Australian Competition and Consumer Commission
23 Marcus Clarke Street
Canberra ACT 2601

Dear ACCC,

Plaid appreciates the opportunity to submit comments in response to the ACCC's CDR consultation on how to best facilitate the participation of third party service providers that collect or facilitate the collection of CDR data from data holders ("intermediaries"). As a financial data aggregator operating in major global markets including the US, Canada, UK, Ireland, France, and Spain, Plaid plays an important intermediary role in enabling the efficient functioning of consumer data-driven ecosystems.

The ACCC requested Plaid's input on the role of intermediaries and the implications of various approaches to accreditation and licensing in the markets in which we operate.

Our comments therefore focus on two key elements for the ACCC's consideration:

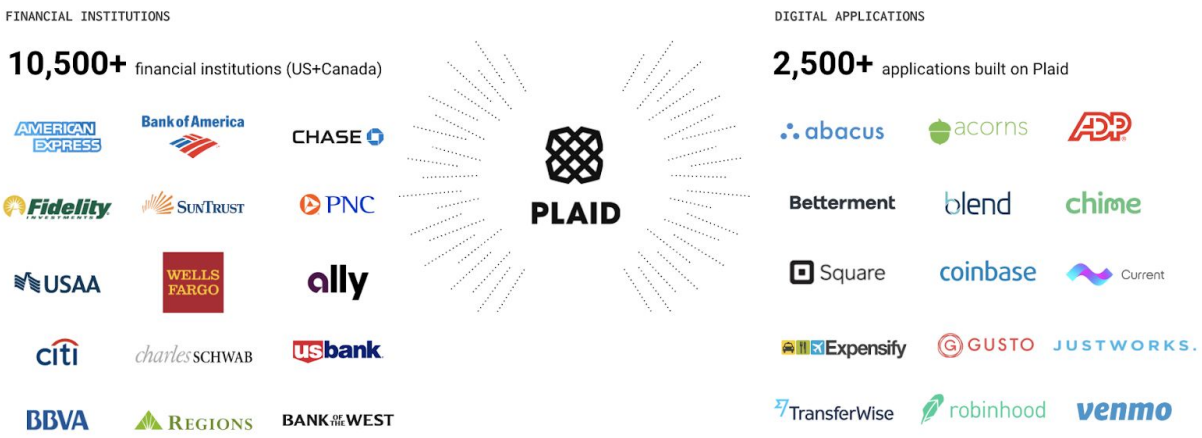
1. The ACCC must restructure CDR around intermediaries as key licensees
2. The ACCC must prioritize consumer rights over contractual standards

Intermediaries provide benefits to three stakeholders:

Intermediaries benefit ecosystems:

Plaid serves ecosystems as an intermediary by building integrations across financial institutions and financial technology applications to enable the seamless and secure flow of data. In the US, there are more than 10,000 financial institutions. Without Plaid, each financial institution would need to develop Application Programming Interfaces (APIs), and every application would need to build integrations into every financial institution, in order to allow consumers to permission their financial information to third parties. But API development is not the core business of banks, and integration management isn't the core business of consumer financial apps. Plaid and other intermediaries specialize in this connectivity and compete with each other based on data quality and consumer and developer experience. This frees banks and financial apps from inefficiently building redundant API connections, and allows them to compete with each other on the quality and price of their consumer products.

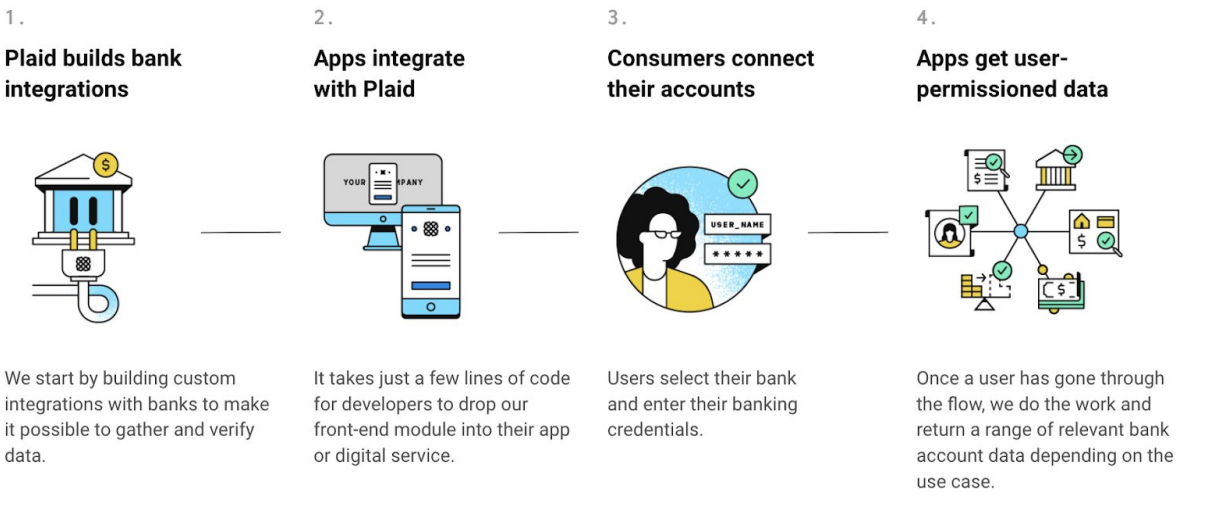
Plaid builds the infrastructure that powers modern, digital financial services



While Australia has fewer financial institutions, the CDR is expansive and is intended to ultimately apply to hundreds of different businesses, all with different types of data and few of which develop APIs.

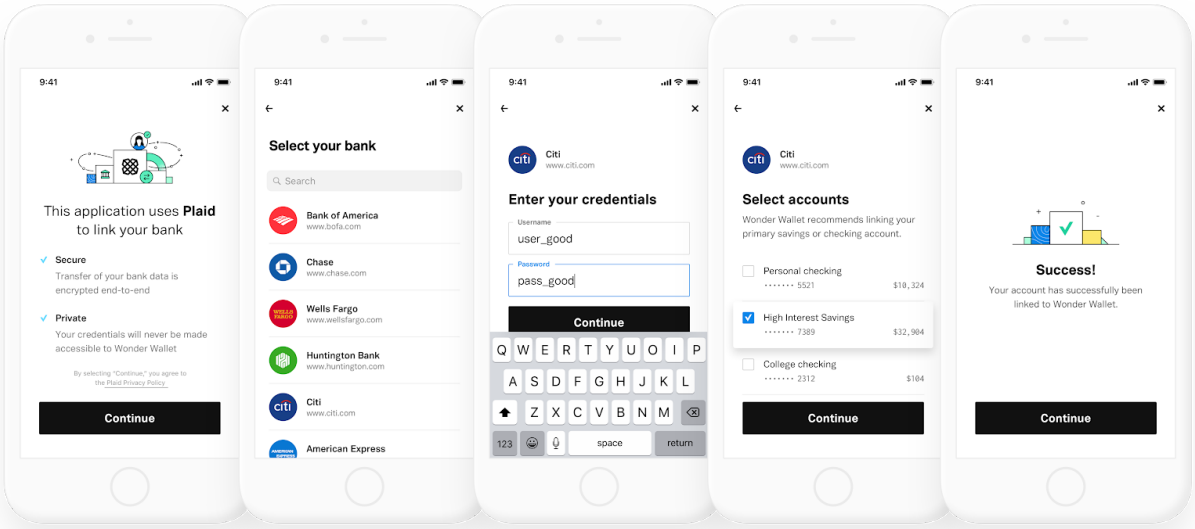
Intermediary specialists can build integrations to a variety of data sources, standardize consumers' data and deliver it to third party applications providers in the format best suited for consumers' desired use cases. This lets businesses across the ecosystem focus on their core services, while giving consumers the benefits of data access and portability across the entire ecosystem.

Integrating with Plaid allows users to grant access to data



Intermediaries benefit consumers:

Plaid provides consumers with a transparent and consistent consent process for data sharing. Our Link portal explains to consumers that Plaid connects their accounts, and enables consumers to consent to share their data (see visual below). Plaid enforces this consistent Link experience across the ecosystem. Without intermediaries taking this role, consumers would experience different consent flows each time they link accounts, potentially undermining their understanding and control over data sharing.



Intermediaries benefit regulators:

With intermediaries, supervision is centralized, not diffuse. Regulators can look to intermediaries for visibility into the ecosystem rather than trying to track issues across several thousand players. Intermediaries can also enforce changes uniformly across the ecosystem - when adjustments to data sharing rules are necessary, they can be implemented across the full ecosystem by a few sophisticated parties, who in turn can easily be supervised on the speed and quality of that implementation.

Intermediaries can also set behavioral standards across the ecosystem through contractual obligations, reducing the need for prescriptive regulations. For example, Plaid mandates sound privacy and security practices as an intermediary by establishing requirements on third party providers that receive data through Plaid. (Please find attached in Appendix A our Developer Policy, which includes details on these flowdown requirements.) These policies greatly reduce the need for regulators to provide and oversee licenses to each and every third party provider, as intermediaries can enforce standards across the ecosystem in concert with regulators. With

streamlined oversight, regulators can build a tiered system of accreditation reflective of individual third parties' market size and risk.

Consumer rights supersede contractual standards

Core consumer rights vs contractual obligations

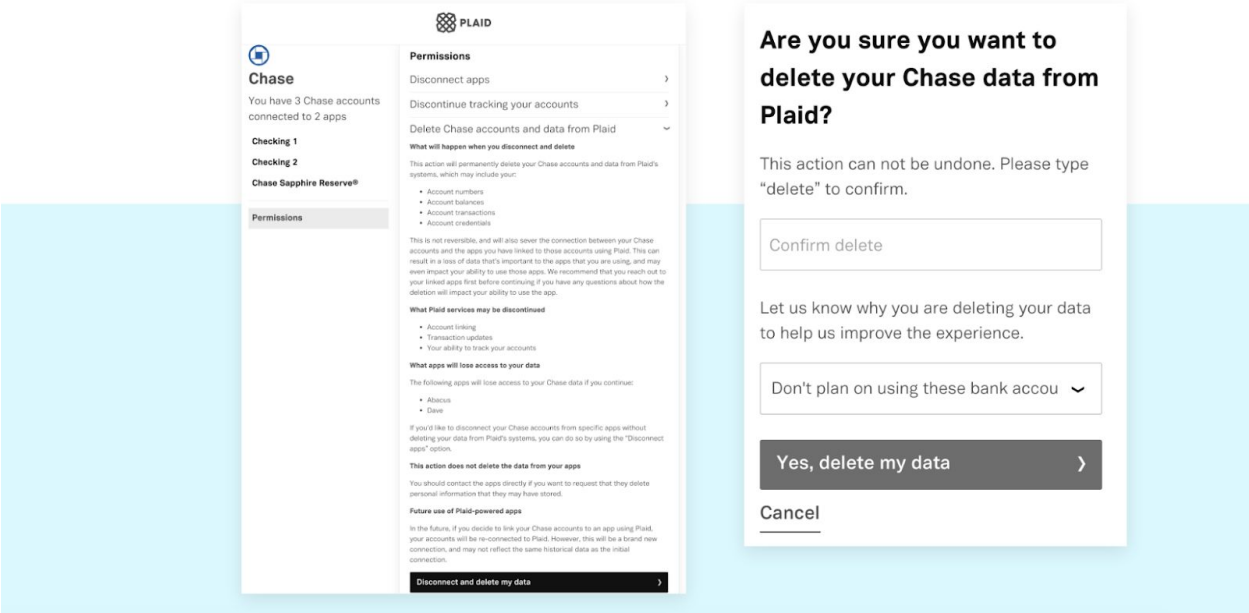
Plaid's developer policy enforces certain consumer rights through contract. However, we believe that certain core consumer data rights should be universal, and should not be left to the individual contracting of intermediaries. To ensure that consumers are empowered and in control of their data, an ecosystem centered on intermediaries should include regulatory mandates that require the intermediary to honor fundamental consumer data rights. The most fundamental consumer rights to which Plaid wittingly abides are included in CDR Section 1.10, establishing rules for outsourced providers:

- Prohibiting the use or sale of data beyond consumers' direction
- Granting consumers rights to transparency and control over their data, including the ability to de-permission and/or delete information they have previously shared

Data sales change the incentive structure of the market away from consumers. Instead of sharing specific information in return for a specific service, the consumer would be at risk of having their information used for a variety of opaque ways unrelated to the the service they requested. Plaid does not sell data or share it beyond the explicit direction of the consumer. Other intermediaries do, suggesting that regulatory intervention is necessary to ensure consistency.

Transparency and control are critical to building trust in data sharing, as highlighted in Plaid's white paper "Give Consumers Control of their Data" (see appendix B). Data deletion is important because consumers often change their minds about products, or wish to delete their data once the purpose of their data sharing is fulfilled. Repurposing CDR Section 1.10 as part of an intermediary accreditation process can ensure that intermediaries propagate transparency, control, and deletion through a complex system.

Consumers can disconnect and delete financial institution connections and data



Attempts at implementing standard contractual obligations can introduce barriers to entry and reinforce competitive asymmetries where larger institutions leverage advantages over new entrants (this is the case in the United Kingdom, for example).

Intermediaries play an essential role in serving data sharing ecosystems. Plaid takes on complexity from parties whose resources are better directed towards serving consumers, empowers consumers to share and manage their data, and provides regulators with visibility across the system.

Australia's Consumer Data Right leads the world in placing consumers at the center of the ecosystem. To ensure the system built upon CDR is most effective for consumers, the best role for intermediaries to play is one in which they become accredited parties under CDR, are prohibited from selling consumer data beyond consumer consent, and are able to enter into contractual agreements with financial institutions, outsourced parties, and un-accredited third party providers to best serve consumer demands.

We appreciate your consideration of these comments.

Sincerely,

Benjamin White
Policy R&D, Plaid

See below for appendices A and B
Appendix A: Plaid's Developer Policy
Appendix B: Plaid's 2019 White Paper, "Give Consumers Control of their Financial Data"

Developer Policy
Effective Date: December 30, 2019

This Developer Policy ("Policy") provides rules and guidelines that govern access to or use by our developers (“you” or “your”) of the Plaid API, websites (“Site”), dashboards, related tools, and other products or services (collectively, the "Service") provided by Plaid Inc. and its subsidiaries, including Plaid Financial Ltd. and Plaid, B.V. (“Plaid”, “we”, “our”, and “us”). Any violation of this Policy may result in suspension or termination of your access to the Service and/or access to end users’ personal and financial information ("End User Data").

By accessing and using the Service, you agree to comply with all the terms of this Policy. This Policy will apply each time you access or use the Service. If you are agreeing to the terms of this Policy on behalf of an organization or entity, you represent and warrant that you are so authorized to agree on behalf of that organization or entity. This Policy is important; please read it carefully.

We may update or change this Policy at any time in our discretion. If we make any changes to this Policy that we deem to be material, we will make a reasonable effort to inform you of such change. If you don’t agree with the change, you are free to reject it; unfortunately, that means you will no longer be able to use the Service.

Jump to section:

Registration

To sign up for the Service, you must create an account ("Account") by registering on our Site and providing true, accurate, and complete information about yourself and your use of the Service. You agree not to misrepresent your identity or any information that you provide for your Account, and to keep your Account information up to date at all times. It is your responsibility to maintain access to your Account; you may never share your Account information, including your

Plaid Dashboard password, as well as your API authentication credentials, including your Client Identification Number ("Client ID") and secret, with a third party or allow any other application or service to act as you.

If you become aware of any unauthorized use of your Account or any other breach of security, please immediately notify us via email to security@plaid.com.

Compliance with Applicable Law

When using the Service, you must abide by all applicable local, state, national, and international laws. You also confirm that you, your business, your employees, your service providers, and any others acting on your behalf adhere to all applicable laws, especially those pertaining to financial data and to data protection, privacy and data security.

In addition, you certify that you, your officers, directors, shareholders, direct and indirect parent entities, subsidiaries, and affiliates:

- are and will remain in compliance with all applicable import, re-import, sanctions, anti-boycott, export, and re-export control laws and regulations (including all such laws and regulations that apply to a U.S. company, such as the Export Administration Regulations, the International Traffic in Arms Regulations, and economic sanctions programs implemented by the Office of Foreign Assets Control (OFAC));
- are not subject to, or owned by parties that are subject to, sanctions or otherwise identified on any sanctions-related list, including but not limited to lists maintained by the United States government (such as the List of Specially Designated Nationals and Blocked Persons, maintained by OFAC, the Entity List maintained by the U.S. Commerce Department's Bureau of Industry and Security, and the CAATSA section 231(d) list maintained by the U.S. State Department), the United Nations Security Council, the United Kingdom, the European Union or its Member States, or other applicable government authority; and
- are not engaging, and will not engage, in activities which may require or permit any applicable government authority to pursue an enforcement action against, or impose economic sanctions on you or us.

The certifications immediately above are not sought, and are not provided, if and to the extent such request or certification would constitute a violation of the EU Blocking Statute, of laws or regulations implementing the EU Blocking Statute in the EU Member States or in the United Kingdom, or any similar anti-boycott, non-discrimination, or blocking provisions foreseen in applicable local laws.

You are solely responsible for ensuring that your use of the Service is in compliance with all laws applicable to you, including without limitation, the rules and guidelines of any system or network that facilitates payments and any security requirements, including under the Payment Card Industry Data Security Standards (PCI-DSS), as may be applicable to you.

Security

You are responsible for securely maintaining your Plaid Dashboard username and password, as well as your API authentication credentials, including your Client ID and secret. You must notify us immediately in the event of any breach of security or unauthorized use of your Account or any End User Data. You must never publish, distribute, or share your Client ID or secret, and must encrypt this information in storage and during transit.

Your systems and application(s) must handle End User Data securely. With respect to End User Data, you should follow industry best practices but, at a minimum, must perform the following:

- Maintain administrative, technical, and physical safeguards that are designed to ensure the security, privacy, and confidentiality of End User Data.
- Use modern and industry standard cryptography when storing or transmitting any End User Data.
- Maintain reasonable access controls to ensure that only authorized individuals that have a business need have access to any End User Data.
- Monitor your systems for any unauthorized access. Patch vulnerabilities in a timely fashion. Log and review any events suggesting unauthorized access.
- Plan for and respond to security incidents.
- Comply with relevant rules and regulations with regard to the type of data you are handling, such as the Safeguards Rule.

Data Storage

Any End User Data in your possession must be stored securely and in accordance with applicable laws.

Account Deactivation

Once you stop using the Service in accordance with any applicable agreement you may have with us, you may deactivate your Account by following the instructions on the Site. We may also deactivate your Account if you have ceased using the Service for three months; your applicable agreement with us terminates or expires; or as reasonably necessary under applicable law. After your Account deactivation, we will deprovision your access to all End User Data associated with your integration.

Even after your Account deactivation, and to the extent permitted under applicable law, we may still retain any information we collected about you for as long as necessary to fulfill the purposes outlined in our privacy policy/statement, or for a longer retention period if required or permitted under applicable law.

Prohibited Conduct

You agree not to, and agree not to assist or otherwise enable any third party to:

- sell or rent End User Data to marketers or any other third party;
- access or use the Service or End User Data for any unlawful, infringing, threatening, abusive, obscene, harassing, defamatory, deceptive, or fraudulent purpose;
- collect and store end users' bank credentials and/or End User Data other than as required to access or use the Service, as authorized by the end user, as permitted by Plaid, and as permitted under applicable law;
- use, disclose, or retain any "nonpublic personal information" (as defined under the Gramm-Leach-Bliley Act) or "personal information" (as defined under the California Consumer Privacy Act) other than in strict compliance with applicable law;
- use, disclose, or otherwise process any "personal data" (as defined in Regulation (EU) 2016/679 (General Data Protection Regulation)) other than in strict compliance with applicable law;
- access or use the Service or access, transmit, process, or store End User Data in violation of any applicable privacy laws or in any manner that would be a breach of contract or agreement with the applicable end user;
- access or use the Service to infringe any patent, trademark, trade secret, copyright, right of publicity, or other right of any person or entity;
- access or use the Service for any purpose other than for which it is provided by us, including for competitive evaluation, spying, creating a substitute or similar service to any of the Service, or other nefarious purpose;
- scan or test (manually or in an automated fashion) the vulnerability of any Plaid infrastructure without express prior written permission from Plaid;
- breach, disable, interfere with, or otherwise circumvent any security or authentication measures or any other aspect of the Service;
- overload, flood, or spam any part of the Service;
- create developer accounts for the Service by any means other than our publicly-supported interfaces (e.g., creating developer accounts in an automated fashion or otherwise in bulk);
- transfer, syndicate, or otherwise distribute the Service or End User Data without express prior written permission from Plaid;
- decipher, decompile, disassemble, copy, reverse engineer, or attempt to derive any source code or underlying ideas or algorithms of any part of the Service, except as permitted by applicable law;
- modify, translate, or otherwise create derivative works of any part of the Service;
- access or use the Service or End User Data in a manner that violates any agreement between you or the end user and Plaid; or
- access or use the Service or End User Data in a manner that violates any applicable law, statute, ordinance, or regulation.

Suspension and Termination

We reserve the right to withhold, refuse, or terminate access to the Service and/or End User Data in whole or in part where we believe the Service is being accessed or used in violation of this Policy or any other Plaid agreement, including Plaid's agreements with any third party partners or data sources of Plaid (each, a "Partner"), or where use would pose a risk of harm, including reputational harm, to Plaid, its infrastructure, its data, the Service, an end user, or a Partner.

We will use reasonable efforts to notify you via email or other method when deciding to withhold, refuse, or terminate access to the Service and/or End User Data. We may immediately suspend or terminate access without notice if appropriate under the circumstances, such as when we become aware of activity that is a violation of any applicable law or when we determine, in our sole discretion, that harm is imminent.

Plaid will not be liable for any damages of any nature suffered by you or any third party resulting from Plaid's exercise of its rights under this Policy or under applicable law.

Reporting Violations

If any person becomes aware of a violation of this Policy, we request that you immediately notify us via email to legalnotices@plaid.com. We may take any appropriate action -- including reporting any activity or conduct that we suspect violates the law to appropriate law enforcement officials, regulators, or other appropriate third parties -- in our sole discretion in respect to such violations.

Miscellaneous

The failure by you or Plaid to exercise in any respect any right provided for herein shall not be deemed a waiver of any further rights hereunder.

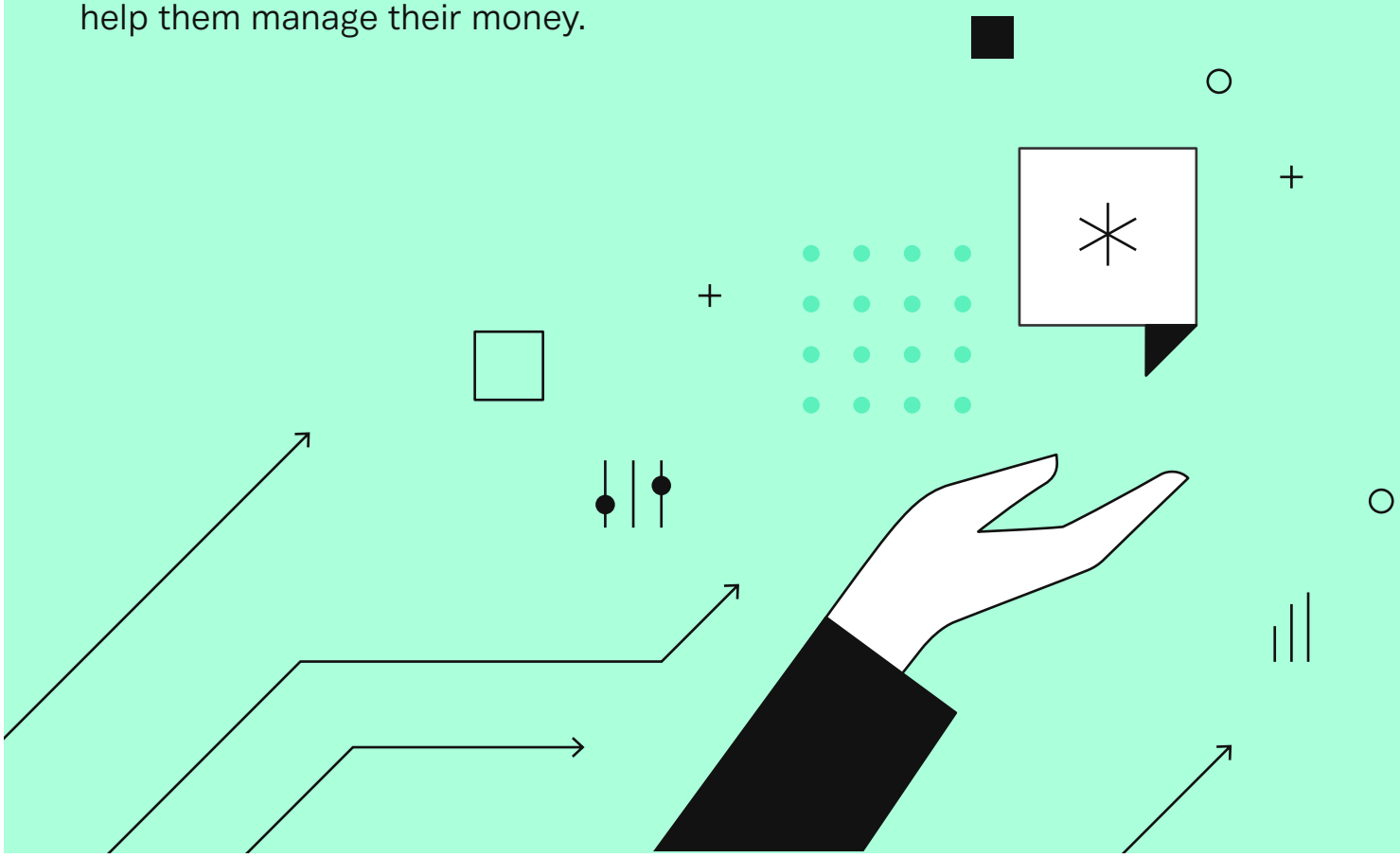
If any provision of this Policy is found to be unenforceable or invalid, that provision shall be limited or eliminated to the minimum extent necessary so that this Policy shall otherwise remain in full force and effect and enforceable.

PLAID

plaid.com

Give Consumers Control of Their Financial Data

As financial services go digital, millions of consumers benefit from apps that help them manage their money.



Protect consumer control of data to build trust.

As financial services go digital, millions of consumers benefit from apps that help them manage their money.

Millions of consumers today choose to share their financial data to access personalized financial products and services designed with their needs and goals in mind. In the United States, 46% of consumers now use a digital financial product or service. While impressive, there is an opportunity to encourage even broader adoption among a wider variety of consumers. For these tools to become ubiquitous—like ATMs or credit cards—two key conditions must be met:

1. Providers must offer financial products that are easily accessed by **all** consumers.
2. Consumers must be guaranteed control over their data when engaging with these services.

The market has made significant progress toward meeting the first need. For example, 40 million people use peer-to-peer payments app Venmo to pay friends, family, and service providers. And in 2018 alone, consumers saved more than $5.6 billion with micro-savings and micro-investing tools like Stash and Acorns. However, a portion of consumers remains wary of sharing their financial data and will benefit from clear rules of the road.

The second need still must be robustly addressed to encourage larger-scale adoption. For fintech to have the wide-sweeping impact of innovations like ATMs and credit cards, which consumers were slow to trust but ultimately changed the consumer finance landscape, consumers must be in control.

In this whitepaper, we survey the ways in which the fintech ecosystem is delivering on consumer demand for personalized financial services. We examine the current state of consumer trust in digital financial services and explore past precedents for building trust by giving consumers meaningful controls. Finally, we propose **four principles—understanding, choice, neutrality, and protection**—to follow when giving consumers control over their digital financial data.

A portion of consumers remains wary of sharing their financial data and will benefit from clear rules of the road.

46%

46 percent of consumers now use a digital financial product or service.

Consumers use their data to take control of their financial lives.

By permissioning their financial data to secure financial technology providers, consumers gain access to a rich new set of products and services to meet their individualized needs. Take, for example:

- A loan underwritten with bank balance and transactions data
- A service that helps prevent insufficient funds by modeling user cash flow over time
- An app that rounds up credit card purchases and invests the spare change in an investment account

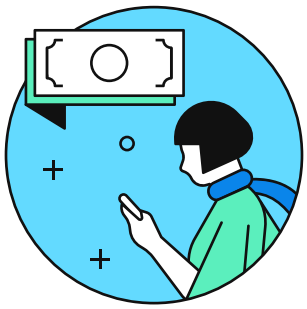
Though widely different products, they share certain traits: they're personalized, they're built on a consumer's financial data, and none of them would have been possible 10 years ago.

In many cases, products built on consumer financial data can be offered to those who wouldn't be able to access them otherwise. The Consumer Financial Protection Bureau (CFPB) recently announced that Upstart's underwriting model, which draws on consumer banking data, approves 27% more applicants than the traditional model and yields 16% lower average APRs for approved loans. In addition, Upstart's model has yielded the following results:

- "Near prime" consumers with FICO scores from 620 to 660 are approved approximately twice as frequently
- Applicants under 25 years of age are 32% more likely to be approved
- Consumers with incomes under $50,000 are 13% more likely to be approved

At Plaid, we see first-hand how quickly consumer demand for services like these is growing. Over a quarter of Americans with bank accounts have used Plaid to connect their accounts to third-party apps and services, and that number is growing every day.

The consumer's right to access their data is essential to these services. Ensuring consumers have control over their data is necessary for their continued engagement with them, especially in the face of rising concerns around privacy and security.



1/4

1 in 4 users connect their accounts through Plaid.

Consumers' concerns about data practices weaken trust.

In a December 2018 nationally representative survey of 1,000 US adults, Plaid found that 61% of consumers reported concern over the privacy of their financial data.

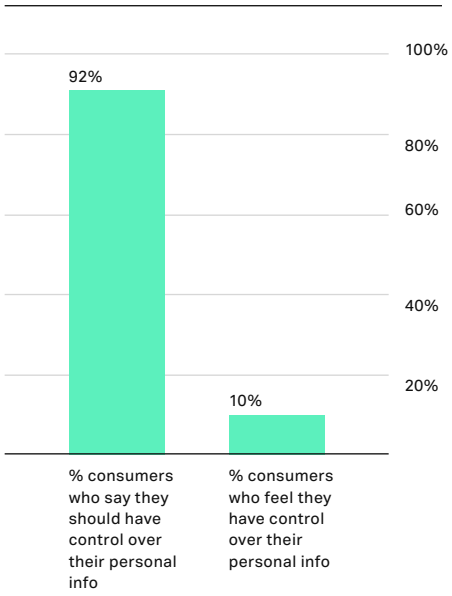
This sentiment aligns with broader consumer concerns around data handling. A 2018 Harris poll found that 78% of respondents identified a company's ability to maintain data privacy as extremely important, yet only 20% of respondents said they trust the organizations they interact with to actually provide that privacy and security.

An even wider gap exists when it comes to consumer control over their data: while 92% of consumers say they should be able to control what information is available about them on the internet, only 10% feel they have complete control over their personal information.[1] Despite this gap, only half of companies worth over $100 million say they are making significant investments in data governance, in creating transparency in the use and storage of data, and toward increasing the control individuals have over their data.[2]

Customer experience is essential to building trust in financial services, with 56% of respondents to a 2017 survey saying they trust fintech companies with which they had a positive experience, a significant spike from fintech's overall trust rating.[3]

With recent high-profile data breaches, it's understandable that the public feels a degree of mistrust when it comes to companies' data and information security practices. That several breaches happened at firms operating in either the finance or technology sectors places fintech at an especially scrutinized intersection. In order to build the trust needed to achieve scale, the fintech ecosystem needs to put consumers first when it comes to financial data.

CONSUMER CONTROL OVER DATA



[1] https://www.pwc.com/us/en/services/consulting/library/consumer-intelligence-series/cybersecurity-protect-me.html

[2] https://www.pwc.com/us/en/services/consulting/cybersecurity/digital-trust/2018-insights.html

[3] https://business.linkedin.com/marketing-solutions/blog/marketing-for-financial-services/2016/world-fintech-report-2017--the-battle-is-about-trust-not-tech

Consumers know what they want: control over their financial data.

The evidence is mounting: consumer control over their data facilitates greater trust in the financial services ecosystem.

But what does “control” mean? It’s more than the ability for consumers to switch off access. Increasingly, they want to make productive use of their data. In the Plaid survey, we found that a majority of American adults believe they should be able to control their data in the following ways:

With the push of a button, withdraw consent for a company to access my data

Share the rates and fees I am paying on a credit card or other financial product with competitors to see if I can get a better rate

Access my data, or give permission for anyone I choose to access my data, without paying a fee

When asked what actions companies should take to “enhance convenience and people’s control over their own data,” the three most commonly selected options were:

Ensure custom consumer control of what personal financial data third parties can access

Ensure transparency around what personal financial data third-party providers are given and what they are doing with it

Allow consumers to revoke their previous authorizations to let a third party access their financial data at any time

Past innovations have built trust by giving consumers control.

Consumers developed trust in other financial innovations as measures were put in place to ensure elements of control and transparency.

Consumers swipe their cards and make online purchases multiple times per day. In each case, they put sensitive financial data (card number, expiration date, CVC) into the hands of others with confidence that it won't be misused. Thanks to a mix of regulatory provisions, product innovations, and transparency measures, consumers feel empowered to trust these transactions. We can take lessons from these earlier periods of innovation:

- The advent of the ATM
- The rise of ecommerce

THE ADVENT OF THE ATM

ATMs have become a staple of the financial landscape – but initially, adoption was slow.

First introduced in the 1960s, the ATM was part of a larger trend toward self-service. According to one origin story, the creator of the ATM wondered why he couldn't get cash from a vending machine as easily as he got a candy bar.

In the past, people did their banking face-to-face. Convincing them to interact with a machine required creativity and tender steering on the part of the ATM's designer, as well as nimble oversight by regulators to balance new security and access tradeoffs.

Many of those trust-building features still persist today. They include:

- Printed receipts for every transaction
- Personal Identification Numbers (PINs) set by consumers
- Clear customer service options to resolve disputes in cases of theft or security issues

THE RISE OF ECOMMERCE

The origins of modern ecommerce date to the late 1990s, with the emergence of companies like Amazon and eBay.

These companies faced challenges similar to those encountered by the early ATM. Consumers would need to feel comfortable conducting their purchases online and abandoning an in-person interaction for a digital one.

In this new world, consumers would no longer be able to touch a product before they purchased it or rely on their relationships with store employees. And yet ecommerce sales in the United States have grown to more than $500 billion annually. What happened?

Much like ATM designers, ecommerce companies increased transparency, gave consumers more control, and reduced risk. In so doing, they enabled the convenience of online purchases to overcome the initial trust gap. Their innovations include:

- Low-cost or free returns in case of product deficiencies
- Excellent consumer experience
- Transparent third-party reviews
- Trust seals and certifications from respected third parties
- Dispute resolution through a variety of user-friendly means, including responsive communication via phone, email, social media, and chat

Four principles for building trust with consumers by giving greater control over their financial data.

As we've seen, consumers want the innovative services data sharing enables, but are concerned about the privacy and security of their financial data. We propose the following four principles that will give consumers the control they want and drive trust in an interconnected financial system.

Understanding	Consumers should understand how their data is being used. • Consumers should have the ability to know what data is being shared and with whom. • Data practices should be clearly disclosed and easy to understand. • Consumers should get information when they need it for a decision, and the information should empower that decision.
Choice	Consumers should be given controls that let them make meaningful choices about whether, how, and with whom their data is shared. • For example, they might un-link an app or bank account they had previously connected. • Those controls should be available to consumers in a consistent and accessible format. • When consumers take actions, such as unlinking an app, those actions should be effective immediately across the entire data chain.
Neutrality	When consumers share data across multiple accounts and apps, controls should be enabled on a data management platform that stays neutral. • Consumers should have control tools at their bank, app, or other data source to manage their connections. • As consumers connect multiple accounts and apps, they should be given the option of a platform approach that enables them to see and control all their accounts in one place. • Such a platform must be agnostic to where consumers choose to hold their financial accounts, and work with the control tools at banks and fintechs.
Protection	Consumers should have their problems addressed by the company they go to with a problem, and shouldn't have to go to multiple companies to figure out who is "responsible" if something goes wrong. • Companies should promptly notify users when their data has been breached and provide clear directions for remedy. • Consumer protection regulations should be updated to account for–and protect–how consumers use their financial data today.

Unlock innovation with consumer control

We've seen time and time again that when consumers are in control, they are more likely to trust the experience and reap the rewards from doing so. Plaid is committed to these principles as we continue to build a platform to support consumers who want to use their financial data to live healthier financial lives. By aligning to a framework that prioritizes the consumer's control over their financial data, the digital financial services ecosystem can ensure the broadest set of consumers will benefit from innovations that make money easier for everyone.

About Plaid

Plaid is a technology platform and data network that enables applications to connect with users' financial accounts. We focus on lowering the barriers to entry in financial services by making it easier and safer to use financial data.

plaid.com

growth@plaid.com

PLAID HEADQUARTERS
1098 HARRISON ST.
SAN FRANCISCO, CA 94103