# CGAP Guidance Note: Key Considerations When Developing Legal Terms and Conditions for Financial Services APIs

**January 2020**


# DISCLAIMER

This work was funded in whole or in part by CGAP. Unlike CGAP's official publications, it has not been peer reviewed or edited by CGAP. Any conclusions or viewpoints expressed are those of the authors, who are legal experts on the topic, and they may or may not reflect the views of CGAP staff.

This guidance note includes references to open banking frameworks that are available in different jurisdictions as examples of ways in which open banking can be approached, but neither Hogan Lovells nor CGAP endorses any particular approach. Any person referring to this note should not rely on any templates or examples without seeking assistance from their own counsel.

The recommendations made in this note are based on English law principles. However, this note does not constitute advice in any jurisdiction or territory. Any person referring to this note will need to validate that the options and recommendations work for the particular use case that is being applied and that they are supported by local laws and regulation.

**CONTENTS**

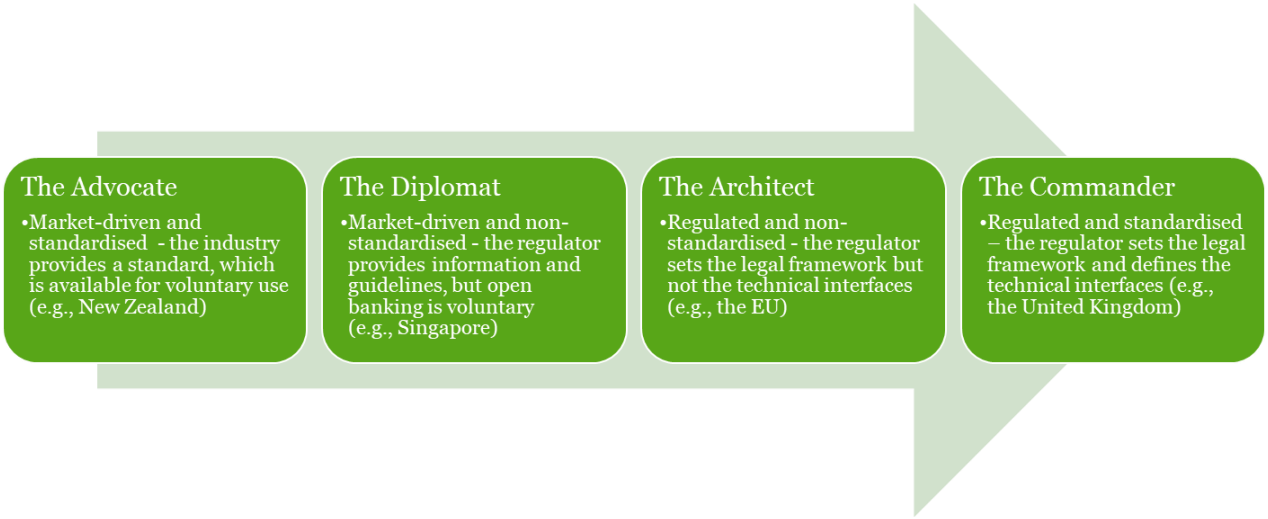
## INTRODUCTION TO THE GUIDANCE NOTE

### (A) Market context

CGAP[1] is working with several providers of digital financial services (**DFS Providers**) to understand how Open APIs (application programming interfaces) can enable nimble third party innovators to expand the range of useful financial, and other, services available to low-income customers, benefiting financial services providers, third party developers and end customers alike. Open APIs are a way of sharing a set amount of data with a large group of users. As explained in its paper titled '*Digital Rails - How Providers Can Unlock Innovation in DFS Ecosystems Through Open APIs*'[2], CGAP and its partners believe that open APIs enable third parties to use the digital "rails" of payment providers in a way that will benefit all stakeholders in digital financial services ecosystems and improve financial inclusion. CGAP has partnered with five DFS Providers in Africa and South East Asia to support the creation of open API demonstration cases, whilst learning along the way. Further information can be found at: https://www.cgap.org/topics/collections/open-apis

The payments landscape has completely changed in the past decade, and many jurisdictions are reviewing their regulatory approach towards payments to ensure that it serves the changing needs of customers and providers. The focus on regulation is happening against a backdrop of increased adoption of innovative technologies and expanding cooperation between regulators in different countries.

Regulators are increasingly looking at how retail payments markets can be opened up to improve services for consumers and small and medium-sized enterprises. Key motivators are to increase competition and encourage innovation, but also to enable consumers to control their own financial data and share it with other service providers, so that their needs can be better served. Some regulators are following the EU in mandating an open banking framework, while others are creating common standards to support the opening up of services in a way that ensures customer data is shared securely. In a number of countries, it is the industry itself, rather than a regulator, that is taking the lead. In its paper "*Regulating Open Banking*"[3], the Open Bank Project identifies four open banking regime models globally:




1 Consultative Group to Assist the Poor (CGAP), a global partnership of more than 30 leading development organisations that works to advance the lives of people through financial inclusion.

2 Olga Morawczynski, Lesley-Ann Vaughan, Michel Hanouch, and Xavier Faz (November 2016), '*Digital Rails - How Providers Can Unlock Innovation in DFS Ecosystems Through Open APIs*', CGAP.

3 Ismail Chaib (November 2018), '*Regulating Open Banking - How regulators around the world are shaping the future of financial services*', Open Bank Project.

Regulatory compulsion is not the only driver for using open APIs, however, and organisations are embracing them for commercial reasons, including the ability to commercialise their data and other resources, to reach a wider (or different) audience and to increase business.

## (B) Purpose of this note

Opening up data and services through open APIs has many benefits, but it does give rise to new challenges and considerations for DFS Providers.

CGAP engaged Hogan Lovells International LLP (**Hogan Lovells**) to produce this note to offer guidance to DFS Providers, in particular their legal teams, on the main risks involved in opening up access to their assets through APIs, and how to manage those risks in a way that is as fair as possible for all parties.

Hogan Lovells has experience of advising organisations on the use of open APIs in the UK and across the EU, where there are mandatory open banking frameworks in place, as well as in certain other markets that are moving towards open banking and/or increasing use of open APIs. These organisations include banks and other payment service providers, infrastructure providers, third party providers (including FinTechs) and industry bodies, including the UK Open Banking Implementation Entity. Hogan Lovells has also advised government bodies, including in Asia and Latin America, on the implementation of an open banking framework in their country.

The main function of this guidance note is to:

- highlight the key risks and legal issues arising for each of the API use cases supported by this note;
- consider how the risks could be managed through the DFS Provider's contract with the API consumer (**API Contract**), drawing attention to provisions that a DFS Provider might consider including in the API Contract. Where appropriate, the note outlines other options for mitigating or managing the risks.

In addition to this guidance note, CGAP intends to publish a set of template API terms and conditions (**API Template**) that could be used by any DFS Provider to manage the key risks associated with the implementation of a payments API or customer data API. For those DFS Providers that do not already have an API agreement, the intent is that the API Template will provide a simple reference set of terms that can help to reduce the cost in developing an agreement and save parties time by not having to start from scratch.

It is hoped that this note, and the API Template, will help give a head start to legal teams that may not have experience of advising on open APIs, by providing examples of the approach taken in other jurisdictions to open APIs and open banking models.

While this guidance note can be read in its entirety, we expect some DFS Providers might prefer to skip directly to the issues they are currently grappling with. We also expect the legal teams of DFS Providers to engage more fully with the note than business teams, who might be more interested in specific elements in the note. In that respect the table of contents above can be used to direct readers to the specific content of interest.

## (C) Scope

### Assumptions

The note is intended for DFS Providers that are making available their resources (services and/or data) to third party service providers through a dedicated interface, namely an API. The service provider is referred to in this note either as an '**API consumer**' or a '**TPSP**' (third party service provider).

The note refers throughout to the APIs of a DFS Provider; however, it is acknowledged that a DFS Provider may make available a Software Development Kit or SDK – rather than the API itself – to enable a third party to build applications that can access the DFS Provider's services. Our assumption is that any such SDK will include an API to enable communication.

### Use cases

This note has been produced for the financial services use cases listed below where the end customer is a consumer and any activity (e.g., payment initiation, data request) is initiated by an authenticated customer. It supports use cases where the TPSP requires access to assets of the DFS Provider, in order to provide its services to customers; it does not support the provision of services by a TPSP to the DFS Provider.

(a) **Payments APIs:**

(i) Single immediate payments – a single payment is initiated and authorised by the customer in real-time.

(ii) Single future-dated payments – a single payment is initiated and authorised by the customer but payment will be made on a fixed date in the future.

(iii) Fixed recurring payments – this envisages a push payment mechanism, where the customer gives the TPSP a mandate to make payments to a defined payee at regular intervals (e.g., a subscription fee that is paid on the same date each month). This is in contrast to Direct Debit and other models in which the payee is given the authority to "pull" payment from the customer's account.

(iv) Variable recurring payments[4] – similar to the fixed recurring payment, but in this scenario the amount and frequency of payments will vary. This envisages TPSP services that allow the customer to manage his or her money, such as automated 'sweeping' functionality that moves monies between bank accounts to avoid overdraft charges or that rounds up a customer's retail payment and pays the difference into the customer's savings account. The TPSP initiates the payment based on a mandate within pre-defined parameters.

(b) **Customer Data API:**

The note supports APIs providing access to the customer's account balance and transaction history.

---

[4] In the EU, there are unresolved questions as to whether variable recurring payments are supported by the open banking legislation, and resulting challenges given that the Regulatory Technical Standards on Strong Customer Authentication appear to have been written on the assumption that payer-initiated transactions will always involve the payer, even where made via a payment initiation service provider.

**KYC APIs**

There is an increasing interest in using APIs to confirm identity, given the desire to streamline and speed up the process of onboarding customers and, where possible, to undertake the whole process electronically. API calls can be used to gather all of the information about an individual that is required to complete the onboarding process. APIs might enable access to raw customer data for 'know your customer' (**KYC**) or anti-money laundering (**AML**) checks or to carry out credit risk scoring, while others might provide the output of an analysis of customer data (e.g., KYC-as-a-service or credit scoring-as-a-service APIs).

Such API use cases are not in-scope for this note. However, section 5.5 outlines some general considerations for parties in relation to such APIs.

**(D) Reliance on a contract**

This note assumes that local law allows a contract to be put in place. This may not be the case in specific jurisdictions that have mandatory open banking regimes in place. In the EU, where a bank or any other payment account provider is required under PSD2 to give open access to payment accounts, it cannot compel the third party provider to enter into a contract for the in-scope data or services. This does not mean that the law prohibits a contract from being in place, only that the account provider cannot refuse open access if the third party will not sign up to its terms. We mention this as a number of territories that are seeking to implement rules around open banking have indicated that they are looking at the framework adopted by the EU, and a similar approach to ensuring open access may be followed.

It should be noted also that not all risk can be mitigated through a contract, and some risk can be more effectively mitigated through technical or operational measures. For example, if a third party does not need access to customer personal data in order to undertake an activity (e.g., testing the API), provide anonymised or fictional data - the contract could make the TPSP liable for any misuse or disclosure of personal data, but the risk could be removed completely by simply not providing access to personal data. Each DFS Provider needs to understand the risks presented by its particular use case and whether the treatment of those risks in this note is the best approach and/or supported by local law. In our experience, such a risk review is likely to need a local lawyer with experience across the legal and regulatory areas outlined in this note and someone within the commercial or technical team to explain the differences between the use cases that we have focussed on in this note and what the business is trying to achieve.

The parties should remember also that services may evolve over time and/or additional APIs may be added to the scope of the contract during its term. The DFS Provider will need to consider different risks that arise during the life of the contract and how those need to be managed.

**(E) Open banking in the EU**

The note draws heavily on Hogan Lovells' experience of advising businesses on their implementation of the mandatory open banking regimes in the UK and the EU, namely UK Open Banking and PSD2. There are frequent references to these regimes throughout this note, not least because a number of territories seeking to implement rules around open banking have indicated that they are looking at the frameworks adopted by the EU and the UK, and similar approaches to ensuring open access may be implemented.

**UK Open Banking – what is it?**

Open banking is a mandatory regime that has applied since 2018 to the nine largest providers of current accounts in the UK. The UK Competition and Markets Authority (**CMA**) mandated open banking on these nine banks and building societies (collectively referred to as the '**CMA 9**') after it investigated the UK's retail banking market and found, amongst other things, a lack of competition, innovation and customer engagement.

The CMA 9 are required to build standard open APIs that allow customers to share their data securely with authorised third parties. The regime sets out how an authorised third party can, with the customer's consent, access customer account data held by the bank or initiate payments from the account on the customer's behalf. The aim is to open up the retail banking market to third parties who can provide customers with other products and services (e.g. a service that aggregates all of a customer's account information in one place so that banking products can be compared). The regime is mandatory for the CMA 9 but voluntary for other market participants. Note that the CMA 9 are required to comply with Open Banking in addition to PSD2 (explained below), which applies across the EU.

The Open Banking Implementation Entity (**OBIE**) is the entity set up by the government to deliver open banking. It is overseen by the CMA with input from the CMA 9. The OBIE has created the API standards, which includes not only technical specifications, but also operational guidelines and customer experience guidelines[5].

**PSD2 – what is it?**

The Second Payment Services Directive[6], known as PSD2, is European legislation that brings fundamental changes to the payments market in the EU. It is intended to enhance competition and facilitate innovation by opening payment ecosystems and enabling customers to allow third party providers to access their financial data. At the same time, the legislation addresses the need to regulate the emergence of these third party providers in the market and ensure the protection of consumers, including formalising payment security requirements across the EU and ensuring that customers' financial data is shared in a secure way. It replaces the original Payment Services Directive (PSD1)[7], adopted by the EU in 2007, which first established an EU single market for payments to encourage the creation of safer, more innovative payment services.

PSD2 builds on the previous legislation by:

- enabling third party providers (payment initiation service providers and account information service providers, collectively "**TPPs**") to access customer account information, with the customer's consent, allowing third parties to develop their own payment and account services;
- mandating that strong customer authentication (explained further in section 4.2(a)) is applied by payment service providers when a customer is accessing an online account or carrying out remote electronic payment transactions (from September 2019[8]); and
- increasing customer rights (e.g., complaints handling and new rules on surcharging and currency conversion).

---

5 The Open Banking Standards can be found at: https://www.openbanking.org.uk/providers/standards/

6 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

7 Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC.

8 The implementation date is subject to an optional 'adjustment period' that can be introduced by individual regulators.

## KEY ISSUES

This section sets out the key issues identified for the in-scope APIs, how those could be addressed by the DFS Provider in the contract with the TPSP / API consumer and, where appropriate, other ways the risks could be addressed (e.g., through technical or operational steps).

### 1. PARTNER SELECTION AND ONBOARDING

#### 1.1 What is the risk?

A customer is entitled to assume that a DFS Provider will have carried out diligence on its partners before giving them access to his or her data. A DFS Provider's reputation could, by association, be negatively impacted by any failures of the TPSP. Further, if a DFS Provider shares customer data with unscrupulous third parties, it could be very difficult for the DFS Provider to argue that it has no responsibility for any resulting customer losses if it undertook little or no diligence on those parties.

If the DFS Provider is a regulated entity, it is likely to be subject to law and regulation that ensures (i) it has measures in place to secure its systems and to protect the integrity and confidentiality of customer data that it holds, and (ii) that it carries out a certain level of due diligence on any counterparty with whom it enters into arrangements, particularly an arrangement that will involve the sharing of customer data and/or providing access to the DFS Provider's systems.

#### 1.2 Due diligence and onboarding

We would expect every DFS Provider to have an onboarding process that looks at the suitability of the TPSP as a business partner and whether the TPSP meets the DFS Provider's criteria for ensuring the integrity of its systems and data, in order to judge the risk of partnering with the TPSP in the circumstances.

The onboarding process can vary widely between providers, as the level of diligence undertaken on TPSPs will depend on a number of factors. These include the provider's own risk appetite, internal processes, and the nature of the TPSP's activities. The risks posed will depend on what type of data is being shared and what the TPSP will be doing, but also the level of trust which the DFS Provider will be placing in the TPSP.

A common complaint by API consumers is how long the onboarding process can take. One of the challenges for a DFS Provider, particularly if it is a regulated organisation, is finding the balance between managing risk, meeting its legal and regulatory obligations, and having a process that does not put off potential partners. One way that DFS Providers seek to do this is by matching the level of due diligence to the level of API access required.

As an example, Starling Bank (which was the first digital, mobile-only, challenger bank in the UK) explains on its API developer site[9] that access to its data is grouped together into 'permissions', with each permission relating to one or more API endpoints / data elements. Starling outlines what type of functionality requires additional access and the process for upgrading to elevated permissions. It highlights to API consumers that certain permissions will require additional checks and therefore the API consumer should request the minimal access required for its application's functionality, which seems a pragmatic approach to take.

---

9 https://developer.starlingbank.com/get-started

Another difference in onboarding processes can be the stage at which a contract is entered into. While many providers will not sign a contract until any onboarding process has been successfully concluded, it is acknowledged that other parties may view contract signature as one step in completing the onboarding process.

There are likely to be two elements to any onboarding process: general checks on the partner and technical due diligence on the partner's solution. These are explained further in the following sections.

1.3 **General partner due diligence and risk checks**

(a) Due diligence checks will typically look at a number of aspects of the prospective partner, such as:

- its financial soundness (including whether the TPSP is able to meet the liabilities that could arise from the provision of their services and what insurance cover it holds) and its reputation;
- anti-money laundering and checking that the TPSP is not named on any financial crime sanctions list;
- if the TPSP holds all necessary permissions or authorisations (e.g., regulatory) for the activities which it intends to carry out;
- whether it is (or has been) subject to litigation or regulatory or government enforcement action;
- its security measures and controls, including its cybersecurity policy and what monitoring it has in place. A security breach at the TPSP could have serious consequences for the DFS Provider;
- its business continuity and disaster recovery plans; and
- the operation and security risk management controls that the TPSP has in place, particularly in relation to the protection of personal data (e.g., staff training in data privacy law and practices, data retention and destruction practices, data breach planning, measures in place to avoid excessive collection of personal data). A DFS Provider may also wish to check that these controls are reviewed regularly by the TPSP or third party auditors.

(b) Factors that may influence the scope and depth of due diligence that needs to be carried out on a TPSP include:

- whether the DFS Provider is a regulated entity - local law and regulation may dictate the nature and level of pre-contractual due diligence and risk assessment that the DFS Provider must carry out on the TPSP;

- the nature of the TPSP's services and how the TPSP intends to use any data received from the DFS Provider - for example, if the DFS Provider is disclosing publicly available or general product information via its API, this is low risk and minimal diligence may be needed. However, if the API is being used to submit payment instructions, there is a high reliance on the TPSP and liability risk if the instruction is incorrect or fraudulent. If the TPSP is providing payment services, a further factor will be the value and level of payment transactions that it expects to be handling;

- how long the TPSP has been operating in the market, and the quality of its products and services - if the TPSP is a new entrant, does the DFS Provider have confidence in the TPSP's capacity to deliver the services to scale, and that quality of their solutions will not adversely impact its reputation and the trust of its customers?;

- how and where the TPSP will be processing customer personal data and the purposes for which that data will be used - for example, if the TPSP intends to share customer data with third parties or will be pooling large volumes of customer data and using data analytics, DFS Providers may want greater comfort around the data measures that are in place to ensure that customers are protected;

- if the TPSP will be undertaking activities that are regulated in that market - if the TPSP is a regulated entity in its own right, that could streamline the due diligence process for the DFS Provider. Whilst is should not be relied on in and of itself, it potentially de-risks elements of the services, as a TPSP could be held to account directly by the local supervisory authority for any misuse of data and for any fraudulent or negligent activity in respect of the end customer. Similarly, in territories that have mandatory licensing regimes, parties can to some extent rely on that as a measure of the TPSPs suitability. By contrast, where the TPSP does not require any licence or permissions in order to undertake its activities, DFS Providers may have to carry out more in-depth diligence and/or impose more stringent obligations and liability provisions on the TPSP; and

- if the TPSP will be sending messages via a third party's system (e.g., if an outsourced service provider will be calling on the APIs on behalf of the TPSP).

**Practical tip**

A TPSP's business model may involve more than one service provider in delivering the services to the customer. A DFS Provider may not be comfortable with "chains" of third parties involved, particularly if the DFS Provider has no direct relationship with these parties and no control over where the customer data is being stored and used. Contractual protections include prohibiting the use by the TPSP of sub-contractors (which may not be possible given the TPSP's model) or permitting the use only of specific sub-contractors who have been approved in advance by the DFS Provider. With the latter approach, the DFS Provider should make the TPSP liable for any act or omission of its sub-contractors, and the TPSP will be responsible for flow-down of the obligations from the API Contract. There should also be a requirement for the TPSP to conduct diligence on the subcontractors that it uses. In addition, the DFS Provider may require that the TPSP's insurance cover extends to its sub-contractors (where such cover is available in the market).

## 1.4 Technical onboarding

It is considered good practice for DFS Providers to make available a sandbox or other test environment within which API consumers can test the responses of the API before moving to a live environment, and to require prospective partners to use the sandbox before being given live API access.

**EU approach to API testing**

In the EU, financial institutions that offer a payment account with online access (referred to as '**ASPSPs**') are required to provide a testing facility at least three months before their dedicated interface goes live. Their technical specifications must be provided at least six months before go-live. There is a sensible principle behind this, bearing in mind that one of the policy reasons behind the EU legislation was to improve competition in the payments market – the mandatory timescales are meant to ensure that third parties who wish to call on the ASPSPs services have sufficient time to develop and test their integration with the API or other dedicated interface.

The sandbox can be used by the DFS Provider to collect the technical information it needs from the TPSP and at the same time the TPSP can access API resources (including the technical specifications and any software development kits) and test the functionality of the APIs. As a minimum, the TPSP should be able to test the stability of the connection, its ability to identify itself, the ability to send and receive error messages, and the ability to carry out the services for which access is being provided. The sandbox may support live end-user authentication, albeit with test data, in order to run end-to-end testing of the customer journey. The onboarding process may require that certain test results must be achieved by the TPSP before it is allowed to access live data and services, including to demonstrate that there is a stable and secure connection and that the authentication process works as expected.

**Practical tip**

Even if the DFS Provider requires every TPSP to use the sandbox and test the interface, the API Contract should make clear that it is the TPSP's responsibility to integrate the API into its solution and to use the API correctly during the term of the contract. This means that whenever the DFS Provider publishes changes to the API specification, the TPSP is responsible for making any changes to its solution that are needed to ensure continued access.

### 1.5 Mandated access

It is important to bear in mind that local law or regulatory requirements may influence whether the DFS Provider **must** provide open access to particular third parties. In the EU, PSD2 requires an account provider (such as a bank) to provide access to all parties that are authorised as "PISPs" or registered as "AISPs" on a non-discriminatory basis and without carrying out due diligence. By contrast, in Hong Kong, third party service providers carrying out a regulated activity require a licence, but the HKMA's Open API Framework[10] will allow a bank to choose which service providers it will work with, based on the bank's own due diligence.

### 1.6 Approach in the API Contract

We would not expect the API Contract to set out the onboarding or due diligence process, as in many cases the signature of the API Contract will be one of the onboarding steps and the DFS Provider will not enter into the API Contract unless it has successfully concluded its diligence on the TPSP.

The successful completion of the onboarding process is one thing, but it is important also that the TPSP continues to meet the relevant criteria during the term of the relationship. Onboarding is just one aspect of supply chain management and governance.

In this respect, we would recommend that the API Contract:

(a) requires the TPSP to tell the DFS Provider if its circumstances change such that it no longer fulfils the eligibility criteria;

(b) requires the TPSP to promptly notify the DFS Provider if it has had a security breach regarding the information it has accessed;

(c) includes a warranty (i.e., a contractual promise) that the TPSP will have and maintain all legal or regulatory permissions or authorisations that are needed for the services which it is providing to customers; and

[10] Hong Kong Monetary Authority (July 2018), '*Open API Framework for the Hong Kong Banking Sector*'.

(d) gives the DFS Provider the right to suspend or terminate the API Contract if it has reason to believe the TPSP no longer fulfils the eligibility criteria (whether the DFS Provider learns of this from the TPSP or otherwise becomes aware). While we would not expect the API Contract to narrate the due diligence process, we would expect it to capture any key criteria or facts on which the DFS Provider based its decision to contract with the TPSP and that might impact its decision to continue doing business with that party (e.g., it becomes insolvent, loses any regulatory permissions, or becomes part of a competitor's business). Whether suspension or termination is appropriate will depend on the seriousness of the non-compliance and whether it is capable of being cured. For example, if there has been a lapse in any necessary authorisations or regulatory permissions that the TPSP must have to carry out its services, but it can reapply for these, the DFS Provider may be willing to suspend the contract until those have been procured.

## 2. WITHDRAWAL OF ACCESS FOLLOWING ONBOARDING

### 2.1 What is the risk?

Once a TPSP has been on-boarded and given access to the DFS Provider's APIs, there may be situations in which the DFS Provider needs to suspend or terminate that access or where the DFS Provider should not be compelled to action an instruction (e.g., where it has doubts about the authenticity of an instruction, or it has suspicions that the TPSP is misusing the APIs). The API Contract needs to deal with such situations.

It should be noted that if the DFS Provider is operating in any market where there is an open banking regime that requires the "forced opening" of certain bank data, such as with UK Open Banking or in the EU, there may be limitations on the circumstances in which the DFS Provider can withdraw access to that data.

### 2.2 Approach in the API Contract

The API Contract should set out the basis on which the TPSP is granted access to the DFS Provider's APIs and allow the DFS Provider to withdraw access in the event of misuse, in addition to recovering any losses arising from the TPSP's misuse of the APIs.

If the DFS Provider has concerns about a TPSP's possible misuse of the APIs, it may not wish to terminate the API Contract until it has validated those concerns (particularly if there is any risk of the TPSP arguing that the API Contract is being wrongfully terminated). Having the right to suspend access will give the DFS Provider time to investigate. We recommend that the API Contract sets out a process whereby the DFS Provider must notify the partner of the reasons for the suspension and give the TPSP a period in which to respond and remedy the situation (assuming the issue can be fixed). If the TPSP fails to do so, the DFS Provider then has the right to terminate the API Contract with immediate effect.

DFS Providers may want to consider the following list as a starting point for the circumstances in which the DFS Provider can suspend or terminate access to APIs:

(a) A right not to action an instruction, such as a payment instruction, where the DFS Provider has concerns about security or fraudulent transactions or use of the APIs (e.g., a number of unreasonable calls on the API or bombarding with messages).

(b) The right to terminate the API Contract in circumstances where:

(i) the TPSP no longer meets the eligibility criteria assessed as part of the onboarding process, or the TPSP is using the data or service in a manner that was not disclosed to the DFS Provider, or the DFS Provider changes the way in which it uses customer data;

(ii) the TPSP has become insolvent or a similar event has occurred in the relevant jurisdiction;

(iii) the TPSP introduces malware into, or otherwise disrupts or attempts to disrupt (e.g., tries to circumvent any security measures that have been applied) the DFS Provider's systems;

(iv) there is a change of control of the TPSP in favour of a competitor of the DFS Provider – whether this is a concern may depend on the nature of the DFS Provider's organisation and the market in which it operates; however, it is often cited as a concern for banks, who are worried about FinTechs being acquired by other banks who will have direct access to its customer base; or

(v) the TPSP offers its services or conducts itself in a manner that causes damage to the DFS Provider's reputation, either with customers using the TPSP's services or with the market more widely, which might include regulators – this would apply whether or not the TPSP has the right to use the DFS Provider's brand and logo within its service.

(c) The right to suspend access in circumstances where:

(i) the DFS Provider has the right to terminate the API Contract – depending on the event, it may be possible for the TPSP to remedy the situation and therefore the DFS Provider may choose to suspend rather than terminate;

(ii) the TPSP suffers a security breach or other unauthorised access to the systems through which the APIs are accessed or customers use the TPSP's services; or

(iii) the DFS Provider has a legitimate concern about the TPSP's access to or use of the APIs, or the DFS Provider is subject to a security incident (actual or suspected).

While the contract might be helpful after the event, there should also be checks and balances in place to help detect and prevent misuse. This could include internal monitoring by the DFS Provider of how APIs are being used, and taking action if any abnormal use is detected, as well as rejection of the API call if there are validation errors within the request.

**Practical tip**

In standard API contracts, it is common to see provisions that allow the API provider maximum flexibility to withdraw API access at any time and for any reason, particularly if the APIs are made available at no charge and the API provider is a bank or other regulated entity that wants maximum control in order to ensure compliance with law and regulation.

However, such a one-sided approach may not be palatable to service providers whose businesses depend on having access to the DFS Provider's data and/or services. A balanced position is one which sets out specific 'for cause' termination and suspension events, i.e., the TPSP knows the circumstances in which access can be withdrawn and there is a reason behind them, it is not simply at the DFS Provider's discretion. Such a position recognises that: (i) even if the DFS Provider is not charging for the APIs, a TPSP will have invested time and resource in ensuring that its software will interface with the APIs, including where the TPSP has developed its proposition using a DFS Provider's SDK, and (ii) the TPSP's business and services to the customer may depend on stable and continuous access to the services made available by the DFS Provider.

In addition to including suspension and termination rights, we recommend that the API Contract includes clauses dealing with:

- the consequences of such suspension or termination, including that the right to access the APIs or use the services accessible through the APIs fall away. The DFS Provider may also require the return or destruction of customer data that it has provided to the TPSP. However, depending on local law and regulation, and on the role of the TPSP, the TPSP may have rights to retain the data – or a copy of the data – for the purposes of its own compliance with law and regulation; and

- the reinstatement of services following a suspension. Each DFS Provider may have its own requirements depending on the event that gave rise to the suspension (e.g., in the event of a security breach, the DFS Provider may require to see evidence that any identified vulnerability has been adequately secured or patched).

## 3. ACCESS TO APIS – PRACTICAL CONSIDERATIONS

### 3.1 What is the risk?

In opening up payment accounts and account information to third parties, the greatest concerns for DFS Providers are the risk of fraud and the risk of customer data being misused or compromised.

### 3.2 User involvement

When a DFS Provider is allowing TPSPs access to its data or services via APIs, a key consideration is the extent to which TPSPs will be dependent on the active involvement of the customer in each instance of access.

DFS Providers should consider which approach to take:

(a) A TPSP can access data only when the customer is actively involved in the access process.

In this instance, it is assumed that the customer must input their security credentials to access the service, which means that the TPSP cannot carry out any activity without the customer being present. The benefit of this approach is that users have complete control over who has access to their data and when. However, the downside is that not all TPSP business models or use cases can support this approach, and users may lose out on all of the functionality offered by TPSPs. By way of example, it would mean that an account aggregator cannot carry out background refreshes of information and cannot actively provide users with updates, such as a warning that the customer is nearing their overdraft limit or any spending limit. Similarly, this approach could impact one-click payment models and automated "sweeping" functionality.

(b) A TPSP can access data independently without the customer being involved in the access process.

This approach supports a greater number of use cases. In the account aggregation space, TPSPs will want to background refresh on a regular basis - such activity is not directly initiated by the customer, although their authorisation to access account data will have been sought in advance. In respect of payment services, allowing the TPSP to operate on the basis of a variable recurring payment mandate would allow for TPSP applications that provide functionality such as variable subscription payments, 'one-click' e-commerce payments, and automated "sweeping" services.

To mitigate the risk of unauthorised access to account information or unauthorised transactions, such an approach should be based on the customer:

- being informed of the access in advance;
- giving explicit, ongoing consent to the access; and
- being able to revoke that consent.

If customers are informed in advance of the date and the amount of payment, it may not be necessary - but may be desirable - to notify the transaction after the event. DFS Providers should have regard to any information requirements in local laws or relevant payment scheme rules.

To give an example of how this has been implemented technically, UK Open Banking has adopted tokenisation as a way to provide secure, revocable and controlled access on an enduring basis.

If a DFS Provider does opt for the route of allowing independent access by the TPSP, it will need to consider what restrictions or controls should be placed on that access to counter the increased risk of fraud or error. It will depend on the nature of the TPSP's services what access controls are appropriate, but DFS Providers may want to consider controls such as:

- limits on transaction values, to minimise exposure to fraudulent transactions;

- limit how frequently a TPSP can access a customer's account without the customer actively requesting information. For example, under the PDS2 RTS (the regulatory technical standards that accompany PSD2), an AISP can only access information up to four times in any 24-hour period unless otherwise agreed with the account provider and with the customer's consent;

- limits on frequency and volume of unattended access. This is to minimise the risk that frequent automated calls on the APIs from multiple TPSPs will negatively impact the DFS Provider's systems and/or its ability to provide services directly to customers;

- for payments that are initiated by the TPSP, requiring that the customer is given advance notice of the amount, the customer is given confirmation that the payment was made and the TPSP is liable to refund the customer immediately if the amount is higher than was notified; and

- in respect of a variable recurring payment, the TPSP will be prohibited from changing any feature of a transaction that cannot be changed without going back to the payer / customer (e.g., changing the payee or payment dates).

Such operational controls will supplement any allocation of risk that is addressed in the API Contract, such as a requirement on the TPSP to indemnify or 'make whole' the DFS Provider for any losses resulting from the TPSP's fraud or error.

**Practical tip**

DFS Providers may want to have an area within their customer website or mobile app where customers can see which partners are accessing their data and have the option to stop the access, particularly where third parties have an on-going right to access data based on an advanced authorisation. TPSPs may also provide such a facility to customers, allowing a customer to see and manage in one place all of the consents given to that TPSP (e.g., all of the accounts which the TPSP is entitled to access on behalf of that customer). The customer should also be notified by the DFS Providers when a TPSP is added or removed.

A 'dashboard' approach such as this is becoming increasingly popular following the introduction of GDPR in the EU. GDPR is compelling businesses that provide services to EU consumers to be more transparent about how consumer data is used and who the data is shared with, as well as giving consumers more rights over how their data is used and by whom. In the context of open banking, giving the customer the ability to see such access, and to raise concerns or block access at his or her discretion, could be a non-contractual way to help to mitigate the risks inherent in continuous access.

## 3.3 Customer consent

To guard against the risks of fraud and unauthorised transactions, and to provide consumers with confidence, payment services should be carried out only with the consent of the customer. This is the principle underpinning the mandatory open banking systems in the UK and the EU, to ensure that the customer is in control of its money and who has access to its data.

In this context, 'consent' means the consent required to take any actions relevant to the provision of payment services, including initiating payments through the TPSP or allowing the TPSP to aggregate account data. Customer consent can also be an important element of accessing, processing and sharing personal data, but consent to carrying out payment services is not the same as consent to data processing (see section 5).

We recommend that the customer must provide consent before any payment can be initiated, and that any payment made otherwise than with consent will be an unauthorised payment. With this approach, parties will need to consider the following points.

(a) **What is the procedure for giving consent and how should consent be withdrawn?**

Consent could be provided directly to the DFS Provider or via the TPSP[11] and may be given:

(i) individually per transaction; or

(ii) as an ongoing consent subject to pre-determined parameters (e.g., the parameters that apply to a variable recurring payment).

Different channels and payment types may need their own form of consent and authorisation. For example: (i) consent to a single, real-time transaction can be given at the time the transaction is requested and linked with authentication, whereas a different procedure will be needed for variable recurring payments where the payment amounts will not be known at the time the customer gives authorisation for the future payments to be made; (ii) notice can be given to the consumer before variable payments are made so as to check that the consumer agrees with that payment.

Local law may have a bearing on how consent can or cannot be given. In the EU, PSD2 allows for consent to be provided by the payee (e.g., pull payments such as direct debits and card-based payments) or through the payment initiation service provider. This is to ensure that payments through such service providers and payments with cards can be carried out smoothly, and that the ASPSP does not need to check consent directly with the customer.

---

[11] This is a choice for the DFS Provider, who will need to weigh up the relative considerations of minimal friction (by relying on a consent given to the TPSP) vs trust and certainty (by requiring duplication of the consent directly to the DFS Provider).

(b) **What is the cut-off point beyond which a user can no longer withdraw consent, and what payment use cases does this apply to?**

Any cut-off point needs to be objective and independently verifiable, to give the customer and the TPSP certainty as to the point beyond which any payment cannot be cancelled. In PSD2, cancellation rights are limited to future dated payments, and the time limit is set at the end of the working day prior to the working day on which the payment is scheduled to be made. This is one approach that parties could follow, but will depend on the internal processes of the DFS Provider and any local law applicable to consumer protection and payments.

If there are payments that cannot be cancelled (e.g., payments for goods or services that are being provided immediately, such as immediate downloads and streaming services), the DFS Provider will want to make sure that the TPSP highlights these to the customer.

(c) **Collection of customer consent through a third party**

The expectation is that most DFS Providers will want to collect consent directly from the customer, to ensure that the consent has been freely given, properly collected, and not manipulated in any way. However, there are models where the consent is collected by the TPSP.

Unless supported by a mandatory legal framework, these models inherently carry additional risk, which a DFS Provider will want to mitigate in its API Contract. If the DFS Provider is willing to agree to customer consent being collected via the TPSP, then as a minimum the API Contract should set out that:

(i) the DFS Provider is entitled to rely on the TPSP having obtained the customer's consent and also has the right to request evidence of the consent, including where required in order to comply with law and regulation;

(ii) if the customer denies that it gave consent (or argues that it withdrew consent) and the TPSP cannot or will not provide evidence that it has properly collected the customer's consent, then the DFS Provider is entitled to assume that the necessary consent was not collected and that the action was unauthorised;

(iii) the TPSP is liable for any activities undertaken without the customer's consent, including accessing and using account data;

(iv) the TPSP must make customers aware of the form and procedure for giving and withdrawing consent before they sign up to the TPSP's services. The DFS Provider will want to ensure that this is drawn to the customer's attention;

(v) the TPSP is liable for any payment instructions sent or payments made after the customer withdraws consent if the TPSP has not communicated that withdrawal to the DFS Provider before the cut-off point; and

(vi) the DFS Provider is liable for any payments made after being told by the TPSP or the customer (before the cut-off point) that consent has been withdrawn.

## 4. AUTHENTICATING THE CUSTOMER

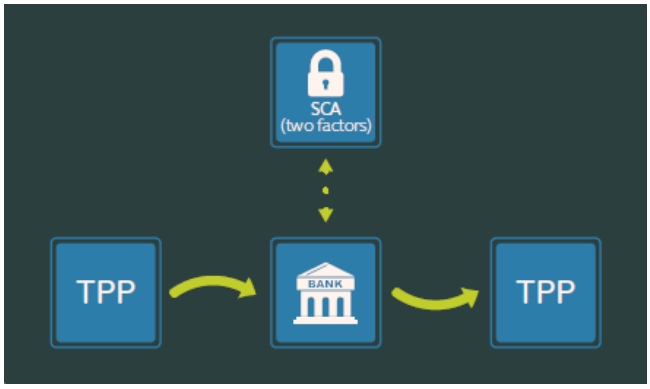
### 4.1 Method of authentication

The aim of customer authentication is to prevent fraud by ensuring that the person who is giving the instruction is actually the customer and that the payment instruction is valid. There are a number of ways in which the secure authentication of the customer can be achieved. Usually the option selected will involve balancing user-friendliness, security and the needs of TPSPs. The TPSP's ability to innovate and define and control the customer experience needs to be balanced against the DFS Provider's responsibility for the user authentication and ensuring that associated security and fraud risks are mitigated against.

There appear to be four main methods that are currently used for authenticating an end-user, as set out below (using the EU model in the illustrations, where 'SCA' refers to Strong Customer Authentication, explained further in section 4.2)[12]:

**A.** **Redirection**: This involves the user being redirected from the TPSP's domain to a domain provided by the DFS Provider (e.g., the DFS's Provider's application or website) for the purpose of carrying out customer authentication directly. The user does not need to disclose his or her security credentials to the TPSP and the DFS Provider has control over the authentication process and environment in which the authentication is carried out. With this model, consent to a transaction can be captured directly from the customer by the DFS Provider. From the TPSP's perspective, this approach impacts the user journey and means that the TPSP is dependent on the DFS Provider's implementation of the authentication interface. It should be noted that redirection has a specific dependency on the channel and device used by the TPSP, and therefore will not support all use cases.

*Example illustration - redirection method*

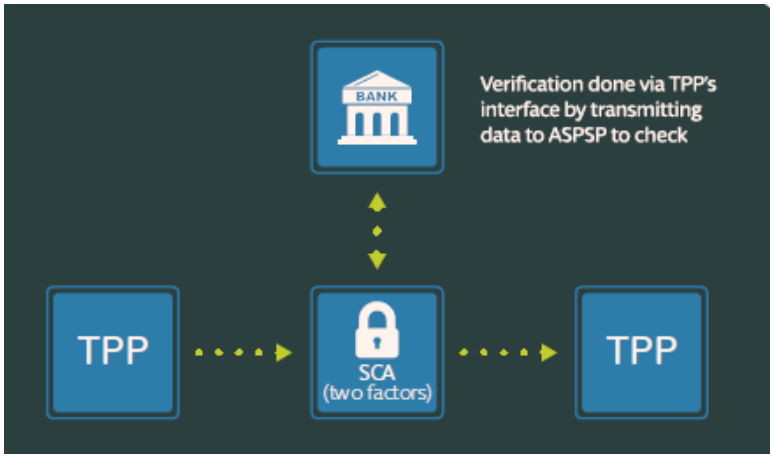



**B.** **Embedded**: In this model, the customer's security credentials are passed directly through to the DFS Provider's environment. As far as the customer is concerned, authentication takes place through the TPSP's interface, with no interruption to the communication session, but the authentication itself is performed in the background by the DFS Provider. The TPSP does not store the user's credentials. As with redirection, the benefit of this approach is that the DFS Provider has control over the authentication process.

---

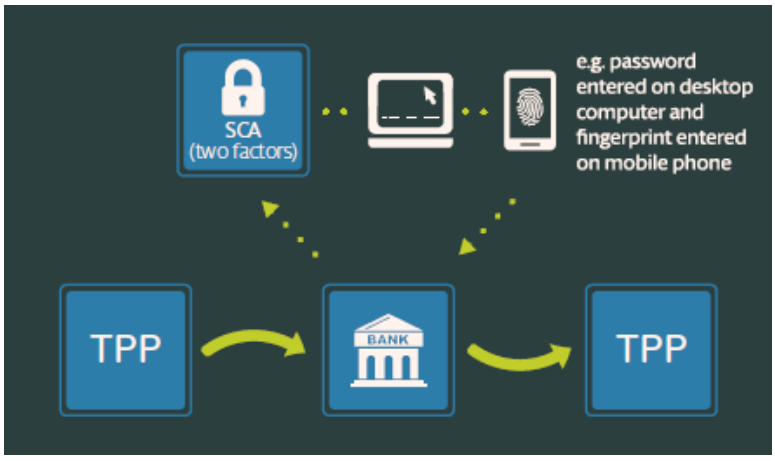
[12] This note is based on technology solutions available at a point in time. Given the pace of innovation in financial services, and payments in particular, it is likely that authentication methods and ways of initiating payments will develop rapidly, and specific methods or technology referred to in this note may be superseded.

*Example illustration - embedded method*




**C.** **Decoupled**: A decoupled model involves the use of a separate device or channel, such as a dedicated application, to complete customer authentication. For example, a customer could start his journey through a TPSP's browser-based website, but when he is prompted to authenticate himself, he provides a password through the browser and provides his fingerprint using the fingerprint reader on his mobile phone or otherwise responds to a push notification directly to a secure application on his mobile phone alerting him that authentication is needed. The decoupled model allows for the same or different devices to be used, and a decoupled element can be used with redirection or with an embedded model. It therefore allows for a number of solutions and can allow a user to authenticate using their mobile phone. As with redirection, authentication data are exchanged directly between the customer and the DFS Provider, and not with the third party.

*Example illustration - decoupled method*



**D.** **Delegated**: Customer authentication is delegated to the TPSP. It is performed completely through the TPSP's interface and the entire authentication process is handled by the TPSP, rather than the DFS Provider. As the DFS Provider will be reliant on the TPSP having carried out proper authentication, the contract needs to (i) cover the TPSP's obligation to conduct the customer authentication on behalf of the DFS Provider in accordance with the agreed authentication process, and (ii) determine the liability of the parties.

With both embedded and delegated approaches, there is a perceived increased risk of fraud as the security credentials of the user are shared with the TPSP or transmitted via the TPSP to the DFS Provider. This creates a potential point of weakness for hackers to exploit, and makes it more difficult to determine where liability should lie for fraudulent access. By contrast, where authentication happens within the DFS Provider's environment, it has evidence of the authentication if there is any dispute over liability for a fraudulent transaction.

*Example illustration – delegated method*


**Practical tip**

For further examples and diagrams of user journeys for each authentication method, the UK Open Banking Customer Experience Guidelines (version 1.3.0 dated 30 April 2019) is a useful reference: https://www.openbanking.org.uk/wp-content/uploads/Customer-Experience-Guidelines-V1.3.0.pdf

The Guidelines highlight that research shows consumers are familiar with decoupled authentication when making a payment or setting up a new payment, and many welcome the additional level of security that is provided by decoupled authentication. This means that, if journey designs follow similar patterns, consumers are likely to be more comfortable with them.

The DFS Provider's preferred approach may involve one or a combination of the above authentication methods, depending on the nature of the service or data being accessed and security practices (e.g., web redirection may not be a favoured approach, due to concerns about phishing risks for customers). This might also be influenced by the functionality / capability of the dominant phones in use in the market. The authentication method inherently involves trade-offs between risk, liability, ability to innovate and preserving as good a customer experience as possible. If the object of opening up access is to encourage customer uptake of TPSPs, user convenience needs to be considered. If the API does not support all of the authentication methods that are offered via the DFS Provider's user interface, that could be an obstacle to customers using TPSPs that call on the API for access to services.

The scope of this guidance note does not extend to recommending the type of customer authentication that parties should use when allowing customers access to services. Multi-factor authentication is increasingly being used to increase the level of certainty about an individual's identity, and this may be something that is mandated by local law. However, the strength of authentication needed will be influenced by the type of service, the value of any transaction, the recurrence of the transaction, the channel that is used, evolving threats, and regulatory requirements. For example, if a TPSP simply provides "read only" access to account balance or recent transactions, and without the ability to initiate transactions, a customer may not expect to use multi-factor authentication each time.

### 4.2 Guidance from the approach in the EU

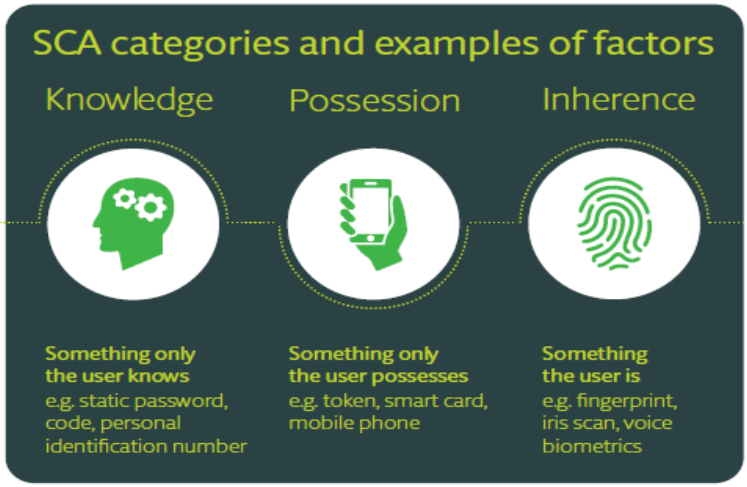
In the EU, PSD2 sets specific authentication rules, as does UK Open Banking. In each case, the aim behind the rules is to reduce fraud and make online payments secure, and therefore the rules may provide useful guidance in other jurisdictions:

(a) **PSD2:** PSD2 sets a high standard for customer authentication, by requiring 'strong customer authentication' (SCA) (as well as additional security measures - see section 6.3).

**What is strong customer authentication?**

SCA is defined as:

'*an authentication based on the **use of two or more elements** categorised as **knowledge** (something only the user knows) **possession** (something only the user possesses) and **inherence** (something the user is) that are independent, in that the breach of one does not compromise the reliability of the other, and is designed in such a way as to protect confidentiality*.'



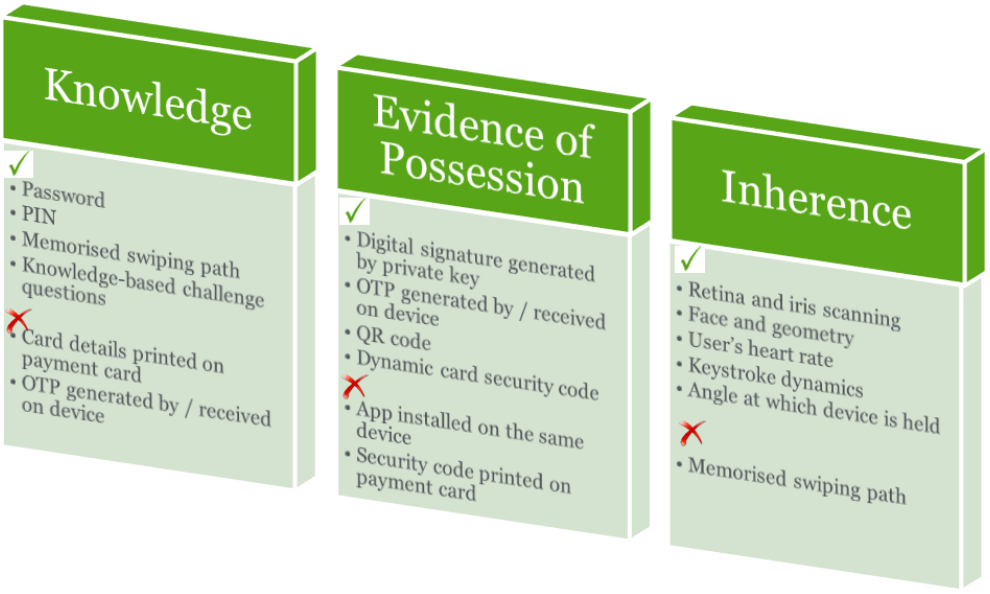

PSD2 mandates that a payment service provider must apply SCA whenever the user does one of the following (unless one of the prescribed exemptions applies):

- accesses its payment account online;
- initiates an electronic payment; or
- carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.

The exemptions aim to cover particular situations where there is a low risk of fraud and where the user experience is smoother by not requiring SCA or by requiring it only if particular conditions are met. For example, SCA does not need to be applied where the user is accessing online payment account information (unless this includes sensitive payment data, such as security credentials, which could be used to carry out fraud), and can only access balances and transactions which have taken place in the last 90 days. Another example is that SCA is not required for payments below a set threshold.

PSD2 does not detail how the SCA authentication rules should be satisfied. When the European Banking Authority published its accompanying regulatory technical standards on strong customer authentication, it made clear that it wanted the standards to be technology neutral and therefore it intentionally did not specify what methods are required to satisfy SCA. However, this approach gave rise to uncertainty in the industry around what would be compliant. The EBA has subsequently published its views on what may or may not constitute SCA[13], and some examples are shown in the diagram below.

[13] European Banking Authority (June 2019), '*Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2*', EBA-Op-2019-06




While this guidance is specific to the EU and what is needed for compliance with PSD2, it may be useful for any DFS Provider that is considering what authentication methods might be appropriate when providing secure access to its services.

(b) **UK Open Banking**: The previous Open Banking standards (v2.0) specified redirection authentication flows only, but Open Banking 3.0 standards support both redirection and decoupled authentication. This ensures that the customer can use the same authentication mechanisms when using a third party as it does when accessing it bank directly, so that it does not have a poorer experience when accessing the third party's services (e.g., the authentication process takes longer or involves more steps).

(c) **Common themes**: It appears that both PSD2 and Open Banking steer away from a simple form of redirection alone, as it is difficult to support all methods of SCA (such as biometrics) through, for example, an app-to-browser redirection. An open banking regime that restricts technical solutions to redirection only could inhibit user-friendly and secure alternative service implementations from being developed, reduce the opportunities for innovation, and may result in a user experience that is less than optimal.

(d) **Risks:** DFS Providers and TPSPs will need to consider the risks arising from the particular customer authentication method that they are using and how those can be mitigated contractually or operationally. For example, a mobile device can be set up for multiple people to use, which could mean that any registered fingerprint on the device could also authorise a payment. To mitigate this risk where a fingerprint is being used as a factor on a device, payment service providers in the EU have been advised (i) that their terms and conditions should include a specific limitation on the user allowing multiple people to access the device using their fingerprints and (ii) to provide specific warnings to users when registering for the service.

4.3 **Approach in the API Contract**

We are aware that certain DFS Providers will not support an approach that involves the TPSP carrying out the customer authentication or collecting security credentials, given the level of risk involved in relying on the TPSP and in the TPSP having access to customer security credentials issued by the DFS Provider.

It is expected that the DFS Provider will want to have control of authenticating the customers and obtaining consent directly from the customer. If the DFS Provider has issued the security credentials for its services to the customer and will authenticate the customer before allowing access, it will bear the risk if the individual accessing confidential data or instructing a payment is not the customer, but it is able to mitigate that risk in the way that it authenticates users.

However, if the DFS Provider wants to use a delegated authentication model and rely on the TPSP's authentication of the user, the risks will need to be addressed in the API Contract. As the TPSP is the party that will have control over the risk (i.e. whether or not the user is properly authenticated), we would recommend that the API Contract places responsibility squarely with the TPSP through the following as minimum:

(i) The TPSP has an obligation to authenticate the customer and obtain consent in accordance with the process notified to the DFS Provider or approved by the DFS Provider (as applicable), and to retain evidence it has done this. The process may include agreement on the level of security that is required (e.g., that the security credentials follow strong customer authentication requirements). The evidence will be important if there is any customer complaint and dispute over who is liable to the customer.

(ii) There is a warranty (i.e., a contractual promise) from the TPSP that it has obtained the customer's consent and that the transaction is authorised. Under English law, breach of a warranty by one party entitles the other party to claim damages arising from the breach.

(iii) The TPSP must tell the DFS Provider if it makes changes to the way it authenticates customers, as this may change the risk profile of the arrangement for the DFS Provider.

(iv) The TPSP is liable for any losses suffered by the DFS Provider as a result of the TPSP having failed to comply with the above provisions. While the customer may be accessing its account with a DFS Provider via the TPSP's mobile app, if there is a fraudulent transaction there is a likelihood that the customer will raise any complaint directly with the DFS Provider, on the basis that the DFS provider transferred money from the customer's account without his or her consent. We would expect such loss to be covered on an indemnity basis (i.e., the TPSP will agree to compensate the DFS Provider for the loss suffered as a consequence of its failure to comply).

Whether a TPSP will agree to accept this responsibility is a point for negotiation, and it may depend on the relative bargaining power of the parties. However, if the TPSP will not agree to these provisions, any DFS Provider should consider if it is willing to bear the risk of relying on that party's authentication, particularly if local law places primary liability on the DFS Provider and requires the DFS Provider to refund the customer if something goes wrong.

## 5. DATA PROTECTION

### 5.1 What is the risk?

The success of the TPSP's services and of the open APIs is likely to depend on customers having confidence that their data is going to be protected outside of the domain of the DFS Provider. The risks of opening up data to a TPSP will be dependent on the nature of the data (e.g., customer personal data, financial data or static product data) and volume of the data that is accessible, as well as the way in which data is made accessible.

In respect of customer personal data, any processing, disclosure, transmission and storage will need to be done in accordance with applicable data protection law. Local law may require that the personal data is processed only with the consent of the user. Even where it does not, a DFS Provider may choose to only process it if has the user's consent. Law and best practices vary considerably between jurisdictions, and the law will impact what must be included in the API Contract to protect customers. As such, this note deals with data protection only at a principles level.

### 5.2 Legitimate processing and consent

One of the key issues for a DFS Provider will be ensuring that it has the right to share customer data with the TPSP.

Most data protection law will require a legitimate basis for personal data to be collected, processed, stored, disclosed to and used by any third party. In the EU, the data protection legislation (GDPR) allows six grounds for processing data, including explicit consent, contractual necessity and legitimate interests. Explicit consent is only a requirement for specific circumstances, such as where decisions are going to be made about customers based on data analytics. However, in other jurisdictions, explicit consent may be the only basis under data protection law on which the DFS Provider can use data and share data with third parties.

Even where it is not the only basis, a DFS Provider may take the view that consent – which usually requires some positive action on the part of the individual giving the consent - is the least risky approach to ensuring that the customer permits its data to be shared with the TPSP.

**Practical tip**

In the EU, there are specific requirements that apply to consent under the GDPR. The principle behind these requirements is to ensure there is a clear indication of an individual's agreement to the processing of his or her personal data, so these can provide helpful pointers for any DFS Provider who wants to rely on customer consent. Consent must be:

- Freely given – it must be given on a voluntary basis (e.g., if a customer is offered a lesser service if he does not consent, that would not be freely given consent).
- Specific, informed and unambiguous – how can an individual truly give consent to something that he does not understand? As a starting point, customers should be told clearly what data is being collected and used, for what purposes, and who will be using it (including who it is being shared with).
- Given by a statement or by clear affirmative action - this requires conduct which clearly indicates acceptance by the customer of the proposed data use (e.g., checking a box or clicking a button to proceed). Silence, pre-ticked boxes and inactivity will not constitute consent.

## 5.3 Approach in the API Contract

Subject to local law, the following are the principles that we suggest DFS Providers will want to follow in their API Contract:

***Table 1 – Data protection principles***

| Area of risk | Proposed principle | Comment |
|---|---|---|
| Compliance with data protection law | *Each of the DFS Provider and the TPSP promises that it will process customer data in compliance with its obligations under applicable data protection law.* | The extent to which this is effective will depend on whether local data protection law imposes obligations directly on each party. As each of the DFS Provider and the TPSP will have its own relationship and contract with the customer (in respect of the services that it offers), the assumption is that each party will have its own legal obligations in respect of the customer's data - the TPSPs processing of customer data should be addressed through its own data protection notice or privacy policy with the customer. |

| Area of risk | Proposed principle | Comment |
|---|---|---|
| Security of data | *The TPSP will use and secure all data provided by the DFS Provider in compliance with agreed security requirements or a security policy* (explained further in section 6). | Security considerations are wider than just securing personal data. Not all data will be personal data, and confidential information is being shared (e.g., transactional data). Therefore, the API Contract should apply the security obligations in respect of all data that the DFS Provider discloses, and not just customer personal data. This obligation should also recognise that any security policy may include wider security requirements than just secure communication (e.g., minimum requirements applicable to the secure storage of data, obligation to notify the DFS Provider of any security breach of the TPSP's systems or other event that could impact the security of customer data or the secure provision of services to customers). |
| Scope of data accessed | *The TPSP will only request data that it is permitted to use and will not request more data than is required for the purposes of the TPSP providing its services to the customer.* | Many jurisdictions require that use of personal data should be limited to what is necessary (in the EU this is referred to as the 'data minimisation' principle), and that data are only collected and used for specific purposes notified to – or consented to by – the individual. This is also a sensible principle for a DFS Provider to follow in sharing data with third parties, as not providing more customer data than absolutely necessary could be one way of limiting the risk if data is exposed.<br><br>As mentioned earlier in the note, the DFS Provider should seek to manage risk not just through the contract, but also technically. Given the scope of the APIs supported by this note, DFS Providers should be able to mitigate the risks relating to data privacy and data minimisation through the API parameters, defining what data is available via the API and over what period. For example, the transactions history API could be set at various time periods and the TPSP must select the shortest time period that gives it only the information that it needs.<br><br>This risk may be mitigated also through the APIs themselves and the permissions that are applied. |

| Area of risk | Proposed principle | Comment |
|---|---|---|
| Misuse of data | *Any data transmitted to or accessed by the TPSP is subject to a limited licence linked to the purposes for which it has been provided (i.e., the customer request or transaction or the particular service the TPSP is providing to the customer).*<br><br>*Any breach of the licence terms, which includes the TPSP using customer personal data for purposes not agreed to by the DFS Provider, will entitle the DFS Provider to terminate the API Contract with immediate effect.* | Data ownership – who owns the rights in data – is a separate issue from data protection and who is responsible for how personal data are used and secured. To the extent that there is any intellectual property or other rights in the data provided by the DFS Provider, the DFS Provider will retain ownership of those rights and it is not transferring those rights to the TPSP.<br><br>The DFS Provider should have the right to revoke API access immediately if the TPSP starts using data for new services or for commercial purposes not approved by the DFS Provider. |

Note that in addition to laws relating to data privacy, there may be other local law and regulation that imposes specific requirements in respect of the services being provided and the data that is being disclosed. This could be very wide reaching and include, for example:

(i) law relating to confidentiality and banking privacy;

(ii) law relating to payment services;

(iii) law that ensures consumer protection. For example, in South Africa, lenders using lending APIs need to comply with the National Credit Act. In the UK, in response to concerns that open banking could result in an increase in authorised push payment fraud (APP fraud), the Financial Conduct Authority has introduced new rules on handling complaints about APP fraud; and

(iv) regulatory requirements. For example, in Hong Kong the HKMA expects banks to have terms in place with third party service providers that address a number of specific issues, including that the bank should require the third parties (i) not to misrepresent banks, and (ii) to make it explicit to their customers that the collection of personal data is neither carried out by banks nor directly related to bank business. In addition, the third parties should make clear the associated risk and liability of their services to their customers.

### 5.4 Derived data

Many TPSPs services are based on the aggregation of data, and valuable insights might be gained through analysis of the DFS Provider's data (either alone or in combination with data received from other DFS Providers) or the activity of its customers. In addition to thinking about the data sets made available via its APIs, a DFS Provider should consider its position in relation to any data that is derived by the TPSP from using those data sets.

In our experience, banks and other regulated DFS Providers typically want to limit what the API consumer can do with its data - including limiting the ability of the API consumer to create derived data that it can commercially exploit - even where the DFS Provider's data is being used on an anonymised and aggregated basis. If the API consumer's services are such that they rely on aggregation of data, this approach may not be commercially feasible. The DFS Provider should consider at the TPSP onboarding stage whether it is comfortable with the uses to which its customer data is being put, as the TPSP will not be able to accept contractual limitations later that prevent it from providing its products and services to customers.

If a TPSP's services are based on the processing of raw data received from the DFS Provider, the DFS Provider should set out clearly in the API Contract on what basis its data is being provided and that the DFS Provider takes no responsibility for aggregation of that data or any outputs from use of the data. In addition, the DFS Provider may require the API consumer to present disclaimers in relation to the DFS Provider's involvement and liability (see also section 10.6).

### 5.5 KYC APIs

As noted earlier in the note, the use of KYC-as-a-service or credit scoring-as-a-service APIs is not supported by this note. It is a complex area, and legal and regulatory requirements in the jurisdiction can significantly impact how such a service is managed and the risks. However, there are some general considerations for parties in relation to such use cases.

A key issue is the nature of the customer data that is being processed with such APIs. It will involve data that in most jurisdictions is classed as sensitive personal information, as there is a considerable risk of harm to the individual if that data is disclosed to unauthorised parties (e.g., identity theft and fraud). As such, higher standards of care and security usually apply in respect of the handling and security of such data.

Other considerations as a provider of such data / services:

- Rights to share the data - If you have gathered the data from different sources, do you have the necessary rights to share it with third parties and make commercial use of that data? This applies whether the data has been provided by the customer itself, or procured from commercial third party sources under licence, open data from publicly available resources, or data available on individuals from the internet (e.g., data scraped from an individual's online profiles or activity).

- Legal compliance - Are you processing the data in compliance with law and regulation? For example, if you are undertaking automated decision-making on or profiling EU citizens as part of the service you provide (e.g., using artificial intelligence to analyse and make predictions or decisions about an individual based on aspects of their economic situation, behaviour, interests and habits), you would have to take account of the specific rules and the rights of individuals under GDPR.

- Liability - What level of responsibility are you willing to accept in respect of either customer data that you are providing or any outcomes or conclusions that you have derived from the data? You will want to make clear in the contract any limitations and assumptions that apply.

Considerations as a consumer of such data / services:

- Reliability of the data sources:
    - Where you are receiving the raw data, what assurances are you being given about the accuracy and reliability of that data, and about the provider's right to process and share that data with you? You will want to understand the sources from which the provider derives its data (e.g., from verified sources or scraped from an individual's social media profile and feeds, or a mixture of sources). This could affect your risk assessment of the uses to which the data is being put (including the impact and consequences of you taking actions or decisions based upon that data) and the level of confidence that you place in such data.
    - If you are not receiving the raw data, but instead are receiving a 'packaged' service (e.g., where the data is processed and enriched by the service provider), what protections do you have if you are relying on that data? The provider may not be willing or able to give you the level of comfort that you need in order to rely on the data for full KYC / AML checks, particularly if they have acquired that data from a number of sources.
- Rights to use and store the data - Do the rights granted to you enable you to fulfil your legal and regulatory requirements? One particular consideration is that an organisation typically has to maintain evidence of its KYC and AML checks for a minimum prescribed period, in case it is asked to provide such evidence to regulatory authorities; therefore, it needs to have the right to retain and store certain data as part of its records.
- Reliability of the service - Is the provider giving any service levels around the availability of the service or the level of service it will deliver? If you have onboarding and application processes that are dependent on the service, it is likely to be a business critical service.

## 6. SECURITY

### 6.1 What is the risk?

When a DFS Provider gives a third party access to customer account information and allows a third party to initiate payments, there is a risk of fraud through unauthorised access, unauthorised use of information and unauthorised initiation of transactions. Further, while a DFS Provider might have stringent security measures in place to protect its customers' data, the data could be exposed if a TPSP suffers a data breach, potentially causing harm to the customers. As noted in section 5.3, security relates not only to personal data, but also to non-personal financial data.

To mitigate these risks, security considerations must encompass: how the confidentiality and integrity of the user's security credentials will be protected; robust standards for the communication between the DFS Provider and the TPSP; and what technical and organisational measures the TPSP has in place to protect customer data.

**Cyber resilience**

The rise in cyber attacks has led to regulators across different industries increasing their scrutiny of cyber resilience and how regulated organisations manage information, technology and communications risks. For DFS Providers that are regulated entities, this will need to form part of wider security considerations – and internal risk management policies - on how its systems, data and other assets are opened up to third party access. Parties should regularly conduct risk assessments and seek to learn from security incidents that have been identified or have occurred and, in addition to updating the necessary security measures, make sure that any lessons learned are fed back into incident response plans.

One way that DFS Providers can be proactive and take steps to identify security and operational threats is by participating in information sharing arrangements, both within and outside the industry, to achieve a greater awareness of cybersecurity issues and threats.

## 6.2 The risks of screen-scraping

One of the drivers for a DFS Provider to use a dedicated interface, like an API, is to have control and security around access to its data and services.

Many third party services still rely on screen-scraping to access account data, which involves the third party collecting and using the customer's log-in details to directly access the customer's data or account on their behalf. This is not the most secure method of access, as it involves the customer sharing security credentials with a third party, and requiring users to share credentials may increase the risk of hacking attempts or 'phishing' attempts (tricking users into sharing credentials with unauthorised third parties).

A further concern is that the DFS Provider cannot limit the data that is visible to the TPSP through screen-scraping, which could create data privacy issues for both the DFS Provider and the TPSP. It is likely also that the customer is in breach of its account terms and conditions by disclosing its access credentials to the third party. The recourse available to the customer could be limited if there are unauthorised transactions as a result of having shared security credentials with an unregulated third party.

## 6.3 Payment security

(a) While not exhaustive, the following list sets out certain security related points that DFS Providers may wish to consider in relation to payments. This is based on the PSD2 regulatory technical standards (**RTS**) in the EU, which has introduced requirements on secure open standards for communication, the secure creation and delivery of the personalised security credentials, as well as their association with the user, and conditions for the renewal and deactivation of those credentials. Parties will also need to take account of any specific legal requirements or industry standards that apply to the transactions, such as the Payment Card Industry Data Security Standards (PCI DSS), a set of security standards that apply if a business is storing, transmitting or processing payment cardholder data.

**Secure communication**

(i) **Does data need to be encrypted and when (e.g., during the communication session, when in transit, in storage)? If so, what is the level of encryption that is required?**

In the absence of prescribed security standards, it is recommended that parties apply secure encryption to the communications between them using internationally recognised encryption techniques.

Parties may need to take account of any local laws that apply to encrypted data, in particular the ability of law enforcement to request an unencrypted version of the data.

Even if a strong means of customer authentication (e.g., multi-factor authentication) is used by customers to access the service, fraud can still occur if communications between two systems are intercepted through a 'man-in-the-middle attack'. Such attacks can happen after the user has authenticated the transaction, with the fraudster intercepting the communication and altering some of the information. For example, the fraudulent party could alter the details of the payee and the amount - the customer would not know because he has already authorised the transaction. For this reason, it is important to ensure that any payment executed is to the same payee and for the same amount as was authorised by the customer.

The EU has sought to address this issue by requiring:

- that there is an **authentication code** generated for each payment transaction;

**Practical tip – Authentication codes**

The PSD2 RTS set out stringent requirements for the authentication code, including that it:

- should only be accepted once by the payment service provider,
- must be a unique code, and
- must be difficult to forge.

The customer must be made aware of the payment amount and the payee, so that the customer knows what is being authenticated. However, the authentication code itself can be 'behind the scenes' and does not need to be disclosed to the customer.

An authentication code could be based on solutions such as generating and validating one-time passwords, digital signatures or other cryptographically underpinned validity assertions using keys or cryptographic material stored in the authentication elements.

- the authentication code that is generated must be **'dynamically linked'** to the amount of the payment and the payee, i.e. the code must be specific to the amount and the payee; and

**Practical tip – Dynamic linking**

Dynamic linking could also be applied to batch transactions with different beneficiaries, if the authentication code is specific to both the total amount of all transactions and the various beneficiaries within the batch.

It is difficult to see how dynamic linking could be applied to a variable recurring payment, since at set-up the payment amount is not known and it is therefore not possible to dynamically link the authentication code to the amount of the transaction.

- invalidation of the authentication code if the new details do not match (and a requirement that authentication be re-applied).

While these requirements are specific to the EU, the key principle behind them – that a customer knows what he is authenticating and that he is authenticating that particular transaction data – can be applied to payment transactions anywhere.

(ii) **Is there a requirement on the TPSP to actively terminate any secure communication session as soon as the requested action is complete?**

To minimise the risk of data being intercepted, DFS Providers will want access sessions to be as short as possible.

(iii) **What processes does the TPSP have in place to ensure that all parts of any payment transactions and other interactions with the user and other entities (e.g., merchants and other third party service providers) are traceable?**

If a customer raises an issue with the DFS Provider relating to its account (e.g., disputes a transaction), the DFS Provider may need to rely on the TPSP's audit trail to identify where any issue occurred and who is at fault. In the EU, the RTS does not prescribe any time recording protocols, but it does require payment service providers to ensure that any communication session established relies on a unique identifier of the session, security mechanisms for the detailed logging of the transaction and timestamps.

(b) **Protection of security credentials (including delivery)**

(i) **How will the DFS Provider ensure the confidentiality and integrity of the security credentials of users during all phases of authentication?**

The API may not allow the TPSP to see or store the customer's security credentials (e.g., an API that uses the OAuth protocol for authorisation or uses other access tokens for each communication session).

The RTS sets out requirements to ensure that security credentials and authentication codes are protected when they are being used by the customer. This includes that the security credentials are masked when displayed (and are not readable to their full extent when input by the user) and that security credentials in data format are not stored in plaintext.

(ii) **What procedures does the DFS Provider have in place to ensure that personalised security credentials are created in a secure environment and sent to the user in a way which mitigates the risk of unauthorised access due to their loss, theft or copying?**

In the EU, the RTS requires the use of '*strong and widely recognised*' industry standards in the processing and routing of personalised security credentials and of the authentication codes. This has been kept broad to avoid endorsing a particular standard, but in practice any payment services provider will be subject to any standards stipulated by particular payment schemes in the market.

(iii) **What procedures does the provider have in place to ensure that only the user is associated with the personalised security credentials and authentication devices?**

Such association will mitigate against the risk of fraud or unauthorised use of those credentials or devices. To reduce the risk of interception, the association should ideally be carried out in a secure environment under the DFS Provider's responsibility (where it is undertaking authentication).

(iv) **What processes does the DFS Provider have in place for the secure destruction, deactivation or revocation of security credentials or authentication devices?**

The approach taken in the EU under the RTS is that all payment service providers must have effective processes in place to ensure: (i) the secure destruction, deactivation or revocation of personalised security credentials, authentication devices and software; (ii) the secure deactivation or revocation of information related to personalised credentials stored in the PSP's systems and databases; and (iii) the secure re-use of a device (or software) is established before making it available to another user.

6.4 **Approach in the API Contract**

We would expect each DFS Provider to stipulate, or to agree with the TPSP, the security measures that will apply. The DFS Provider may wish to stipulate in the API Contract that the TPSP must comply with the DFS Provider's standard security requirements. Alternatively, the DFS Provider may agree a security policy with the TPSP that applies to the API Contract. The security requirements or security policy may be set out in a Schedule to the API Contract or within a separate document that is cross-referenced from (and incorporated into) the API Contract.

The level of security requirements must be balanced against the user journey, as a process that is overly cumbersome could put off customers using the TPSP's service or equally could put off TPSPs from using the DFS Provider's services.

It is not within the scope of this note to provide a set of default security requirements, but we recommend that the security requirements cover the following points as a minimum:

(a) a secure connection must be established before data is transferred;

(b) each party will be responsible for the security of its own system;

(c) each party will agree to not transmit any malware through use of the APIs or introduce malware into any data or transmission sent to the other party or introduced into the other party's system, and will notify the other immediately after becoming aware that there might have been malware in any transmission;

(d) each party will use commercially available and current scanning tools (in line with good industry practice) to scan for malware;

(e) the TPSP must conduct regular risk analysis and take steps to update any security measures as needed to remedy any security incidents or identified vulnerabilities and ensure such an incident does not re-occur; and

(f) the TPSP will notify the DFS Provider within any specified timescale (or, as a default, as soon as possible after becoming aware) of any actual or suspected security breach of the TPSP's systems.

Local law and regulation may impose data breach notification requirements on the DFS Provider which need to be reflected in the API Contract. For example, in the UK, a controller[14] must notify the Information Commissioner's Office (the UK data protection regulator) within 72 hours of becoming aware of a personal data breach that meets certain criteria. If the DFS Provider is a bank or other regulated entity for financial services, it will have to notify its financial regulator also of such a data breach. Depending on the nature of the breach, the DFS Provider may also be required by law to inform affected customers.

We recommend that the API defines "security breach" to include not only actual events but indications of a breach and also any near misses and attempted breaches, so that the DFS Provider is made aware if a TPSP is subject to frequent attacks. However, parties will need to ensure that the definition of "security breach" aligns with their internal security policy and applicable law.

[14] Under laws in the UK, the 'controller' of personal data is the party that determines the purposes and means of processing that data. Each of the DFS Provider and the API consumer would be a controller of personal data that it collects from customers and uses to provide its services to customers, and each would have its own legal obligations to protect that data.

**Practical tip**

Other things that a DFS Provider can do to mitigate risk:

- Keep up-to-date with best practices, including promptly installing updates and patches, for API security in your market and on common security threats and known vulnerabilities.

- Monitor the TPSP's compliance with the security requirements on an ongoing basis and seek assurance that the TPSP is complying with the agreed security measures. This may be through auditing the TPSP's compliance with the security requirements, but you may be willing to rely on the results of any security audit carried out by an accredited third party or on the TPSP's compliance with recognised security standards / third-party security certification. Linked to this will be the right to withdraw access to the services if the TPSP is non-compliant.

- Use analytics and other tools to detect fraud, where practicable. Transaction risk analysis (TRA) – which can be deployed in real time – can be used to detect fraud by monitoring activity and behaviour. For example, TRA can be used to identify suspicious transactions through picking up abnormal behaviour of a customer (e.g., unexpectedly high amounts given the payer's previous spending pattern), unusual requests from a TPSP, or an unusual sequence of calls on the APIs. Advanced analytics could be used also to validate the origin of inbound calls to the API.

## 7. LIABILITY

### 7.1 Approach to allocation of risk

A key consideration for the DFS Provider is how liability should be allocated between it and the API consumer if something goes wrong.

In order to distribute a risk logically and fairly between the parties under a balanced contract, the parties should consider:

- which of the parties is most likely to have been at fault;
- which party is most able to control the risk; and
- which party is most able to mitigate the losses arising from the risk. This could be operational mitigation (e.g., the party that will be able to withdraw access to the service, preventing further loss) or financial mitigation (e.g., the party that can purchase insurance cover for the particular risk).

The table below sets out suggested liability positions for certain key risks identified in this note, based on the principles above. While this is not an exhaustive list, the suggested positions are intended to give DFS Providers a starting point in respect of how responsibility for such risks could be allocated. However, it is acknowledged that:

(i) not all parties may be willing or able to accept these positions, given their own risk appetite;

(ii) liability may be dictated by applicable law and by who is responsible for the different activities, which may not be the same across API arrangements (e.g., different authentication methods) – DFS Providers will need to consider this for their own territory and arrangements; and

(iii) such positions may not reflect the party who was at fault in the circumstances - a dispute resolution process (see section 9.2) should help the parties to resolve disputes about which of the parties was actually at fault, and who should bear the liability in the circumstances, without immediate recourse to court action.

***Table 2 – Key risks and allocation of responsibility***

| Area of risk | Primary responsibility | Comments / considerations |
|---|---|---|
| Accuracy of customer data | The DFS Provider is responsible for ensuring that the data it provides is the data requested by the TPSP and that it is error free or at least free from material errors. | This depends on the extent to which the DFS Provider will accept responsibility for the data which it provides, as it may make data available on an 'as is' basis only and look to exclude liability. As developed further in section 10.4, if the TPSP is paying for API access and relying on the data to provide services to the customer, it is not unreasonable for the TPSP to expect a certain standard to apply.<br><br>If the DFS Provider does accept this approach, we assume a DFS Provider will want to accept no greater liability than if the customer had accessed the incorrect data directly from the DFS Provider, i.e., the DFS Provider will not be liable for losses arising from TPSP decisions or outcomes based upon that data. |
| Liability for the TPSP's services | The TPSP is responsible for the services that it provides to the customer and for its use of the data from the DFS Provider, including any losses arising from changes it makes to the customer data and/or outcomes arising from the TPSP's combination of the data with other data sources. | The TPSP should be responsible for its services and outputs, including how it uses the DFS Provider's resources. This is within its control. It should be liable to the DFS Provider for any losses that the DFS Provider incurs to a customer as a result of the TPSP's services.<br><br>Even if the parties try to prevent a customer from raising a claim directly against the DFS Provider (e.g., by presenting disclaimers or agreeing a process under which all direct customer complaints are re-directed to the TPSP), the DFS Provider will still want to be protected against any losses it incurs due to direct customer claims. Such losses would typically be covered on an indemnity basis (i.e., the TPSP will agree to reimburse the DFS Provider for its costs, expenses and other losses as a result of the claim). |

| Area of risk | Primary responsibility | Comments / considerations |
|---|---|---|
| Misuse of the APIs / data | The TPSP is responsible for using the APIs and the DFS Provider's data and services in accordance with the API Contract, the scope of the customer's consent, and applicable data protection law. This will include:<br><br>• only using data for the purposes disclosed to the DFS Provider and permitted by the API Contract; and<br><br>• only accessing (and attempting to access) those resources for which it has been granted access permission.<br><br>**Secondary responsibility**: The DFS Provider will be responsible for authenticating the TPSP (when it makes a call on the APIs) in accordance with the agreed authentication method, and enforcing any access permissions, and ensuring that it only provides the TPSP with the data and access requested and no more. | The TPSP should be liable for losses incurred by the DFS Provider as a result the TPSP using data / the services in breach of the API Contract or undertaking activities without the customer's consent or otherwise in breach of applicable law. We would expect the API Contract to set out any restrictions that apply to use of the APIs, and therefore the losses should include any deliberate or negligent TPSP activity that adversely impacts the DFS Provider's services (e.g., excessive calls on the APIs).<br><br>There is likely to be negotiation on the scope of the losses that a TPSP is willing to accept here. For example, will the TPSP be liable for any regulatory fines that the DFS Provider incurs as a result of the TPSP's misuse of customer information (assuming local law allows recovery of fines from a third party)?<br><br>The DFS Provider should consider what potential losses it could incur as a result of the TPSP's misuse of the APIs, and ensure that such losses are not automatically excluded by the usual list of excluded heads of loss. For example, reputational damage, ex gratia payments to customers and regulatory costs / fines are all heads of loss that are typically excluded under a contract, yet they are losses that the DFS Provider could foreseeably incur if there is misuse of its APIs and/or customer data. |
| Unauthorised payments | The DFS Provider is responsible for authenticating the customer and ensuring that the customer has authorised the payment instruction, and for not accepting a payment initiation request if the user fails authentication.<br><br>The TPSP is responsible for initiating payment transactions only with the consent of the customer and within the parameters of its authority. The TPSP is responsible also for putting in place processes to guard against the fraud or other wilful misconduct of the TPSP's personnel. | This will depend on which party is responsible for issuing the security credentials to the customer and checking that it is the customer who is consenting to the payment. However, on the assumption that the DFS Provider will be authenticating the customer within its domain, the TPSP should have the right to rely on that authentication having been properly carried out.<br><br>The TPSP should be liable for any losses that result from it acting outside the parameters of its authority (e.g., where the TPSP is collecting a variable recurring payment, it collects excessive amounts or changes the payment dates or payee without consent), including where the customer has withdrawn consent to the payment before any cut-off.<br><br>If there is a fraudulent transaction, there is a likelihood that the customer will raise any complaint directly with the DFS Provider, on the basis that the DFS provider transferred money from the customer's account without his or her consent. Local law may make the DFS Provider automatically liable for unauthorised transactions. We expect that DFS Providers will want the TPSP to indemnify or 'make whole' the DFS Provider for any losses suffered as a consequence of the TPSP's breach, negligence or fraud (including the fraud or other wilful misconduct of the TPSP's personnel). The TPSP may expect a mutual indemnity for losses it incurs to customers as a result of the DFS Provider's acts or omissions. |

| Area of risk | Primary responsibility | Comments / considerations |
|---|---|---|
| Payment is incorrectly executed | The DFS Provider is responsible if there is a deficiency in the execution of a payment transaction (e.g., executed late, incorrectly or not at all) due to its fault or negligence.<br><br>The TPSP is responsible if there is a deficiency in the execution of a payment transaction due to its fault or negligence. | Liability will depend on the facts and who is at fault in the circumstances (e.g., did the DFS Provider simply execute the transaction wrongly or was the payment initiation request wrong, and was this due to the fault of the TPSP / its software or due to an issue that arose during transmission)?<br><br>Alternatively, the parties could agree to a default liability position in the API Contract. Under PSD2, the account provider is responsible for refunding the customer for any unauthorised or incorrectly executed transaction, but it can then recover this from the third party provider – the third party provider is liable unless it can show that within its "sphere of competence" (i.e., within its control) the transaction was properly authorised and executed. |
| Security breach | The TPSP is responsible for putting in places measures to ensure the security of customer data and of the services, including complying with the security policy / the agreed security measures in the API Contract, and for not allowing unauthorised individuals to access and use the DFS Provider's data and services via the TPSP's systems. | The TPSP should be liable for failing to comply with agreed security measures and for allowing unauthorised individuals to access and use the services via its systems.<br><br>However, each DFS Provider will need to decide if it expects the TPSP to have strict liability for a security breach (i.e., is the TPSP liable for any fraudulent requests for information and fraudulent transactions a result of any security breach, even where the TPSP is hacked?) or liable only for security breaches resulting from the TPSP's fault or negligence, such as where it fails to patch known vulnerabilities that are later exploited by a hacker. The approach is likely to be influenced by the DFS Provider's exposure under local law for unauthorised transactions and for data breaches. |
| Reputational risk | The TPSP is responsible for any misuse of the DFS Provider's brand and for any activity that causes damage to the DFS Provider's reputation (including fraud, misuse of the APIs, misrepresenting the DFS Provider's products and services, security breach, persistent poor service to customers). | We would expect the TPSP to be liable to the DFS Provider where it offers its services or conducts itself in a manner that causes damage to the DFS Provider's reputation. This should apply whether or not the TPSP has the right to use the DFS Provider's brand and logo within its service, but any misuse of the brand will be a breach of intellectual property rights also.<br><br>There is likely to be negotiation on the type of loss that the TPSP is willing to accept, given that damage to reputation is a commonly excluded head of loss. |
| Malware | Each party is responsible for not introducing malware and viruses into the system of the other party.<br><br>**Secondary responsibility:** Each party should have in place anti-virus software / protections against malware (e.g. commercially available and current scanning tools) in line with good industry practice, in order to protect its own software and systems. | The parties may want to limit their liability to "knowingly or negligently" introducing malware into the system of the other party, or excluding liability to the extent that the other party has failed to mitigate its losses by having in place anti-virus software or other preventative measures. |

7.2 **Considerations relating to liability**

(a) **Financial standing**: the protections offered by the contract will only be as good as the financial standing of the party, particularly if the TPSP is a start-up. If the TPSP accepts unlimited liability for misuse of customer data, but has limited assets and cannot insure itself against the risk, what losses (if any) can the DFS Provider recover if a customer takes action against the DFS Provider? This is one reason why DFS Providers should not rely wholly on a contract to address all risks, but consider also how risks can be mitigated in other ways.

API agreements often include a general obligation that the TPSP will have in place adequate insurance to cover its liability under the contract, but a DFS Provider may wish to specify the minimum type(s) of insurance cover that it expects the TPSP to hold (e.g., cyber and data insurance) and the minimum level of cover. The effectiveness of this provision will depend on the availability and cost of suitable insurance cover in the relevant market.

(b) **Exclusion v. limitation of liabilities**: parties should bear in mind there is a difference between (i) excluding all liability for a risk (e.g., accepting no liability for losses arising from a cyber attack), (ii) excluding all liability for certain losses (e.g., accepting no liability for loss of data), and (iii) accepting liability for a loss but limiting that liability (e.g., applying a monetary cap on liability or restricting the remedies that will apply).

For example, the DFS Provider could look to exclude all liability for losses that the TPSP incurs if the APIs are unavailable, including loss of business and loss of profits. A TPSP may reject this as unacceptable, particularly if the DFS Provider is agreeing to meet service levels (see section 10.3). If the TPSP is paying fees, an alternative approach might therefore be that:

(i) the DFS Provider agrees to accept liability for service level breaches up to a capped amount; or

(ii) a service credit regime applies to a breach of the service levels, and the DFS Provider's only liability for service level breaches is to pay the service credits.

The DFS Provider will need to consider what losses it will be appropriate to exclude or limit in the API Contract, based on local law and the commercial arrangement.

(c) **Local law**: Local law will influence what losses can and cannot be recovered under a contract, and there may be specific types of loss that the applicable law does not allow parties to exclude or limit. In the UK, for example, parties cannot limit or exclude their liability for personal injury or for fraud.

If, by law, the DFS Provider is responsible for refunding the customer for any losses, the API Contract should provide for the recovery of those losses where they result from the breach, negligence or fraud (or other wilful conduct) of the TPSP. We expect that the DFS Provider would want this to be on an indemnity basis.

# 8. TECHNICAL STANDARDS

## 8.1 Technical standards

It will be for DFS Providers to determine and document the technical standards that apply to their APIs. We would expect any specification to cover, as a minimum, how the TPSP will identify itself to the DFS Provider when it makes a call on an API and how secure communication will be ensured between the parties.

Depending on the sector and market in which the DFS Provider operates and the nature of the services being provided, there may be open API standards available. There are a number of industry bodies that have developed or are developing API standards for access to financial data, for example:

| **Jurisdiction** | **New Zealand**  |
|---|---|
| Initiative | Payments NZ |
| Objective | To develop common API standards and a supporting management framework for the New Zealand payments ecosystem, and provide a vehicle to establish and progress an industry API strategy. |
| Summary | Formed in 2010 by the NZ payments industry with the support of the Reserve Bank, it is a governance organisation working with industry to make payments secure and simple. |
| Status | Published first API standards, for Payment Initiation and Account Information. Launched its API Centre in 2019. |

| **Jurisdiction** | **Nigeria**  |
|---|---|
| Initiative | Open Banking Nigeria / Open Technology Foundation (OTF) |
| Objective | To build a common standard for open banking APIs in Nigeria for the financial services industry. Will also provide a sandbox from which testing and certification can be done. |
| Summary | OTF is a not-for-profit organisation founded by a group of industry players to drive the development and adoption of open banking standards in Nigeria. It works with banks, seasoned industry professionals and FinTechs to define an open and non-partisan set of APIs and to design the API standards. |
| Status | The Open Banking Nigeria API is under development. |

| Jurisdiction | Global |
|---|---|
| Initiative | GSMA |
| Objective | To provide common APIs to raise industry capabilities. |
| Summary | GSMA represents the interests of mobile operators worldwide. It has published mobile money APIs that have been jointly developed by key stakeholders - mobile money providers, platform vendors, third party service providers and industry partners - and that combine best practices in the technology industry. |
| Status | Has published mobile money APIs, and provides the API Exchange. |

In the EU, PSD2 specifies the conditions for the technical framework but does not define an interface standard. By contrast, UK Open Banking sets a "Standard", which consists of not only technical specifications for the in-scope APIs (payment initiation, account information, fund confirmation and event notification), but also customer experience guidelines and operational guidelines.

8.2 **Change control / variation**

Each DFS Provider should consider: (i) how any changes to its API specifications will be notified to TPSPs; and (ii) if there will be a minimum notice period or 'lead in' time given, to enable TPSPs to implement the changes.

The channel for communicating changes can often be dictated by how users interact with the API provider. For example, it is not uncommon for developers to advise of API updates via an alert on social media, such as on Twitter. Also, depending on the type of API, it may be possible to use the API itself to notify changes.

The following options appear to be the most common approaches currently taken by organisations for the notification of changes:

(a) Changes to the specification are communicated via the DFS's Provider's website or dedicated API portal, if it has one. This is the most convenient approach for the DFS Provider, who only has to post changes in one place, but it is often less effective than the second option below in terms of ensuring that the TPSP is made aware of a change in advance of it taking effect. It places the onus on the TPSPs to monitor the site for any changes.

(b) Changes to the specification are communicated by email to TPSPs. The DFS Provider could use automated mailing, to minimise its effort. With this approach, however, each TPSP will need to keep the DFS Provider updated as to who is its main point of contact for these purposes.

It is recommended that the DFS Provider gives a minimum period of notice before any material changes to the API take effect, except when emergency changes are needed (e.g., to address a known security vulnerability). What is an appropriate notice period will depend on the nature and extent of any change, and some API providers may take a tiered approach depending on the urgency of the change.

There are no standard positions around how much notice should be given, and some API providers do not commit to any notice period at all. As an example of one approach, UK Open Banking requires API providers to give 60 business days' notice of any creation, deletion or updating of an open data endpoint[15].

In addition to notifying the changes, the DFS Provider should indicate if it will continue to support previous API versions and, if so, for how long.

## 9. ADDITIONAL AREAS TO CONSIDER

### 9.1 Licences

The following licences from the DFS Provider to the TPSP could be considered as a starting point in the API Contract:

(a) a licence to use the APIs (to the extent that a licence is needed - otherwise, the TPSP is granted access to the services via the API and must comply with any restrictions that apply to use of the APIs) and the accompanying documents, such as the API specifications. If the APIs are owned or made available by a third party, the DFS Provider will need to check that the licence is back-to-back with the rights granted to the DFS Provider. Any open source software will need to be provided on the terms of the applicable open source licence;

(b) a licence to use the data provided by the DFS Provider for the purposes of providing its services to the customer and complying with its obligations under the API Contract; and

(c) a licence to use the DFS Provider's brand for approved purposes, subject to the TPSP complying with any applicable brand guidelines and (if required by the DFS Provider) seeking sign-off on the use of the brand before live use. This may not be appropriate in all relationships, and some DFS Providers will have internal policies restricting use of their brand by commercial partners.

Where the DFS Provider suspends or terminates access to the APIs under the API Contract, these licences should be suspended or terminated (as applicable) accordingly.

### 9.2 Dispute resolution procedure (DRP)

There are two categories of dispute resolution process that the DFS Provider may want to consider: in respect of disputes between the parties under the API Contract and in respect of any customer disputes.

(a) **Disputes between the parties**

It is increasingly common for parties to include an agreed dispute resolution process in their contracts, to avoid court action unless the dispute is sufficiently serious and/or the relationship between the parties has broken down. Indeed, the courts in some jurisdictions will expect to see evidence that the parties have tried to resolve the issue between them first.

[15] Open Banking (version 2.0, July 2018), '*Open Data Service Level Agreement for API Providers*', section 5.2.

We would recommend that the API Contract includes a dispute resolution process that encourages parties to resolve any issues through escalation and alternative dispute resolution (ADR). However, this should not prevent either party from going to court in all circumstances, and there should be exceptions that are appropriate for the local jurisdiction (e.g., emergency action to prevent the other party from infringing your intellectual property rights).

DFS Providers should consider the forms of ADR process that are recognised and available in their jurisdiction, and there may be ADR services available in the market that the parties can use. For example, many UK parties agree to refer disputes to the Centre for Effective Dispute Resolution (CEDR) in London and to follow CEDR's documented processes - this avoids the need to set out a detailed process in the contract.

**UK approach to settling open banking disputes**

The Open Banking Implementation Entity – in consultation with stakeholders from UK Government, regulators, the financial services sector and consumer groups - has set up a Dispute Management System (**DMS**) that account providers and third party providers can use to manage complaints or disputes. The DMS, which is not just limited to members of Open Banking, provides a 'structured pathway to mediation, adjudication or arbitration'.

As the OBIE notes on its website, the DMS does not take the place of alternative dispute processes, but it is a voluntary mechanism for account providers and third party providers to talk to one another. All participants must follow the set of principles and best practice standards set out in the DMS Code of Best Practice. Further details on the DMS can be found at https://www.openbanking.org.uk/providers/dispute-management-system/

Depending on the risks associated with the use of the APIs and the likelihood of customers bringing claims directly against the DFS Provider, the DFS Provider may want to compel the TPSP to disclose its electronic audit trail (e.g., electronic records of instructions issued) where the DFS Provider needs this in order to comply with applicable law and regulation or where needed in order to deal with a customer issue. In many jurisdictions, such an obligation will be concurrent with legal or regulatory obligations to retain data, subject always to any legal limitations on how long a party can retain personal data.

(b) **Customer dispute resolution**

The key question is the extent to which the DFS Provider wants to become involved, if at all, in any customer disputes with the TPSP (assuming always that local law does not make the DFS Provider responsible for dealing with customer issues in the first instance). Most DFS Providers will not want to become drawn into disputes about the TPSP's services; however, the risk of having no involvement or oversight means that the TPSP's handling of the complaint could be poor and impact the DFS Provider's reputation in the eyes of its customers.

There are different approaches that a DFS Provider could take to customer disputes:

- Request regular reporting on customer complaints (to include any minimum information that you would want to know) and with the ability to request further information on any particular disputes that might be of concern, such as recurring complaints or complaints that have taken a long time to resolve.

- Ask to see the TPSP's customer complaints process as part of onboarding and due diligence, and include an obligation on the TPSP to follow that process. If the TPSP does not have a complaints process, the parties may want to agree a process in the API Contract that the TPSP will follow. This could have service levels attached, such as timescales for responding to the customer. As part of this, the parties may need to agree what happens if a customer raises a complaint directly with the DFS Provider (i.e., will the DFS Provider redirect the customer to the TPSP or deal with the dispute directly (liaising with the TPSP) and reclaim any costs and expenses from the TPSP?).

- Agree if and when any complaints are directed to the DFS Provider, and the criteria that will apply. For example, if the TPSP sent the correct instruction but the DFS Provider executes the instruction wrongly, the parties may prefer that the customer and the DFS Provider resolve the issue directly between them. There could also be a service level attached to the redirection of disputes by the TPSP, to ensure that the DFS Provider can deal with those promptly.

**Learning from the EU approach to protecting the customer**

If a payment is initiated through a payment initiation service provider, PSD2 allows the customer to claim any loss directly from the ASPSP for an unauthorised transaction or a deficiency in the execution of the payment (e.g., late or incorrect). The ASPSP can then recover from the TPP unless the TPP can show that within their "sphere of competence" the transaction was properly authorised and executed. This position ensures that the customer's issue is dealt with quickly and is not dependent on the parties resolving any disagreement between them as to which party is at fault.

Where there is no default liability position under law, it would be open to DFS Providers and TPSPs to agree a default approach to dealing with customer claims, in order to ensure that claims are dealt with and that the reputation of both parties in the eye of the customer is preserved. The API Contract could be used to stipulate what will happen in situations where it is clear which party is at fault (e.g., where the TPSP collects a payment in excess of the amount authorised or notified, it is liable to immediately reimburse the excess) and/or deal with the recovery of loss where the party bearing default liability was not at fault. The dispute resolution process could be used to facilitate recovery.

The parties should take into account the circumstances in which the customer is the liable party. For example, under PSD2, the payer (customer) can be liable for unauthorised transactions in specific circumstances - he has acted fraudulently, has failed to keep his security credentials safe, or has failed to report the loss - or liable up to a maximum amount of €50 for any other transaction.

## 9.3 Business continuity / contingency

A key question for a TPSP is likely to be: what happens if the API becomes unavailable or is not performing to the expected standard?

If a TPSP is reliant on access to the DFS Provider's services and data in order to provide its own services to customers, it will want to know how it can continue to access that service and data if the API is not working.

If the API is not operating properly, the customer can access the service or data directly from the DFS Provider, but that by-passes the TPSP and its services. A TPSP may – if technically possible and practical – resort to screen-scraping as a simple contingency measure, so that it continues to have access to customer data.

Many providers object to screen-scraping, as it is a less secure method of access (see section 6.2) and the DFS Provider cannot control how the scraped data is used by the TPSP. Screen-scraping is also not the perfect solution for TPSPs. If a DFS Provider updates its user interface, the TPSP may need to update its software in order to read and process that new layout: this could create a challenge to the TPSP's ability to provide a continuous service to its users.

Local law may provide a contingency measure in the event that the open API is unavailable. In the EU, a prescribed form of screen-scraping, known as "screen-scraping+", is permitted if a dedicated interface becomes unavailable or is not performing as required. In relation to a bank account, for example, the third party still accesses a user's account via the same interface as the user, but it is required to identify itself to the ASPSP so that the ASPSP is aware of the fact that this particular access attempt is being carried out by a third party and not by the customer. While this does not address all of the concerns raised around screen-scraping, it is intended to address security concerns.

A DFS Provider may wish to provide for a contingency measure in its API Contract, in order to retain control over the TPSP's access to its service and data. If a DFS Provider wanted to allow an approach similar to "screen-scraping+", it should bear in mind that screen-scraping may give the TPSP access to more data than it needs to provide its services, and more data than the customer might have consented to sharing. Therefore, we would recommend that the API Contract should:

- specify the specific process that must be followed and prohibit access by any other means;
- clearly set out the circumstances in which the alternative process is permitted, to ensure that it can only be used in circumstances where the API is genuinely unavailable or objectively under-performing;
- require that any secure communication requirements are stringent enough to cover communication sessions through screen-scraping;
- require that the TPSP will access data only for the provision of the service that has been requested by the customer and for no other purposes;
- require that the TPSP will store security credentials in a secure way, which may be an obligation on them to encrypt all user access details, or the TPSP will not retain the security credentials at all; and

- deal with the apportionment of risk between the parties during the contingency period (i.e., will the liability position change to reflect any additional risk, such as the TPSP having access to more data than via the API or access to security credentials?).

## 10. COMMERCIAL TERMS

We anticipate that the API Contract will need to deal with a number of commercial issues, but in respect of APIs we expect DFS Providers will want to consider the following areas.

### 10.1 Pricing

Many providers do not charge for access to services through its APIs, and local law or open banking regimes may preclude charging. In the EU, in those circumstances where banks and other account providers must allow permitted third party service providers access to customer accounts under PSD2, they are not allowed to charge the third party service providers for that. They are also not allowed to discriminate against those third parties, e.g., by putting them at the end of a priority queue or providing a lesser service. However, if a DFS Provider does opt to charge for access to its APIs, it may want to consider the ability to change pricing over the term of the contract as a means of adjusting to market circumstances.

> **Practical tip**
>
> A DFS Provider may decide not to charge fees for access to its services, but may expect another form of value exchange. For example, subject to local law the DFS Provider may allow the TPSP to aggregate its data with data from other sources in order to undertake market analysis and gain insights, provided that such insights are shared with the DFS Provider to enable it to improve its own services to customers. Note that any such aggregation and use of the DFS Provider's data would need to be subject to suitable protections. These might include that the TPSP cannot make any customer personal data available to a third party and must anonymise any personal data, and that the DFS Provider must not be capable of being identified from the aggregated data.

### 10.2 Term of the contract

The main consideration is whether the API Contract will be for a fixed term or 'evergreen'. An 'evergreen' contract is one which runs from the start date until it is terminated or it runs for a fixed period and automatically renews at the end of that period. The contract term may be determined by the pricing structure, if the DFS Provider is charging fees for access to its services (e.g., annual contract term linked to annual payment of fees).

One reason why parties might include an automatic renewal clause is to ensure that they are not accidentally operating 'out of contract', where the contract automatically expires at end of the fixed term and neither party has realised.

However, DFS Providers should bear the following in mind with automatic renewal clauses:

- In some jurisdictions, such a clause may be considered as an unfair contract term in non-negotiated contracts (e.g., in a consumer contract or in standard form terms and conditions that must be accepted 'as is'). This is likely to be the case if the clause is seen as locking the other party into the contract, by restricting the ability of the TPSP to bring the contract to an end and/or if a termination fee applies to any termination of the contract during the renewed term.

- Such clause is typically drafted to say that the contract will automatically renew unless one of the parties takes action to positively bring the contract to an end, such as serving written notice of termination. There is usually a cut-off date for this (e.g., not less than 60 days prior to the date on which the contract will automatically renew). The parties will need to diarise far enough in advance to ensure that they have the opportunity to consider whether the contract should continue and, if not, to take the required action by that deadline.

- Does the contract renew on the same terms or do the parties have the opportunity to renegotiate any terms, in particular any fees that are charged? The parties should look to minimise the opportunity for disagreement at the point of automatic renewal. One way of doing this is to foresee changes within set parameters (e.g., allowing the DFS Provider to increase the fees in line with indexation or by no more than a fixed percentage), to limit the scope for negotiation. If the parties have an opportunity to renegotiate the terms on which the contract renews, build in sufficient time to allow for this process and address what happens if the parties cannot agree by the deadline (e.g., does the contract automatically terminate or does it automatically renew on the same terms?).

- Does the contract renew for the same period? For example, if the initial term of the contract is 24 months, does it renew for another 24 months or only for 12 months? The contract should be clear on this point to avoid disagreement over the contract term.

### 10.3 Availability and other SLAs

Each DFS Provider will need to consider if it is willing to give any service levels or undertakings in relation to the level of service (including availability of data via the API) and/or the quality of the data that it provides.

From the various standard API terms and conditions that have been reviewed as part of this project, the typical position is that API providers do not give any undertakings about the availability of their APIs or support for their APIs (e.g., no guarantees around bug fixing or response times). This is particularly the case where the DFS Provider is making the endpoints available at no charge to the TPSP. Further, the DFS Provider usually has broad rights to suspend access to the APIs, and excludes any liability for the APIs being unavailable. While this manages expectations and mitigates the DFS Provider's risk if it cannot provide a stable service, a lack of even basic SLAs – such as the core hours during which the TPSP can, with some certainty, expect the services to be available - could make the DFS Provider's services less attractive to TPSPs. The decision will depend also on the level of competition in the market, and whether the DFS Provider wants to encourage TPSPs to make use of its services in order to provide a richer set of services to the end customers. In this situation, the DFS Provider may view its APIs as another 'product', and look to compete with other DFS Providers in the market on the amount of information it makes available and the level of service it provides.

**Practical tip**

Common service levels that parties might consider are:

- the uptime of the APIs / when services and data will be accessible via the APIs and the downtime (availability);
- the time taken to provide the requested data;
- the level of support provided (e.g., the core hours of any support desk, response times to logged issues and/or fix times for resolving issues).

We would expect the service levels to apply only to a live environment, and not in a testing or sandbox environment.

In the EU, the European Banking Authority has set out minimum key performance indicators that ASPSPs should implement in respect of payment services[16]. The EBA's guidelines may be helpful to DFS Providers in other jurisdictions that are considering what minimum service levels might be appropriate in respect of their APIs. The key performance indicators include, amongst other things:

- The uptime and downtime per day of all interfaces.
- The daily error response rate.
- The daily average time (in milliseconds) taken, per request, to provide the account information requested or to provide all required payment data or to provide a confirmation in relation to card-based payments.

Also, in the EU, an ASPSP must provide the same level of availability, out of hours support and monitoring as provided by an ASPSP for the same service directly to customers through its own user interface (e.g., a bank must provide the same support and availability as it does in respect of its own website or mobile app). It must also have in place the same contingency plans. Under UK Open Banking, the following API provider service levels have been agreed for "Open Data":

- Each API endpoint must be available 95% of the time during each 24-hour period.
- Each API provider must comply with availability under a peak load of 500 requests per minute and under a load of 15,000 requests in an eight hour window, in each case across all of its open APIs for Open Data.

[16] European Banking Authority (December 2018), '*Guidelines on the conditions to benefit from an exemption from the contingency mechanism under Article 33(6) of Regulation (EU) 2018/389 (RTS on SCA & CSC)*', EBA/GL/2018/07

(c) **Other SLA considerations**

Other points that a DFS Provider should consider, if it is agreeing to meet minimum service levels:

- ***How will the SLAs be calculated?***

The calculation should take into account any allowed downtime or other situations in which the DFS Provider has to suspend access and will not be in breach of the SLAs (e.g., during any planned maintenance window, for emergency maintenance, or to address security concerns). Note that in the EBA's guidelines mentioned above, the EBA sets out that an ASPSP should count an interface as 'down' when five consecutive requests are not replied to within a total timeframe of 30 seconds (it does not matter if the requests are from one or multiple TPSPs).

- ***How will performance against the service levels be monitored and how frequently?***

Will the TPSP be able to monitor performance using the DFS Provider's resources (e.g., through its API portal) or will it be reliant on the DFS Provider reporting on performance? The DFS Provider may wish to report individually to TPSPs or to publish statistics on overall performance.

- ***What is the TPSP's remedy if the DFS Provider fails to comply with the SLAs?***

Will there be an impact on any fees payable, for example? Service credits or a fee reduction are common commercial options, but the DFS Provider will need to specify what level of service will trigger these (e.g., only if the availability is less than x% over a continuous period of 6 months or in any 4 out of 6 months).

10.4 **Data quality**

Where the DFS Provider is making data available to TPSPs, it needs to consider if that data is being provided 'as is' or if the DFS Provider is willing to accept any responsibility for the quality of the data.

Many DFS Providers will be unwilling to give any guarantees around data quality and will provide it 'as is', particularly if they are not charging for access to that data and/or the data could include any customer-generated data over which the DFS Provider has no control (e.g., personal notes or reminders). However, this approach may not be entirely acceptable to any TPSP that is paying for access to the APIs and needs to rely on access in order to provide a professional and reliable service to its customers.

If the DFS Provider is willing to accept an obligation in respect of data quality, it needs to consider what liability it is willing to accept if it breaches that obligation. For example, the DFS Provider may endeavour to ensure that any data generated by it is correct and free of errors, subject to any limitations that the DFS Provider needs to impose (e.g., that account information does not including any pending transactions or is only correct at a specified date and time). For the in-scope APIs under this note, the DFS Provider will want to accept no greater liability for incorrect information than it would have if the customer accessed the same incorrect information directly on the DFS Provider's mobile app or website and took action based on that information.

For other types of APIs, such as APIs providing access to customer identification or 'know your customer' information, the consequences of the TPSP relying on incorrect information could be considerable. In such cases, the DFS Provider would need to consider carefully the extent to which it is willing to accept any liability, but a TPSP may not accept that the DFS Provider has no responsibility to ensure the veracity and completeness of the data it provides.

Note that even if the DFS Provider seeks to exclude responsibility for data quality in the API Contract, local law may impose obligations on the DFS Provider in respect of personal data that it holds (e.g., an obligation to ensure that the customer data it holds is up-to-date and that it will delete any incorrect data where instructed by the customer). If the DFS Provider has failed to do so and passes on such incorrect data, the customer may have recourse against the DFS Provider for that failure. If the DFS Provider has an obligation under the API Contract to comply with applicable law and regulation in respect of customer data, it may also be liable to the API consumer for breach of contract.

10.5 **Protection of property**

When a DFS Provider starts opening up its APIs and data to third parties to use for their own products and services, there is a risk that those can be misappropriated or misused.

Intellectual property rights (IPR) around APIs is a complicated area, not least because different countries approach the protection of software differently. In the UK and EU, for example, copyright is the main form of protection for software, whereas in other jurisdictions (such as the USA) it might be possible to benefit from patent protection for software. Copyright only prevents the whole or a substantial part of the original software being copied; it does not stop someone from copying the underlying idea or replicating the software functionality without copying the code.

In addition to any rights the DFS Provider has at law to protect its assets, the API Contract should set out provisions dealing with the ownership and use of:

- the APIs, including the API specifications and any other supporting documentation that is made available;
- the data that is provided by the DFS Provider to the TPSP. However, it can become impossible to identify the sources of data once mixed with other data sets; and
- any derived data. For example, if they aggregate anonymised data across all of your customers or across the market and apply data analytics, do you have a right to receive those insights and use them for your own purposes? (see section 5.4)

In addition to the API Contract, there are practical points that a DFS Provider can consider:

- Are materials made available in a form that can be easily copied?
- How do you make your APIs and resources available to third parties - are these publicly available, or only available through a dedicated developer site or API portal that requires access controls provided and controlled by you? How much do you make visible? Can you track what materials have been accessed and downloaded by individual users?

- Through relationship management and/or monitoring the TPSP's activity in the market, you can keep track of what the TPSP is doing, including if they are expanding their services and using your data for purposes that you were not anticipating (and that is not permitted under the API Contract).

Note that if there is going to be any development work undertaken or collaboration between the DFS Provider and the TPSP, the API Contract should deal with ownership of any intellectual property rights that might arise from such collaboration or in any joint development.

10.6 **User API Contract**

The API Contract can be used to reallocate the risk of customer losses arising from activities that are within the TPSP's control (e.g., the TPSP can indemnify or reimburse the DFS Provider for any customer losses it incurs due to the TPSP's service failures).

However, the DFS Provider may want to go a step further and require the TPSP to explain the limits of the DFS Provider's responsibility to the customer. This could be in the form of agreed disclaimer wording that the TPSP must display to the customer, or a requirement that the TPSP will include particular provisions in its own customer terms and conditions. Such provisions might include:

(a) a provision around access to the service and warning against unauthorised use;

(b) a provision to ensure that the customer consents to its data being passed by the DFS Provider to the TPSP;

(c) (if applicable) a clear explanation of the consent procedure for payments and how consent can be withdrawn, as well as the point beyond which it cannot be withdrawn and any transactions that cannot be cancelled. The DFS Provider may also require TPSPs to make users aware of the dangers of authorised push payment (APP) fraud and other fraud, or it may itself wish to publicise such dangers to its customers;

**APP fraud**

Authorised push payment fraud, where a customer is tricked into making a payment or transfer to a fraudulent third party, is a problem because:

- a payment made in real time is irrevocable, and cannot be cancelled or reversed when the customer realises that he has been the subject of fraud; and

- the customer has consented to the payment and has likely gone through an authentication process – the instruction is "authorised" and the payment service provider will execute it on that basis.

(d) an explanation of the customer complaints process, clearly setting out who should be the first point of contact if any issues arise with the TPSP's services; and

(e) any disclaimer wording that the DFS Provider requires in respect of its liability for the TPSP services and the data provided by the DFS Provider. If the TPSP is providing financial data to the customer 'as is', the DFS Provider may be comfortable relying on the API Contract to ensure that the TPSP will not amend the DFS Provider's data in any way and will present the data to the customer with any disclaimer that the DFS Provider has included. However, the DFS Provider may want the TPSP to make clear in its customer terms and conditions that the DFS Provider will not have any liability for the TPSP's services, particularly if (i) the TPSP has access to raw data and will carry out any further processing of that data (e.g., it will combine the DFS Provider's data with other data before making it available to the customer) and/or (ii) the TPSP's services combine data gathered from other sources (e.g., through screen-scraping).

Security is not entirely the responsibility of the DFS Provider and the TPSP, and the parties may want to highlight to customers that they have a part to play in managing risk. This could include, for example, pointing out to the customer the importance of securing the device that they use to access payment services and of not sharing personal security credentials or access.

## APPENDIX: GLOSSARY OF TERMS AND ACRONYMS USED

| | |
|---|---|
| AISP | (specific term in PSD2) the provider of an account information service, a service that provides consolidated data on payment accounts to a customer and allows the customer to see all of its account information in one place. |
| API<br><br>or Application Programming Interface | 'an architecture that makes it easy for one application to "consume" capabilities or data from another application' (APIgee). It allows software programs to "talk" to one another, defining what information should be supplied and what actions will be taken when it is executed. |
| API Contract | the terms and conditions entered into by the DFS Provider and the TPSP under which the TPSP will have access to the open APIs. |
| API consumer | a third party service provider who wishes to access the DFS Provider's resources in order to provide its own services to the customer (also referred to in the note as a "**TPSP**"). |
| API Template | the template API terms and conditions made available by CGAP for use by DFS Providers. |
| APP fraud | authorised push payment fraud, where a customer is tricked - often by someone posing as their bank or other financial provider - into making a payment or transfer to a fraudster. |
| ASPSP | (specific term in PSD2) an account servicing payment service provider, e.g., a bank. |
| CMA | the UK Competition and Markets Authority, which is an independent non-ministerial department responsible for promoting competition for the benefit of consumers. |
| DFS Provider | a provider of digital financial services (e.g., banks, mobile network operators with a mobile money offering, FinTech wallet providers). |
| EBA | the European Banking Authority, an independent EU authority tasked with ensuring that EU rules are applied in the same way to financial institutions (e.g., banks, investment firms, payment providers, e-money providers) across the EU and that there is harmonised regulation and supervision of financial institutions across the EU. |
| EU | the European Union, consisting of 28 member states at the time of writing. |
| GDPR | the EU General Data Protection Regulation (2016/679/EU), which is available at: https://publications.europa.eu/en/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/language-en. |
| HKMA | the Hong Kong Monetary Authority, the government authority in Hong Kong that is responsible for maintaining monetary and banking stability. |
| OAuth protocol | OAuth is an open standard for access delegation. It is mostly used to enable one application to interact with another on a customer's behalf using an authorisation token (instead of disclosing a customer's password). |
| OBIE | the Open Banking Implementation Entity, the body responsible for the delivery of UK Open Banking. Further information can be found at: https://www.openbanking.org.uk/about-us/. |

| | |
|---|---|
| OTP | one-time password generated by a piece of software or by hardware, such as a token, text message (SMS) or push notification. |
| PCI DSS | the Payment Card Industry Data Security Standards, a set of security standards created to ensure that all businesses that process, store or transmit payment card data maintain a secure environment. If a business fails to comply with the PCI DSS, it may (amongst other things) have to pay a fine and lose its right to accept payment cards.<br><br>The PCI DSS is administered by an independent body made up of the major payment card brands (Discover, Visa, MasterCard, JCB and American Express), but the payment brands and acquirers are responsible themselves for enforcing compliance with the PCI DSS (PCIComplianceGuide.org). |
| PISP | (specific term in PSD2) a payment initiation service provider – a third party that can initiate payment transactions on behalf of a customer, allowing payments to be made directly from the customer's bank account through the service. |
| PSD1 | the EU Payment Services Directive (2007/64/EC), also referred to as the first Payment Services Directive, which is available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32007L0064&from=en. |
| PSD2 | the EU Payment Services Directive (2015/2366/EU), also referred to as the second Payment Services Directive, which is available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2366.<br><br>The Directive requires all payment account providers to let their customers share access to their payment accounts with third parties with the necessary permissions, but it does not specify the means of access or prescribe the scope of access in any detail. The Directive does not have direct effect in each EU member state, but each member state must implement its provisions into local law. |
| RTS | the regulatory technical standards on strong customer authentication and secure open standards of communication (Commission Delegated Regulation 2018/389/EU) which supplements PSD2 and is available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R0389.<br><br>The standards set out how the secure communication between ASPSPs and TPPs should happen. |
| sandbox | for APIs, this is a test environment for API developers. 'It mimics the characteristics of the production environment to create simulated responses for APIs that reflect the behaviour of a real system' (TechTarget). |
| SCA | (specific term used in relation to PSD2) strong customer authentication, an authentication based on the use of two or more elements - categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) - that are independent, in that the breach of one does not compromise the reliability of the other, and is designed in such a way as to protect confidentiality. See section 4.2(a) in the guidance note.<br><br>Further details can be found in the '*Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC*', (EBA-Op-2018-04), available at:<br><br>https://www.eba.europa.eu/documents/10180/2137845/Opinion+on+the+implementation+of+the+RTS+on+SCA+and+CSC+%28EBA-2018-Op-04%29.pdf |

| | |
|---|---|
| screen-scraping | the automated extraction of data or performance of actions that would usually be performed manually by a customer on a website. For example, screen-scraping can be used by a third party to access a customer's banking data by logging in to the bank's website on the customer's behalf using his or her log-in details. |
| SDK | a software development kit is a set of software tools made available by a hardware or software supplier that developers can use to integrate their own applications with that of the supplier. This allows developers to build an application without having to write everything from scratch. SDKs are usually comprised of APIs, sample code, and documentation. (WhatIs.com) |
| TPP | (specific term in PSD2) a third party provider who is an AISP or PISP, i.e. a third party provider with the relevant permissions to whom a bank or other account servicing payment service provider must provide access to in-scope data or services. |
| TPSP | a third party service provider who wishes to access the DFS Provider's resources in order to provide its own services to the customer (also referred to in the note as an "**API consume**r"). |
| UK Open Banking | an arrangement, mandated by the UK Competition and Markets Authority, under which the nine largest banks in the UK are legally required to make certain information widely available via open APIs. |