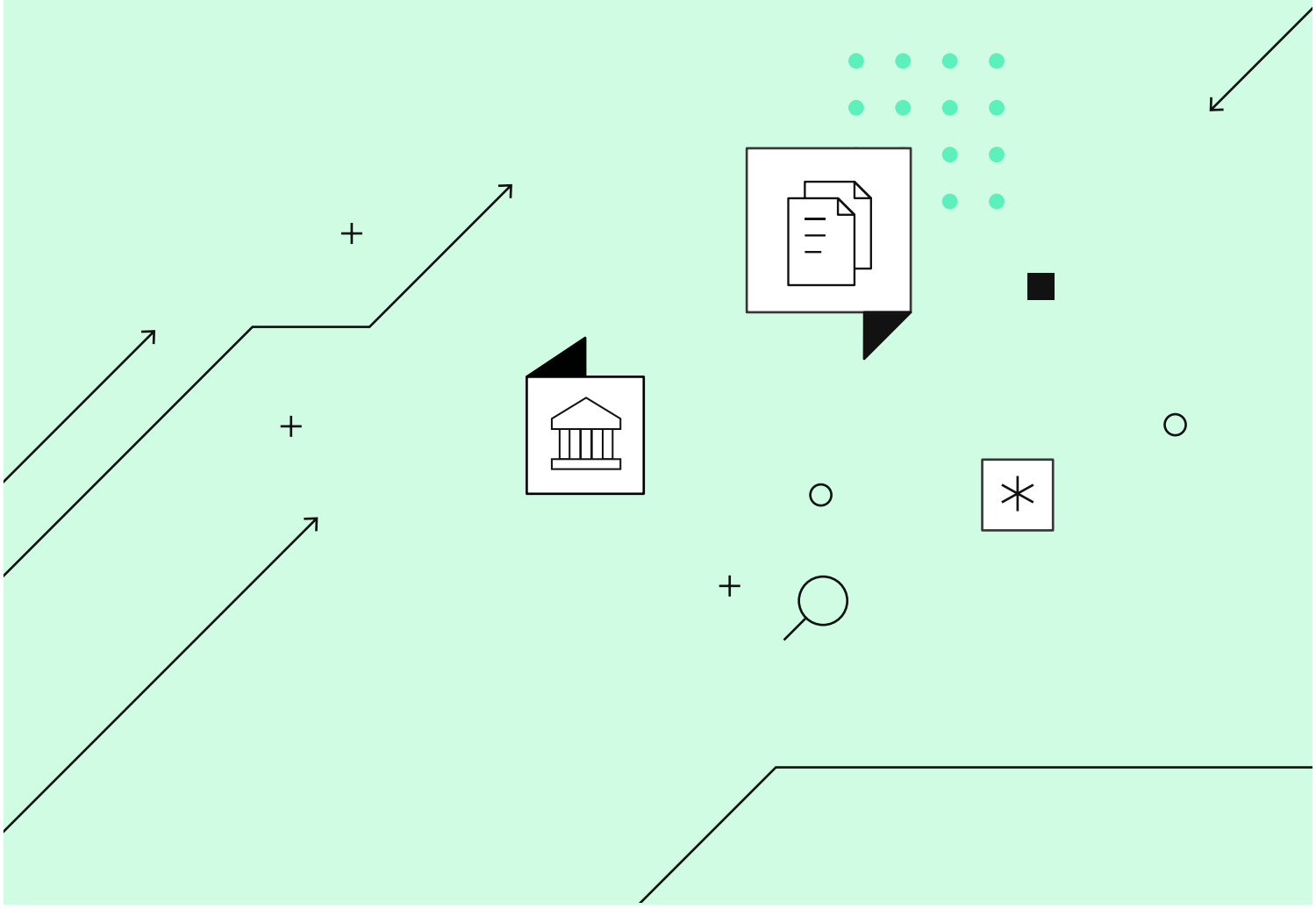
PLAID

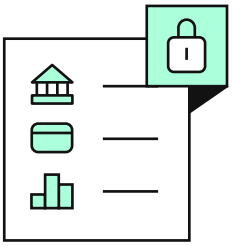
plaid.co.uk

Plaid's response to the FCA's CP21/3



Executive Summary

This document is Plaid's response to FCA's CP21/3 Changes to the SCA-RTS and to the guidance in 'Payment Services and Electronic Money - Our Approach' and the Perimeter Guidance Manual.



Plaid Financial Ltd. (Plaid) is an authorised payment institution regulated by the Financial Conduct Authority under the Payment Services Regulations (PSRs) 2017 (Firm Registration Number: 804718) for the provision of payment services. Plaid builds technical API infrastructure that connects consumers, financial institutions, and fintech developers - giving consumers greater control over their financial data. By enabling fintechs and developers to build creative PSRs-compliant solutions on top of open banking infrastructure, Plaid is focused on ensuring the success of the goals underpinning open banking and the PSRs. Plaid is looking to build on its experience of creating digital financial infrastructure to deliver best in class API experiences and data security for our clients and their consumers.

Founded in 2012, we currently connect 4,500+ apps and services to 11,000+ financial institutions in the UK, Europe, US and Canada. Plaid APIs are being leveraged across various fintech verticals, from personal finance and lending to brokerage and consumer payments. As a result of our global footprint, we have experienced open finance initiatives across the UK, Europe, Canada, and the US, giving us an understanding of the potential barriers and opportunities in different markets. We are working with our clients to leverage open banking while also looking to develop new use cases under open finance.

Plaid is committed to providing the best open banking consumer experience and welcomes the consultation on the 90-day re-authentication requirement. To truly improve the UK's adoption of open banking and maintain the UK's leading status in open banking infrastructure, allowing third party providers (TPPs) to own their full relationship with their customers, including their re-consent journey, is imperative.

But we cannot leave it at just that– the industry needs more guidance on how to collect consumers re-consent. We have proposed two models in our response below. The FCA and TPPs should work together to ensure the re-consent journey meets the needs of consumers and supports the wider development of the open banking ecosystem.

Below is our response to the consultation. We have also provided some drafting suggestions for the Approach Document and draft legal instruments. We would be delighted to support the FCA in any way we can as you finalise the rules on these changes. We would be happy to have a more detailed discussion on our proposals in response to question 1 on 90-day reauthentication.

Annex 1: Detailed response to CP21/3 questions

> *Q1: Do you agree with our proposal to create a new SCA exemption for when customers access customer information through a TPP and add a new requirement for TPPs to check customers' consent every 90 days? If not, please explain why.*

We strongly agree with the FCA's proposals. Plaid firmly believes that the responsibility for carrying out re-consent every 90 days should lie with the TPP that is accessing payment account data with the consumer's explicit consent.

That being said, we suggest the FCA provide guidance on their expectation for TPPs to meet the new requirement. We note paragraph 17.77 of the draft FCA Approach Document provides some guidance. However, it does not provide guidance on how an AISP should collect the PSUs consent every 90 days.

In the absence of this guidance, we have developed two proposals we would like the FCA to consider:

1. Plaid Portal (preferred)
2. Plaid Link (sufficient, but not preferred)

Please note these are how Plaid could meet the new obligations, but other TPPs can choose their own methods to easily replicate these approaches. We would be happy to discuss these proposals in more detail with you. We have also provided screenshots of the Plaid Portal customer experience.

Proposal 1 - Plaid Portal

Current regulations were drafted in a manner that makes it impossible for consumers to reauthentication with all their ASPSPs and TPPs in one smooth journey. Instead the regulations are based on an assumption that consumers have one bank account connected to one TPP and that the relationship is linear and seperate. In practice this means that consumers have to reauthenticate with every single ASPSP in order to benefit from open banking. Consumers with multiple bank accounts have to spend more time reauthenticating all their accounts. In addition, because each account is viewed as separate and linear, the timing of reauthentication does not always sync, and consumers with multiple bank accounts could have to reauthenticate several times throughout the week when they reach the 90 day limit.

Thus the linear regulatory framework for the consumer-TPP relationship negatively impacts consumers and the wider open finance ecosystem.

As the open banking ecosystem continues to grow and consumers increasingly rely on TPPs for their everyday banking needs, this linear approach will only cause more undue friction. It may even limit the growth of open banking and create a disincentive for consumers to connect with additional TPPs.

The solution to this is taking a network approach, where consumers manage their consents across the ecosystem in one place. As seen in Annex 3 below, Plaid Portal is a one-stop-shop where consumers can view and manage the TPPs and payment accounts accessible via open banking.

We are of the view that this portal is the best way to provide consumers with a clear list of:

1 TPPs that have access to their payment account data,

2 the payment accounts they have connected and

3 the transaction data collected by the TPP.

Plaid Portal increases transparency and gives consumers more control over their data, ultimately earning their trust and comfort to use their data to select more individually tailored products and services. Also, it can provide functionality for a consumer to revoke consent if they no longer want their data to be shared.

From a re-consent perspective, Plaid Portal would enable consumers to review and actively decide if they want to re-consent or if they want to revoke their consent and have their data deleted (as per GDPR). At its core, the purpose of 90-day “reauthentication” is to ensure that consumers actively re-engage with the TPP and continue to consent to the use of their data. Put simply, Plaid Portal does that but in a more secure and consumer-focused platform.

As the regulated entity acting as the middleman between our clients (registered agents, TPPs etc.) and the PSUs ASPSP, we can see all the accounts and TPPs using the PSUs data and push the PSU through a one-time re-consent journey. In addition we can monitor the amount of time left until they need to re-consent and when an account does not match the others we can still push the consumer to re-consent and make sure it aligns with the others, cutting down the time needed for future re-consent journeys. It does not make sense for every TPP to build out a portal type functionality as such the entity regulated and actively obtaining the consumers explicit consent should be the responsible party for providing a network view to the PSU.

We would be happy to give you a live demonstration, in addition, please refer to Annex 3 for the full customer journey.

To enable the full suit of benefits for a portal type solution, TPPs will require stable IDs (in the form of an institution-unique user ID)[1] from ASPSPs. This will allow TPPs such as Plaid to identify which accounts are owned by the same PSU for re-consent purposes. It will also allow for a better and more personalised consumer experience[2]. ASPSPs already collect this data, all they would need to do is allow TPPs to access it the same way they allow TPPs to access account holders' full name.

We believe Plaid Portal, enriched with stable IDs, would provide the best in class customer experience, promote data transparency and grow and develop with the broader "open" ecosystem.

Proposal 2 - Plaid Link

Plaid Link is very similar to the current reauthentication journey consumers go through. Every 90 days, we would send our client a notification to tell them they need to get their consumers to re-consent. To provide that re-consent, we would push clients to Plaid Link.

This proposal will comply with the new regulatory requirements, and would provide a better consumer focused customer journey that the current ASPSP reconsent. However, it doesn't help solve the issue of consumers who have more than one payment account connected to more than one TPP. Unlike Plaid Portal, Link would still require consumers to re-consent with each application one by one every 90 days. As discussed above, this can be highly burdensome and is the leading cause of the high consumer attrition rates faced by TPPs at the moment.

To truly improve the adoption of open banking in the UK and maintain the UK's leading status in open banking infrastructure, we believe that allowing TPPs to own the re-consent journey is essential. By building functionality for stable IDs in the open banking ecosystem, TPPs, such as Plaid, will provide consumers with a seamless re-consent experience, thereby increasing confidence, trust and transparency in open banking-enabled products and services.

Given the two options discussed above, we would recommend the FCA provide guidance via the Approach Document that states for a direct (linear) relationship a solution like Plaid Link is acceptable while if the relationship is indirect a solution like Plaid Portal is acceptable.

[1] Example stable IDs include email address, mobile number and full name. Full name alone is not enough to tie specific accounts to the correct consumer, especially in the event of commonly used names (i.e. John Smith).

[2] Without stable IDs portal type solutions can still work but it is significantly harder to accurately trace accounts linked to each PSU.

> *Q2: Do you agree with our proposal to mandate the use of dedicated interfaces for TPP access to retail and SME customers' payment accounts and with our proposed timeline for doing so? If not, please explain why.*

We support mandating dedicated interfaces for TPP access. However, we do not support giving firms 18 months to do so.

The requirement for a firm to implement a dedicated or modified customer interface has been in place since January 2018. To meet the requirement, initiatives like the Open Banking Implementation Entity have developed standards for firms implementing a dedicated interface that makes it faster and easier. In addition, technical service providers can partner with firms to provide them with an "off the shelf" dedicated interface that meets regulatory requirements, such as token.io.

With these additional resources, we believe firms do not need 18 months and *would suggest the FCA give firms six months from the publication of the FCA's response to this consultation with the option for a possible extension.* In addition, we suggest the FCA requires these firms to provide a timeline, information and FAQs via the Open Banking Transparency Calendar.

Finally, to ensure compliance and delivery, we would ask that the FCA Supervision team monitors the development of these dedicated interfaces and, if required, takes supervisory action against firms that do not meet the implementation deadline.

> *Q3: Do you agree with our proposals to only require ASPSPs to make the technical specifications and a testing facility available at market launch of the interface and to delay the need for a fallback interface for six months from the point of launch? If not, please explain why*

We disagree with your proposals. Technical specifications and testing facilities allow TPPs to build and test connections with the dedicated interface before a market-wide launch. Without this testing time, TPPs run the risk of not supporting consumers who have payment accounts with these ASPSPs, which could negatively affect the TPPs ability to compete. Additionally, this could affect the reliability and performance of the ASPSP's API. When a TPP is testing an API, it must provide feedback and raise issues directly with the ASPSP. This helps ensure the API is robust and can withstand traffic. As such, we would suggest ASPSPs be required to provide a testing facility for TPPs two months before the interface's market launch.

On average, after testing, it takes two engineers approximately ten days to integrate with an ASPSP's API, but this timeline can vary if the ASPSP's interface is not based on industry standards (i.e. Open Banking). *We would suggest that ASPSPs be required to provide a testing facility for TPPs two months before the interface's market launch.*

> *Q4: Do you agree with our proposal to treat exemptions from setting up the contingency mechanism fallback interface granted by home state competent authorities, to ASPSPs with temporary authorisation, as though they were granted by the FCA? If not, please explain why.*

We disagree with your proposal. Based on our experience in Europe, some jurisdictions' ASPSPs have been granted exemptions from building contingency mechanisms when their dedicated interfaces do not meet the EBA guidelines' required standards. This has negative impacts for Registered Account Information Service Providers (RAISPs) and Authorised Payment Institutions who rely on the dedicated interface's stability to provide their services to consumers. In addition, the FCA, when granting exemptions, made policy decisions that other jurisdictions did not follow. One example is the requirement for App-2-App redirection. The FCA decided to require firms who provided access for consumers via a mobile app to implement app-2-app redirection. By making this decision, the FCA ensured the best possible customer journey, ultimately helping TPPs as more customers use their services.

If the FCA were to grandfather in exemptions from other jurisdictions, policy decisions like app-2-app will not be the same. *As such, we would suggest the FCA conducts a light-touch review of the firms who received exemptions from other jurisdictions, cross-checking and confirming that these firms provide the required functionality other FCA exempted firms offer (i.e. app-to-app redirection).*

We would also ask the FCA to require all firms who have received or are looking to receive an exemption to update the Open Banking Transparency Calendar with the correct information.

> *Q5: Do you agree with our proposed amendment to increase the cumulative threshold of the contactless exemption from £130 to £200? If not, please explain why?*

N/A.

Q6: What is your view on increasing the current regulatory contactless (single) threshold limit of £45 to £100 (or potentially a maximum of £120)Please explain your rationale, including supporting data and new threshold where applicable. If your response identifies potential risks and benefits, please provide evidence in support of your response.

N/A.

Q7: Do you agree with the proposed changes to SCA? If not, please explain why.

- **Dynamic Linking -** We support adding this clarification, especially in light of this helping develop variable recurring payment and standing orders.
- **Liability for fraudulent or unauthorised transactions -** We support adding guidance in the Approach Document to clarify the firms' requirements.
- **SCA Element -** We support adding guidance in the Approach Document to make the requirements for firms clear.
- **Transaction Risk Analysis -** We support adding guidance in the Approach Document to make firms' requirements clear.
- **Corporate Exemption -** We support adding guidance in the Approach Document to make the requirements for firms clear.
- **Authentication Code -** We support adding guidance in the Approach Document to make the requirements for firms clear.
- **Merchant Initiated Transactions -** We support adding guidance in the Approach Document to make firms' requirements clear.

Q8: Do you agree with our proposal to incorporate our temporary guidance in our AD to make the guidance permanent? If not, please explain why.

- **Safeguarding -** Not applicable for Plaid.
- **Prudential risks management -** Not applicable for Plaid.
- **Wind-down plans -** We support adding guidance in the Approach Document to make the requirements for firms clear.

Q9: Do you agree with our proposal to consolidate in our AD, our guidance on safeguarding insurance as set out in our letter of December 2019 to firms' compliance officers and that we also apply that guidance to the guarantee method of safeguarding? If not, please explain why.

N/A.

Q10: Do you agree with the proposed changes to the sections in chapter 6? If not, please explain why.

1. **BCOBS -** We are supportive of the extension of BCOBS to include payment and e-money providers.
2. **Exclusion from the PSRs and EMRs -** Not applicable for Plaid as we do not use the ECE or LNE exclusions.
3. **Reporting Requirements -** Not applicable for Plaid as we are not an EMI.
4. **Information Sharing -** We support the FCA clarifying that ASPSPs must share the account holder's name, sort code, and account number with PISPs if the name is shown to the customer in their online account.

   As discussed in our response to question 1, to ensure Plaid Portal works, we require ASPSPs to *provide a static ID on the consumer such as an email address, telephone number or registered postal address.*
5. **eIDAS -** We provided comments to CP20/18. We remain supportive of this change and support adding this clarification to the Approach Document.

> *Q11: Do you agree with proposed Brexit-related changes to our AD? If not, please explain why.*

We are supportive of the Brexit-related changes made to the AD.

> *Q12: Do you agree with our proposed changes to PERG on the scope of the LNE and ECE? If not, please explain why.*

N/A.

Annex 2: Drafting suggestions for the Approach Document and Draft Legal Instruments

To ensure maximum understanding by industry participants, we have suggested some changes to the Draft Approach Document. These suggestions are based on our understanding of the requirements, guidelines and regulations:

Chapter 5 Appointment of agents and use of distributors

5.6 RAISPs and APIs ~~PISPs~~ are responsible for the services (an) agent(s) provides on their behalf and must have the correct level of professional indemnity insurance to cover services provided directly as well as those provided through agents.

5.7 The agreement to provide AIS (or PIS) is between the RAISP or API ~~regulated or authorised AISP/PISP~~ and the consumer. ~~and~~ The agreement should make clear that the agent is providing AIS or PIS on the RAISP's or API's ~~AISP's or PISP's~~ behalf. In addition, the RAISP or API must get explicit consent from the consumer to access their accounts to provide AIS.

5.8 The role of an agent is different to the role of a third party. A~~n~~ RAISP or API ~~authorised/registered AIS/PIS~~ may pass payment account information on to a (different) third party for that third party to use to provide a (different) service to the consumer ~~customers~~ (subject to the RAISP/API obtaining the consumers explicit consent ~~customer's agreement~~), such as credit scoring or loan applications. The third party does not need to be authorised or registered as a RAISP or API ~~/AISP or PISP~~ as it is not ~~performing either~~ providing a regulated ~~activity~~ service under the PSRs 2017 or EMRs.

5.9 The role of an agent is also different to the role of a 'technical service provider' (TSP) that supports ~~an authorised or registered account information service provider~~ RAISP or API by using its technology to access relevant payment accounts on behalf of the RAISP or API.~~/AISP or PISP~~ A TSP does not provide the information to the consumer ~~user~~ itself and ~~there is no~~ does not have a direct relationship ~~between the TSP and~~ with the consumer. As set out in PERG 15 Q25A, when providing technical services for a RAISP or API~~/AISP or PISP~~, the TSP does not need to be registered or authorised as a~~n AISP/PISP~~ RAISP or API.

Chapter 17 Payment initiation, and account information and confirmation of availability of funds

17.11 PERG 15.3 provides further guidance on the activities that constitute AIS and PIS.

Chapter 20 Authentication

20.68 Where a PSP chooses...

~~20.69~~

20.70 Subject to the conditions set out...

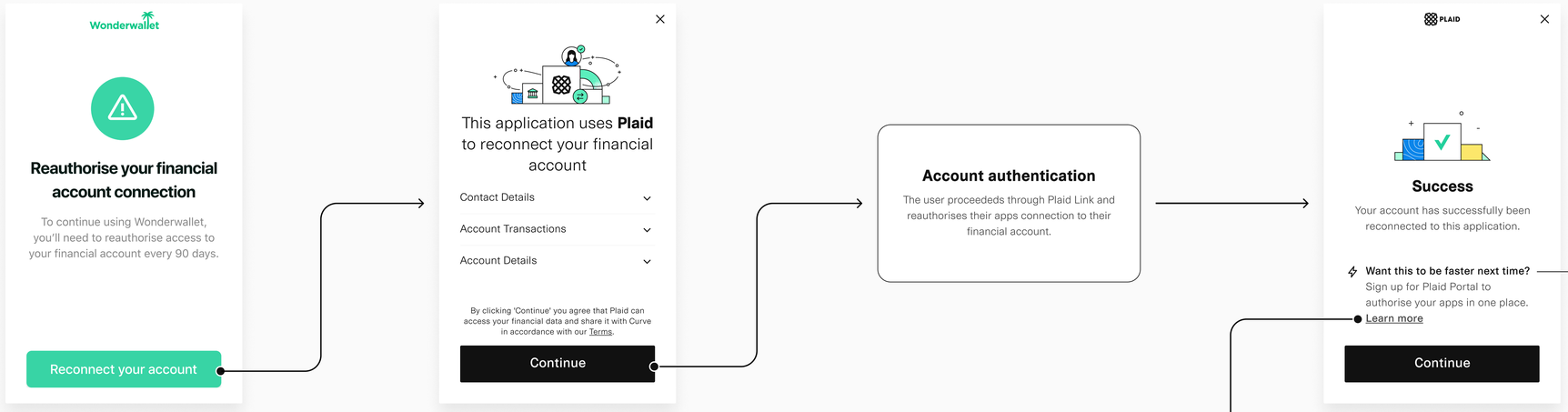
Amendments to the Technical Standards on strong customer authentication and common and secure methods of communication

Article 10A

2 Payment service providers shall be allowed not to apply strong customer authentication, subject to compliance with the requirements laid down in Article 2 and ~~to~~ paragraph 3 of this Article, where a payment service user is limited to accessing either or both of the following items without disclosure of sensitive payment data:

Annex 3: Plaid Portal

As discussed in response to question 1, please see below screenshots depicting what Plaid Portal will provide to consumers to meet the new Article 10A exemption.



Developer app & Plaid Link entrypoint

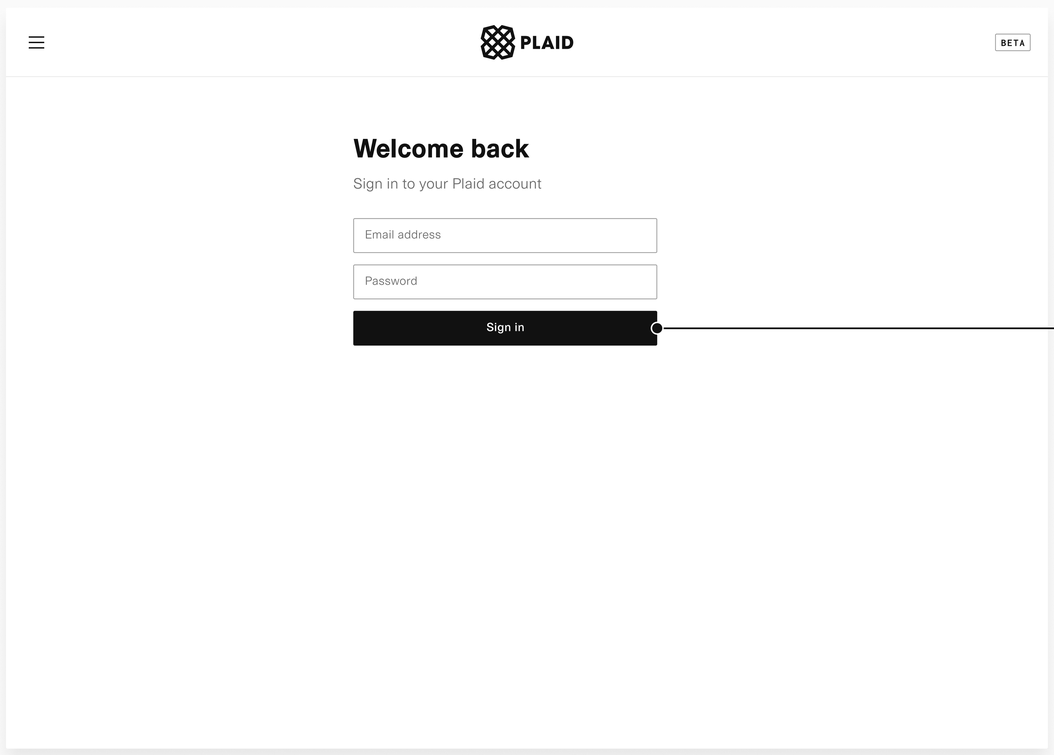
The user is prompted by the developer's app to reauthorise their financial account and given an entrypoint into Plaid Link to complete the authentication process.

Plaid Portal entrypoint & education

After successfully completing the reconnection process through Plaid Link, the user is informed that Plaid Portal is another way to reconnect their accounts — offering a more seamless process than linking each app by itself.

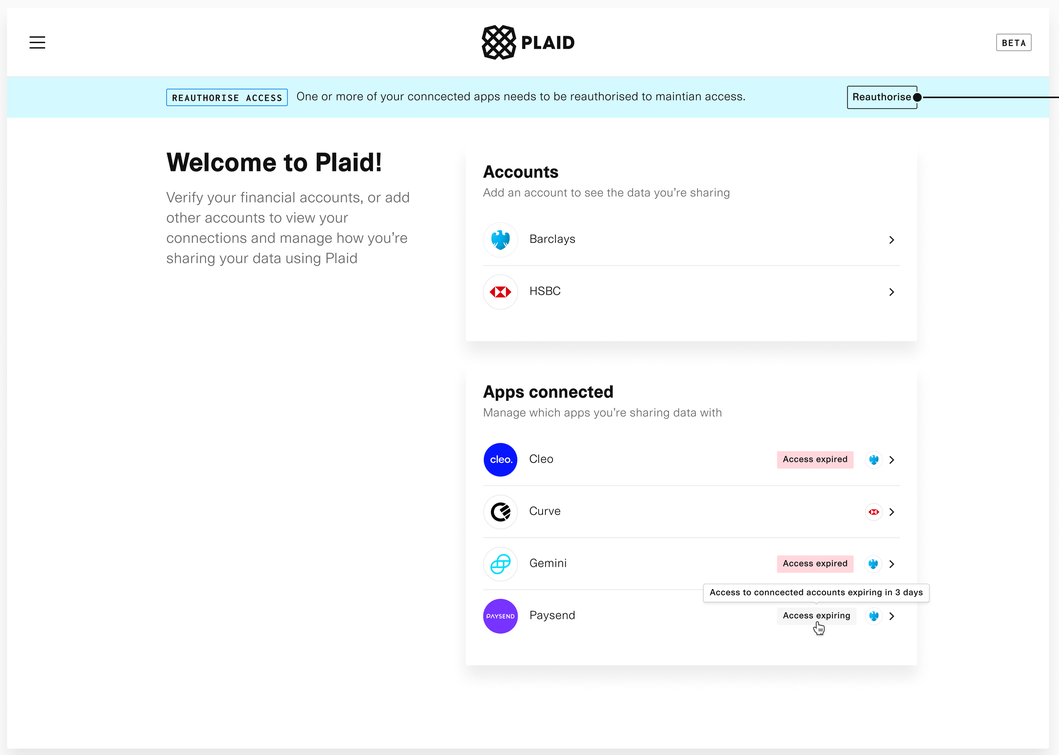
Plaid Portal sign up/sign in

After clicking the link, they are directed to Plaid Portal where they will either sign in or complete the onboarding process for new users.



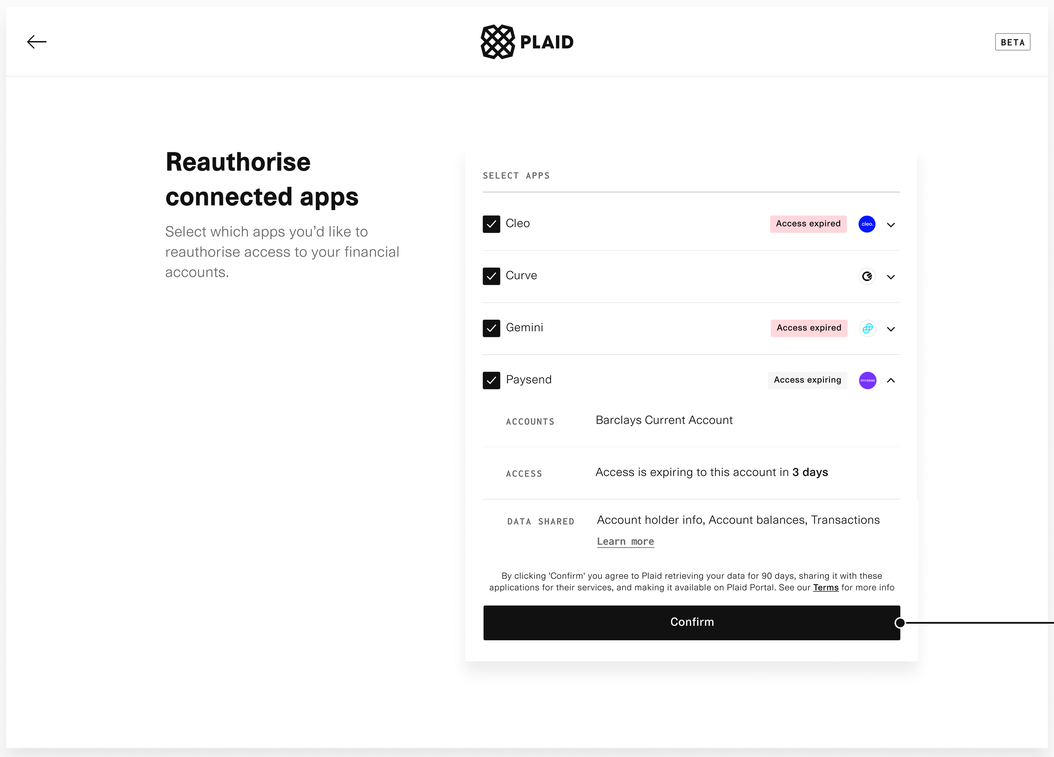
Plaid Portal login

Before reauthorising with Plaid Portal, the user must create an account and link their financial accounts.



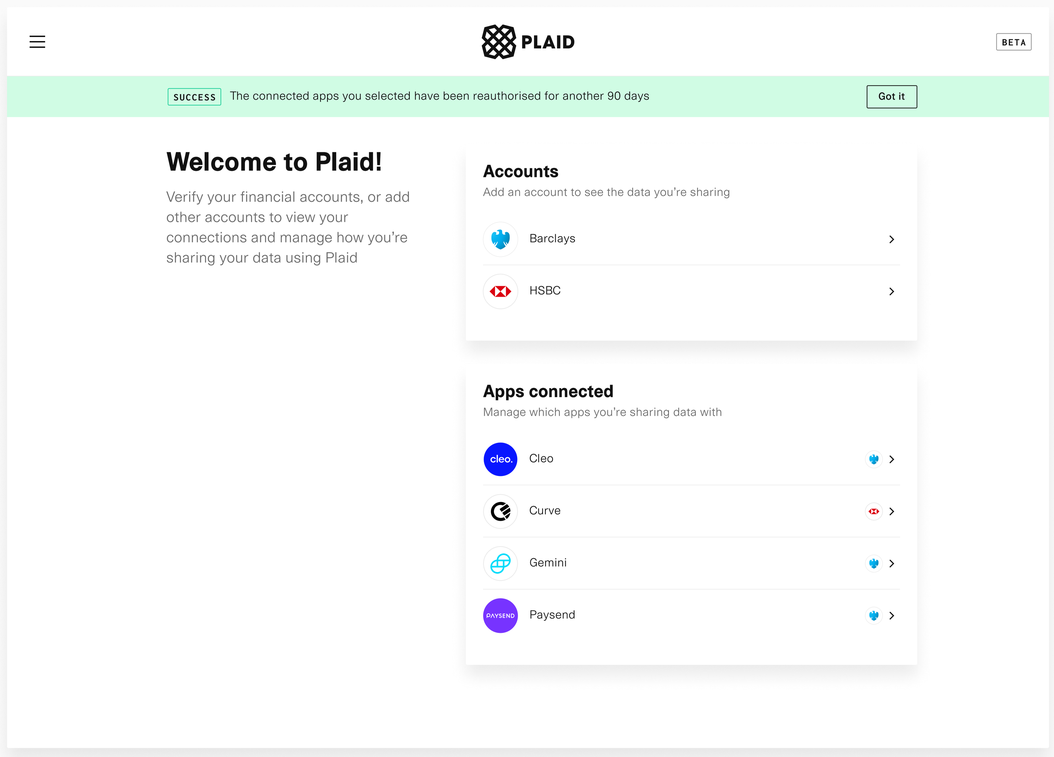
Plaid Portal home

For accounts linked to Portal, Plaid will show the matched apps conencted to those accounts and inform the user which need to be reauthorised.



Reauthorise connected apps

Before reauthorising their connected apps, the user is able to see additional information such as access status and the data they are sharing with the developer.



Process complete

After reauthorising, the user is informed of a successful reconnection and when they will need to complete the process again.

PLAID

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

plaid.co.uk

kcloud@plaid.com

PLAID HEADQUARTERS
1098 HARRISON ST.
SAN FRANCISCO, CA 94103

PLAID FINANCIAL LIMITED
31-45 FOLGATE STREET
LONDON
E1 6BX