consumers to control and securely share their financial data.

- APIs enable direct connections between the financial app and bank website, enabling data sharing without requiring consumers to share their bank account login credentials. This means third parties will only have access to data designated by the customer.

- APIs allow third parties to receive up-to-date data directly from the bank, significantly enhancing data quality.

- Tokens containing consumer preferences for which applications can access which data elements can be stored, updated and exchanged between banks and financial apps.

Common standards are required to implement APIs at a reasonable pace. While APIs require less standardization than other technologies, key elements (i.e., data definitions, use cases and security elements) can be extremely complex to define and rebuild for every implementation. Europe learned this lesson during PSD2, when the lack of API standards across banks significantly slowed third party implementations.

This is why TCH supports and is a founding member of the Financial Data Exchange or FDX. FDX is a subsidiary of the Financial Services Information Sharing and Analysis Center (FS-ISAC) and unites cross-industry participants to support effective and consistent use of an interoperable standard and operating framework centered on the FDX API. Collaboration between industry leaders across banking, data aggregation, and the largest users of data aggregation services is essential to creating standards in a collaborative, sustainable way that will drive adoption.
Standardized Terms that Facilitate Bilateral Contracts:

With more than 10,000 banks and credit unions in the U.S., and a rapidly growing community of data aggregators and financial apps, creating legal contracts can be a significant barrier to adoption. Execution of early contracts between banks and data aggregators have taken up to a year or longer. We believe that a model agreement, which defines key terms and ensures upfront understanding of the key contractual elements, will go a long way toward streamlining this process.

TCH and our member banks developed a model agreement that can be used as a starting point for financial institutions, financial apps and other third party data aggregators. The model agreement outlines suggested terms for agreements that provide for the permissioned sharing of customer data, making data sharing processes faster and more efficient to better service mutual customers. Some key areas include: customer permissions and informed consent for data aggregation and sharing; questions of legal liability; service-level agreements; data access methods and minimum-security requirements; data access for other parties with whom the third party may share consumer information; and dispute resolution.

The model agreement is a set of voluntary guidelines rather than requirements. Parties may use and modify terms as they see fit during their negotiations. The goal of the model agreement is to provide a comprehensive framework that can save time and resources in the negotiating process and lead to agreements with strong data security provisions.

Permissioned Access and Control Mechanisms:

Consumers should control which parties have access to their data. However, in order to maintain consumers’ trust in the data aggregation and sharing process, financial institutions and financial apps should offer mechanisms through which consumers can grant permissions and control how their information is accessed, used, stored and shared. Enabling this level of consumer control requires technology and infrastructure that not all banks have the resources to develop.

TCH and our member banks have outlined five elements that such mechanisms should cover:

1. **Consumer disclosures:** Financial institutions and financial apps should disclose to consumers the accounts and data types that a third party needs to access to perform its services and alert consumers if other entities will or may access their information. The extent of the disclosure should be informed by the sensitivity of the data.

2. **Consumer consent:** Consumers should be given the opportunity to provide explicit consent to each third party that wishes to access their data. The consent should cover which data type(s) the third party can access; how that data is used; which other parties may receive it; and the frequency and duration of data access.

3. **Access permissions:** Once data access has been granted, consumers should have the ability to manage their permissions, including by modifying permissions, revoking consent and having “the right to be forgotten” (i.e., the ability to revoke data access in such a way that the data is no longer stored by the third party).

4. **Opt-in principles:** Financial apps and other third parties should create transparent opt-in mechanisms to obtain consumer consent for all instances of data collection. Opt-ins should happen when a consumer first starts using a financial app, whenever the app is updated and if the consumer permission expires.

5. **Permissions expiry protocols:** Financial institutions should consider establishing guidelines for when consumer permissions for data access expire. There are different approaches financial institutions could take. They may require third parties to renew consumer consent if a consumer has been inactive on an app for a certain period, or they may require renewed consent when certain events, such as a data breach, occur.
1. Consumer signs up for third party app
2. User selects bank & request permissions. User is then redirected to bank portal authorization & consent
3. User selects which account and/or data type(s) they would like to give Data Aggregator and Financial Apps consent to access
4. Data Aggregator can only access bank account and data explicitly consented to by the user
5. Bank data is populated into the app
Centralized Network Infrastructure:

Building out these capabilities is a serious effort. Currently different parties — including large financial institutions, smaller banks and financial apps — have come together to meet the needs of their customers and build technology to deliver these solutions. However, these have been on a bilateral basis, with individual integrations between parties.

A centralized network infrastructure that facilitates the adoption of APIs and token standards for the Data Aggregation ecosystem may help accelerate the technology that the industry needs at scale. While banks have been developing bilateral commercial and technology-integration relationships for some time, a centralized approach would allow the industry to better anticipate and react quickly to market changes. Bilateral relationships are not scalable over the long term, as the need to maintain connectivity and contractual relationships with entities continues to intensify. To date, bilateral relationships have made some progress. However, even for parties who have these relationships, screen scraping has been slow to migrate to APIs. TCH, 11 of its owner banks, and Fidelity have partnered on Akoya, a centralized network that can help implement and integrate thousands of banks and thousands of financial apps through a single touchpoint.

This centralized network approach would streamline industry investment and improve efficiency and security. It will also be scalable and more likely to accelerate adoption from ecosystem participants, including aggregators, banks and fintechs of all sizes. More specifically, the key components include a standard API connection leveraging the FDX standard; infrastructure for consumer control of financial data; sufficient risk management reflective of the highly regulated nature of financial data; and operations required for rapid and scaled implementations.

Third Party Management:

Banks are frequently required to do third party due diligence on the entities they do business with. While data aggregator relationships are distinguishable from that of the typical bank vendor, banks may still be concerned over potential reputational risk that could accrue from data aggregator and financial app relationships that are facilitated on behalf of bank customers. Accordingly, banks may reasonably subject such parties to third party risk management requirements. This means that every data aggregator and, potentially, the clients of the data aggregators may need to undergo bank risk reviews. Given that risk reviews typically take between 3–6 months to perform, this could become a significant bottleneck on the entire system.

Much-needed relief in this regard would be afforded by a standard, centralized assessment process to evaluate the safety and security of third party apps, where common assessments can be completed once and reused across multiple banks. While each bank is required to make an independent evaluation of the results of the assessment, completing a single assessment will be significantly simpler for all parties in the ecosystem. An assessment tool is currently being piloted and will be introduced into the market in the near future.

Conclusion

The Connected Banking ecosystem will tremendously benefit consumers, financial apps, data aggregators and banks. An environment built and managed by its users, and those ultimately responsible for its safety and soundness, will be a more agile system, capable of enabling innovation and customer control through a more secure exchange of financial data.

Robust data security requirements driven by the same principles-based approach adopted by the CFPB will encourage collaboration and ensure a higher standard of consumer protection without hamstringing the implementation process. Consumers can expect the ease with which they can share data to be matched by the security with which their data is protected.

Connected Banking done right is a system for everyone. In collaboration with the financial services industry, financial apps industry, and its employees, stakeholders and customers, we look forward to building a better system together. We invite you to visit our webpage to contact us directly or send us an email at: Gregory.MacSweeney@theclearinghouse.org.