Connectivity + Data + Experience = **Growth**

The **Ultimate Guide** to

FINTECH DATA

MX

From Screen Scraping to APIs

In January of 2020 Chase announced plans to block fintech companies from screen scraping data on their website. Screen scraping, the process of gathering data from one app and displaying it in another, has been a common practice for decades but Chase expressed concerns around potential fraud and a lack of transparency about who was scraping the data and for what purposes. As a result, they announced they would be replacing all screen scraping with sanctioned API channels.

By making the move toward sanctioned API channels, Chase paved the way for banks to proactively share their data in the United States. It's a move that's also representative of an increased focus on data regulation and data standards, and it suggests that the use of APIs in the financial services industry is likely to grow over the coming years.

So, how did we get here? And what's the history of connectivity in financial services?

Most importantly, how can you, as someone who works with financial technology, make the best decisions around connectivity and data today?

These are the questions we'll answer in this ultimate guide.

*If you're reading a hard copy of this guide and want to see hyperlinks to all sources cited, visit mx.com/library/ultimate-guides

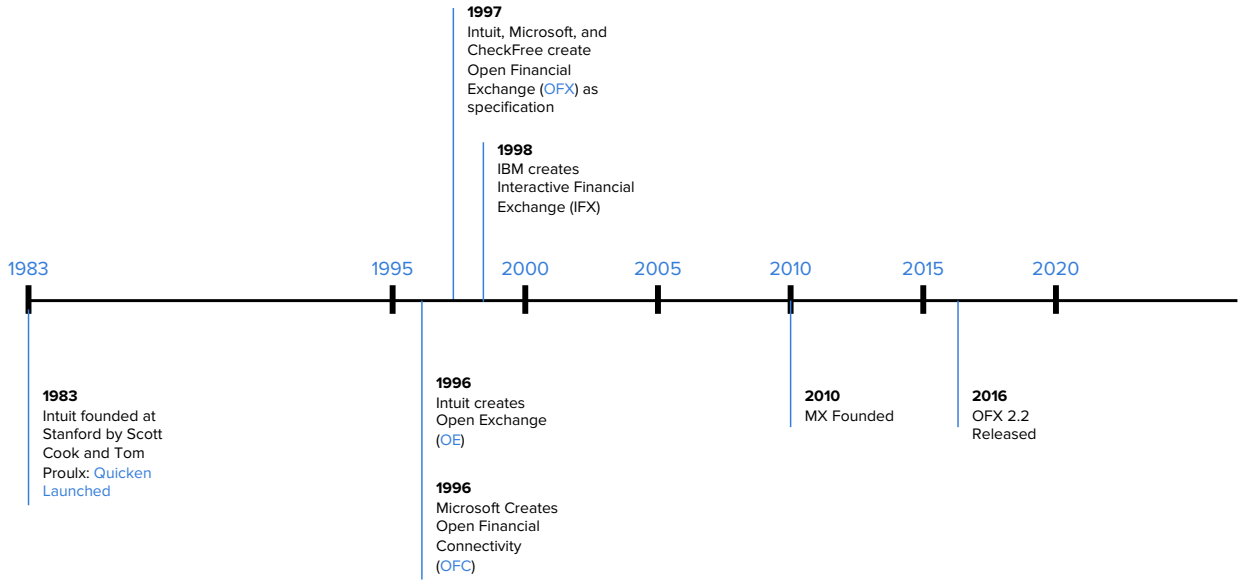
The History of **Connectivity and Data Sharing**

While there were a few software programs in the industry prior to the 1980s, the idea of data sharing started in earnest with the founding of Intuit in 1983.

It was a time of manual entry and skeuomorphic design. For instance, Intuit created an interface that required users to manually enter the information onto a digital check in order to manage their finances.

But most people likely don't want to spend their Saturday and Sunday manually entering all of their financial data. And so in the mid 1990s, there was a heyday of automated approaches where users didn't have to manually enter their data. At first there were a multiplicity of standards including Intuit's open exchange (OE) and Microsoft's open financial connectivity (OFC). In 1997 companies started to unite around the open financial exchange (OFX), a standard driven primarily by the team at Microsoft Money.

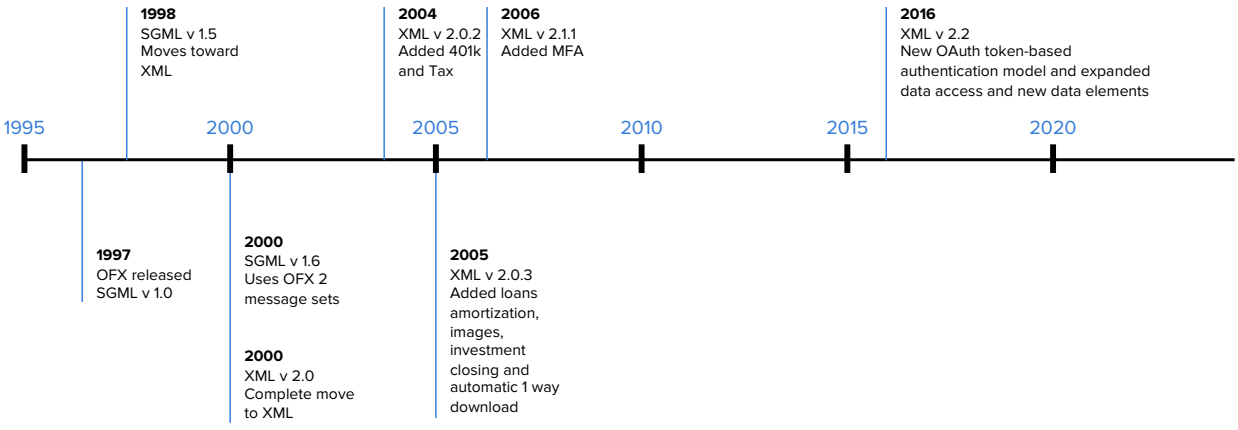
History of Fintech Data



OFX was updated only sparingly since it started in 1997. It moved toward XML in 2000, added 401(k) and tax data in 2004, added MFA data in 2006 and OAuth token based authentication in 2016.

This brings us to today.

OFX Version History



The **Current State** of Data Sharing

There are four primary ways to share data right now.

1. Screen scraping

As stated above, screen scraping is the process of gathering data from one app by inputting user credentials (such as username and password) and displaying their data in another app. Scraping is the foundation of data access today, largely because it allows fintechs to choose which data fields they want to obtain and because fintechs can connect without having an official relationship with the financial institutions they scrape data from. By comparison, sanctioned API channels allow financial institutions to limit the fields they want to share, which can result in consumers losing out on the ability to access the data that's most useful to them in an aggregated experience.

While screen scraping can break when institutions change their site structure, it's still widely useful — especially with whitelisted IPs. By whitelisting, financial institutions and fintech companies can keep each other informed about upcoming changes while shining light on which companies are pulling what data, avoiding the potential for malicious actors.

The biggest downside to screen scraping for financial institutions is that they **aren't always aware of who is scraping their data.**

2. Manual entry

Manual entry is flexible since users can input any data they want — covering all transactions from cash to card payments and beyond.

The downsides are obvious: manual data entry is tedious, prone to user input errors, and doesn't allow for the vast number of benefits that come from automation, including dynamic alerts, AI-driven financial advice, data analysis, and more. It can also break if a website gets updated without considering data that has been manually entered.

3. OFX (API standard)

The upside to OFX is that it's usually reliable and contains known fields and formats since, by definition, it's a standard. As a result, OFX access has had some great adoption (more than 7,000 financial institutions, according to their site).

However, OFX also has a lot of downsides: It isn't regularly maintained, past versions vary considerably, it requires relationships with each financial services company fintechs connect to, and data can be incorrect or missing. Sometimes old or incomplete integrations lead to getting data for the wrong field returned in OFX feeds.

All of these options **have upsides and downsides**, & none are a silver bullet.

4. API (proprietary connections)

Proprietary connections share a lot of the same upsides as OFX, particularly when it comes to reliability, speed, and consistency. The biggest difference is that the best proprietary connections are well maintained, making them the optimal choice in many cases.

The downsides are that proprietary connections are currently not common (though that's quickly changing), the data can be limited in instances where financial institutions restrict the number of accessible fields, and the connections can be turned off in the event a financial institution decides to pivot.

All of these options have upsides and downsides, and none are a silver bullet. That said, APIs are typically the best of the four, all things considered.

The industry is having more conversations around how to develop solutions that will optimize the experience for everyone involved.

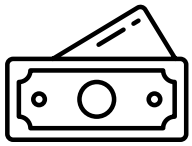
Data **Regulation**

Regulation around data sharing and data privacy can quickly get complicated since opinions differ widely between countries and even between companies and regulators within each country.

We'll touch on just a few of the recent developments here.

PSD2

In 2015, the Revised Payment Services Directive (PSD2) replaced the Payment Services Directive (PSD) of 2007 in the European Union. This updated directive focused on online and mobile payments, with particular attention to open banking and APIs. Ultimately, it requires financial institutions to share data with their customers so those customers can use the apps, UI, and services that create the best financial outcomes. This directive may play an enormous role in preparing other nations to figure out the best approach to connectivity and data sharing.



2015

the Revised Payment Services Directive (PSD2) replaced the Payment Services Directive (PSD).

This directive may play an enormous role in preparing other nations to figure out **the best approach to connectivity & data sharing.**

CFPB Statements

In 2017, the Consumer Financial Protection Bureau (CFPB) outlined principles for data sharing for the purpose of meeting the needs of consumers, fintechs, and financial institutions. These principles, most of which focus on consumers, include:

- **Access** - Consumers can authorize third parties to securely access their data.
- **Data Scope and Usability** - Third parties that have authorized access can “access the data necessary to provide the product(s) or service(s) selected by the consumer.”
- **Control and Informed Consent** - “Consumers can enhance their financial lives when they control information regarding their accounts or use of financial services.” This means that a customer could obtain their data and move it from one bank to another.
- **Authorizing Payments** - “Providers that access information and initiate payments obtain separate and distinct consumer authorizations for these separate activities.” This means that a consumer could initiate a payment from their bank account to a provider of their choice without sharing their bank credentials.
- **Security** - “Consumer data are accessed, stored, used, and distributed securely.”
- **Access Transparency** - “Consumers are informed of, or can readily ascertain, which third parties that they have authorized are accessing or using information regarding the consumers’ accounts or other consumer use of financial services.”
- **Accuracy** - “Consumers can expect the data they access or authorize others to access or use to be accurate and current.”
- **Ability to Dispute and Resolve Unauthorized Access** - “Consumers have reasonable and practical means to dispute and resolve instances of unauthorized access.”
- **Efficient and Effective Accountability Mechanisms** - “The goals and incentives of parties that grant access to, access, use, store, redistribute, and dispose of consumer data align to enable safe consumer access and deter misuse.”

It's a good thing to

CREATE

a new, modernized principle-based standard for data exchange, data security and data portability.

Even though these statements are non-binding, they have generally been applauded by a variety of industry players since they take all the major views into account. For instance, Rob Morgan, VP at the American Bankers Association, said their organization is "pleased that the CFPB's new principles for consumer-authorized data sharing acknowledge key recommendations ABA outlined earlier this year, particularly with regard to security, transparency and control." And Rob Foregger, founder and EVP of the fintech company NextCapital says, "It's a good thing to create a new, modernized principle-based standard for data exchange, data security and data portability." He adds, "Just like in the healthcare industry, a patient has the right to bring their healthcare records to another doctor for a second opinion, financial services customers need to maintain the right to access and use their financial data across institutions."

> "Financial services customers need to **maintain the right to access and use their financial data** across institutions."
>
> **ROB FOREGGER**
> Founder and EVP of the fintech company NextCapital

Financial Institutions

Financial institutions have also been dedicated to preparing for open banking and API connections. For instance, the Financial Services Information Sharing and Analysis Center (FS-ISAC), a consortium of nearly 7,000 financial institutions, has developed durable data APIs (also known as DDAs) to help move the industry forward. DDAs incorporate the principles of PSD2 as well as OAuth 2.0 to tokenize credentials. Another example is the Financial Data and Technology Association (FDATA), "a global association for financial services companies operating in fintech."

In addition, top financial institutions are increasingly providing sanctioned API access to data and building their own API connections. This is almost certainly the direction that the industry will head in, with the largest financial institutions leading the way and smaller institutions following behind.

Some of the institutions that have signed contracts for direct APIs.

On this note, institutions ranging from USAA to Capital One are in discussions or have already signed contracts to get access to direct APIs. Of course, signing the contract and implementing are two different things (the latter obviously being much more difficult), but it's a clear indication of where things are going.

A bank's use of third parties does not diminish the bank's responsibility to perform the activity in a safe and sound manner and in

COMPLIANCE

with applicable laws and regulations.

The OCC

On March 5th, 2020 the Office of the Comptroller of the Currency (OCC) issued an updated set of frequently asked questions in response to a 2013 bulletin titled "Third-Party Relationships: Risk Management Guidance." This bulletin helps with "assessing and managing risks associated with third-party relationships," a term they define as "any business arrangement between a bank and another entity, by contract or otherwise."

In their updated answers, the OCC reiterates that "a bank's use of third parties does not diminish the bank's responsibility to perform the activity in a safe and sound manner and in compliance with applicable laws and regulations." The OCC also calls upon supervised banks to conduct governance over third-party aggregators that employ credential-based scraping to collect customer data. More concretely, they state that banks must plan to provide third-party traffic reports of companies that are scraping data.

This statement might seem like bad news since it brings added governance responsibilities. However, in reality we believe that the change will likely be a net positive as it bolsters cooperation between financial institutions and fintechs while also pushing the industry closer to adopting open banking for data sharing.

General Regulations

Finally, there are the broad regulatory changes, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). These policies affect banking, even though they also extend beyond the industry. They're core to the foundation of data sharing and the rollout of OAuth. They're evidence that regulators in different industries are working to figure out how to protect end users when their data is shared and how to give them better control, insight, and trust. With the case of the CCPA, for instance, consumers have complete control over their personal data — how it's shared, who gets access, and how companies will make money off of it. Both cases are an indication that movements toward more open data and data privacy in one region tend to influence the movement of further protections in other regions.

With so many players involved and so many opinions about data sharing, finding the right approach to regulation can be terribly difficult. To a degree, it's like building a car while driving. Still, the plans are moving along, and the industry as a whole is headed in the right direction.

In the end, clarity benefits everyone involved in the ecosystem. Providing structured data access with better risk mitigation means that financial services companies can better maintain trust with customers, help them make informed decisions, innovate quickly, and securely offer new products.

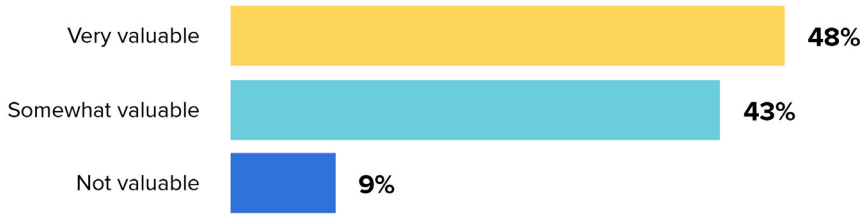
As these initiatives develop, it's essential for companies to maintain security protocols, from SOC2 certification to PCI compliance. Since no one in the industry — financial institutions or fintech companies — wants a data breach, every aggregator should adhere to these standards.

Despite the difficulties and complexity that surrounds connectivity and data sharing, it's clearly the right choice for consumers.

What Consumers Want: **Original Survey Data**

To better understand how consumers view this space, we surveyed more than 1,000 random US consumers. For instance, when we asked people whether it is or would be valuable to see all their accounts (e.g., checking, savings, credit card, auto loans, investment accounts, etc.) in one app, 90% said yes.

How valuable is it or would it be to see all your accounts in one app?



MX research, survey of 1,000+ US consumers

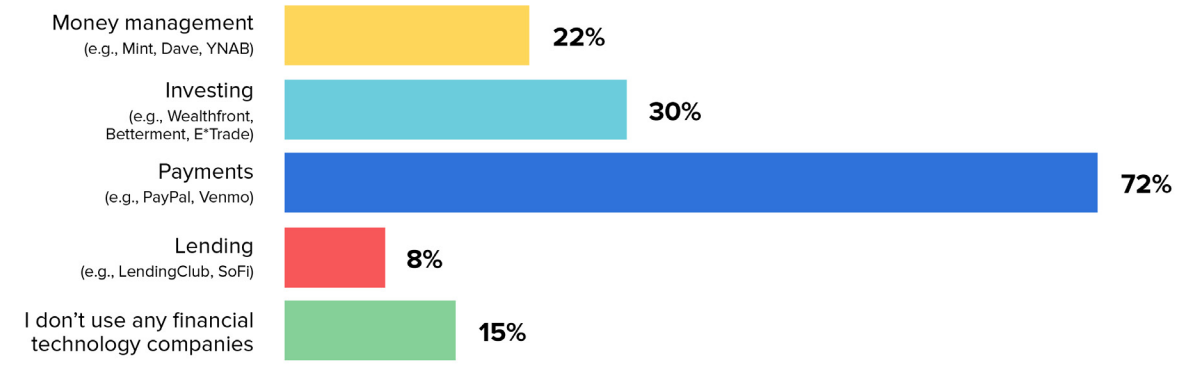
40% of consumers say they currently have this ability, indicating that there's a lot of potential to grow here.

Do you currently have the ability to see all of your financial accounts in one app?

MX research, survey of 1,000+ US consumers

22% of respondents said that they currently use money management (which typically leverages data aggregation) with a fintech company. And 30% say they use a fintech company for investments (which also typically leverages data aggregation). This opens up the potential for these fintech companies to be viewed as a consumer's primary financial hub.

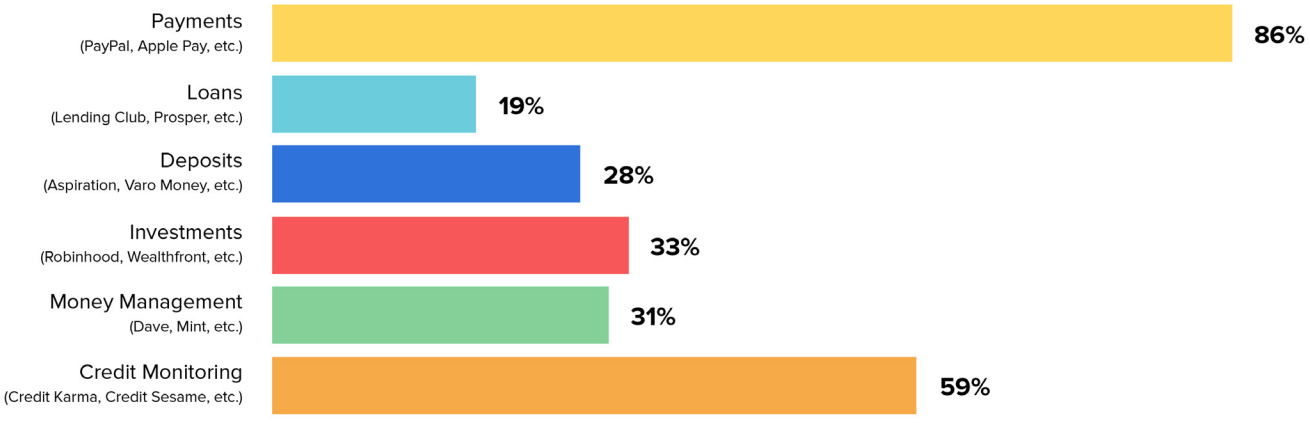
What banking services do you use a financial technology (fintech) company for rather than your bank or credit union? (Select all that apply.)



MX research, survey of 1,000+ US consumers

When we asked a similar question but changed the phrasing to be about which activities they felt comfortable with (rather than which ones they currently use) the numbers were much higher, with 86% saying they felt comfortable with using a tech company for payments.

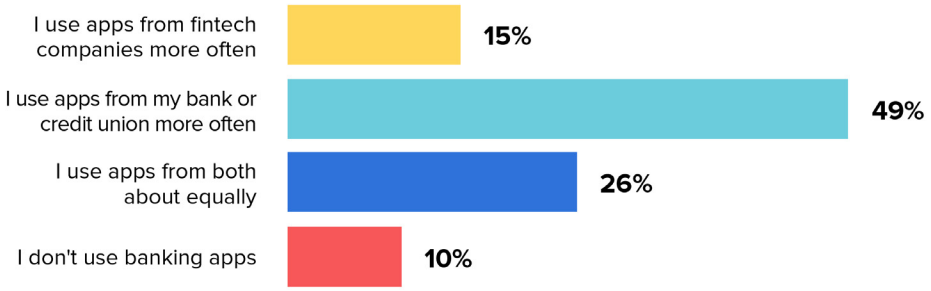
Which of the following banking activities do you feel comfortable doing through a tech company? (Select all that apply.)



MX research, survey of 1,000+ US consumers

That said, most people still use financial apps from their financial institutions more often than they use apps from fintech companies.

How often do you use apps from fintech companies compared to apps from your primary bank or credit union?



MX research, survey of 1,000+ US consumers

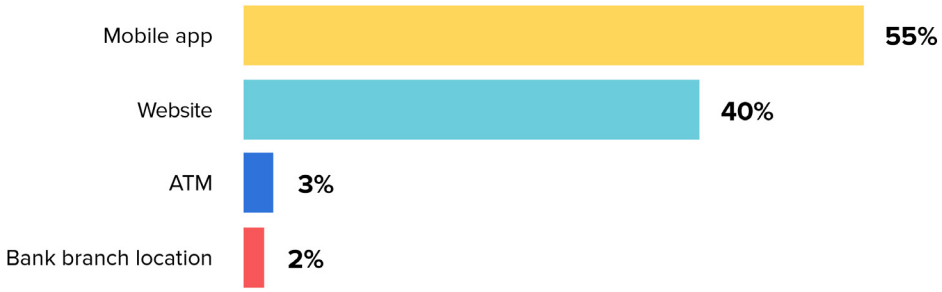
However, 36% say they can foresee the day when they'd switch to fintech companies for the primary financial needs.

Do you think you would ever reach a point where you would do most banking activities through a fintech company instead of a bank or credit union if they offered comparable digital services?

MX research, survey of 1,000+ US consumers

One reason for this: 95% of respondents said that their primary means for checking their account balance is digital.

What is your primary means for checking your account balance?



MX research, survey of 1,000+ US consumers

Since 39% of respondents say they've reduced how often they bank somewhere based on a poor digital experience, getting digital right matters.

Have you ever reduced how often you bank somewhere based on a poor digital experience?

MX research, survey of 1,000+ US consumers

Enabling customers to see all their data in one place also benefits financial services companies. These benefits include added transparency, clearer permissions, and increased security.

Financial institutions that implement APIs will also have full

INSIGHT

into what data is shared and who it's shared with.

1. Added Transparency

By whitelisting data aggregators financial services companies have additional transparency into scraped traffic via IP addresses. In this way, leading banks and credit unions will know via their digital banking provider or core system exactly what's happening in the scraping process and will be able to immediately see if an unwanted, malicious third-party suddenly starts scraping their data. They can rest assured, knowing exactly which companies are scraping and for what purposes.

In addition, financial institutions that implement APIs will also have full insight into what data is shared and who it's shared with, bringing an added level of transparency and clarity to the process.

2. Clearer Permissions

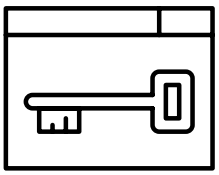
Everyone in the financial services industry — from regulators to fintechs — rightly worries about the potential for customer data to be shared without the customer's direct permission. By whitelisting screen scraping and implementing API connections, financial services companies make it easier for customers to give consent. These permissions can be set on a case-by-case basis, so each customer is empowered to choose what they want people to see and what they don't want people to see. For example, if a customer sets up a budgeting app, they can grant permission for a particular set of data that allows a financial advisor to view their progress toward their financial goals instead of sharing all their account balances.

This added control over permissions reflects the entire banking industry's desire to reduce and mitigate risk on behalf of the customer.

3. Increased Security

With traditional screen scraping, each customer has to input their credentials including username and password. This opens up the possibility, however unlikely, that another party could intercept these credentials.

By whitelisting the screen scraping process, it makes it easier to see who is at fault in the event of a data breach.



API connections bring a higher level of

SECURITY

because the process replaces sharing credentials with anonymized, single-use digital tokens.

By whitelisting the screen scraping process, **it makes it easier to see who is at fault in the event of a data breach.**

In addition, API connections bring a higher level of security because the process replaces sharing credentials with anonymized, single-use digital tokens. This means that bad actors can't access the personal information of end users during a transaction. Tokens de-identify user data, greatly increasing the chances that personal data will not be subject to risk.

At MX, we believe that personally identifiable information should not be shared with third or fourth parties and that systems should be in place to delete or revoke access. We also believe that until token usage is universally adopted (or nearly so), credentials should be handled with the highest security protocols.

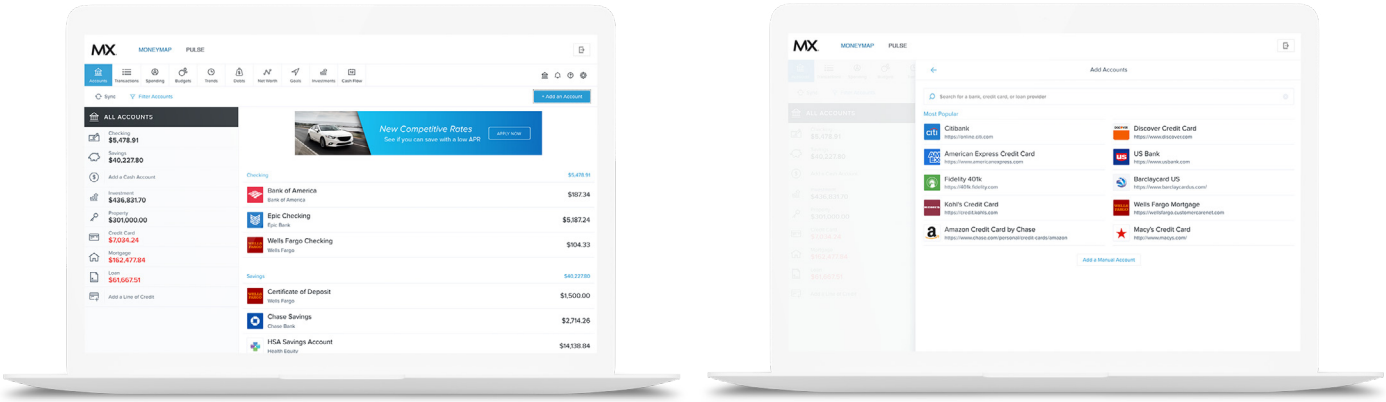
Conclusion: Connectivity and Data Are the **Future of Banking**

Consumers clearly want the ability to see and manage all their accounts in one app. This is the future of banking. As an industry we need to move forward in a way that's secure without ever losing sight of customer demand. By implementing the right approach to connectivity and data sharing, we can do just that.

For the foreseeable future, screen scraping will continue to play an important role in banking. However, more financial institutions are implementing APIs, making the practice increasingly standard, particularly with the largest institutions.

The move to API connections has the potential to greatly benefit financial institutions and fintech companies. In addition to the benefits listed above, API connections also enable increased innovation since customer-permissioned data sharing is bi-directional, meaning that financial institutions and fintech companies share and receive data from the sources they connect with via API. This sets up all parties involved to use that data in creative ways to best serve and advocate for their customers.

Above all, this customer-centered approach to banking is at the heart of where things are headed. And that is potentially terrific news for the industry.



Want to see how MX can be your collaborative partner?
Visit MX.com/atrium.

[Request a Demo]

mx.com