CGAP – API Template Terms and Conditions

**Assumption and Scope:**

1. This document has been drafted for the benefit of the Consultative Group to Assist the Poor ("**CGAP**") and is intended to be used as a template (the "**API Template**") for contracts regulating the provision of application programming interfaces ("**APIs**") by providers of digital financial services ("**DFS Providers**") to third party service providers ("**TPSPs**") ("**API Contracts**").
2. This API Template should be read alongside the note accompanying it (the "**Guidance Note**"). As with the Guidance Note, this API Template does not constitute legal advice in any jurisdiction or territory. A DFS Provider using the API Template will need to validate the options and recommendations against local law and regulation, to ensure that they are supported.
3. Hogan Lovells has sought to produce template terms and conditions that balance the interests of the Parties and, in as far as possible, achieve a fair and reasonable apportionment of risk and liability. As such, the API Template will not seek to entirely remove the liability of the DFS Provider. Each DFS Provider will need to assess whether the position reflected in the API Template is appropriate for the services that it is providing and the level of risk that it is willing to accept under its API Contract. The API Template is not a fixed standard and it is not exhaustive. Parties are free to add to it, or to move away from the recommended positions, in their own API Contract, and are advised to adapt these materials to cater for local market conditions and envisaged use cases.
4. The API Template has not been drafted for bespoke integration and therefore it does not cover any of the considerations that arise in relation to development work or collaboration effort. For example, it does not contain provisions for the testing and acceptance of deliverables or who owns the Intellectual Property Rights in any work product.
5. The API Template has been produced for the Payments API use cases and Customer Data API use cases set out and defined in Clause C of the Guidance Note. It does not specifically support access to KYC-as-a-service or other identity APIs.
6. The API Template assumes that all payments are initiated by the Customer, including where this is done under a mandate.
7. The API Template assumes that all Customer data is collected by the DFS Provider directly and that the DFS Provider will carry out Customer authentication on its own account. If the Parties wish to enter into an API Contract whereby:
   1. the TPSP is responsible for collecting the consent and/or authentication data, the API Contract should address the additional risk posed to the DFS Provider in accordance with 3.3(c) and/or 4.1(D) of the Guidance Note; and/or
   2. the TPSP is responsible for Customer authentication, the API Contract should address the additional risk posed to the DFS Provider in accordance with 4.3(i) – (iv) of the Guidance Note.
8. Each DFS Provider will need to amend the API Template to reflect:
   1. local law on the formation of contracts (i.e., the elements that must exist in order to form a binding contract, and any legal requirements that apply to the execution / signature of a contract), to ensure that the contract is binding between the Parties in their jurisdiction; and
   2. how it wishes to enter into terms and conditions with TPSPs. The API Template has been drafted on the basis that the terms and conditions will be physically signed by both Parties to the arrangement. DFS Providers may prefer that the TPSP "signs" the terms electronically, which could be done through the use of a digital signature, or deemed acceptance of the terms by accessing and using the open APIs, or any other method that is supported by local law.
9. Generally, DFS Providers will need to consider local law, regulatory requirements and applicable company standards and policies.
10. A DFS Provider should consider that the API Template will not always be the best means by which to protect itself from risk – often operational or technical measures might be taken to more effectively mitigate the risk which they are exposed to. DFS Providers should therefore consider the API Template in the context of the APIs and the TPSP Services as a whole and consider the various options available to it outside of its API Contract.

**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 Agreement is made on …………… ……………………………… 20[\*\*]

Between:

1. [\*\*\*], a company incorporated in [\*\*\*] with registered number [\*\*\*], whose registered office is at [\*\*\*] (the "**DFS Provider**"); and
2. **[\*\*\*].**, a company incorporated in [\*\*\*], registered number [\*\*\*], whose registered office is at [\*\*\*] (the "**TPSP**"),

each a "**Party**" and together the "**Parties**" (the "**API Contract**").

# Background

1. The DFS Provider is providing the TPSP with access to its application programming interfaces ("**APIs**") in order that the TPSP can make available the TPSP Services to the Customers, using the Customers' data where necessary.
2. This contract sets out the rights and obligations of each Party as they relate to the provision of the APIs.
3. The TPSP will put in place terms and conditions with the Customers directly in relation to the provision of the TPSP Services.

# Key Definitions

**"Active Session"** means a period of time commencing when a Customer correctly inputs its TPSP security credentials into the TPSP's System and is given access to the TPSP's Services until the same Customer either voluntarily logs out of the TPSP's System or is automatically logged out the due to the Maximum Session Time expiring;

**"APIs"** means the application programming interfaces set out in Schedule 3;

**"Applicable Data Protection Law"** means Applicable Law relating to privacy and the processing of personal data, as applicable to the Parties from time to time including:

[\*\*\*T*o be filled out with the data protection law of the particular jurisdiction in which the TPSP operates*\*\*\*]

"Applicable Law" means any of the following, to the extent that it applies to any person:

* + 1. any and all applicable laws, enactments, statutes, orders, rules, regulations, directives, ordinance or subordinate legislation, any exercise of prerogative and codes of conduct or regulatory policy, whether local, national, international or otherwise existing from time to time, together with any other similar instrument having legal effect in the relevant circumstances;
    2. decisions, orders, judgments and decrees of any relevant court, tribunal, Supervisory Authority or ombudsman; and
    3. any applicable direction, policy, rule or order that is given by a Supervisory Authority;

in each case as amended, supplemented, superseded or replaced from time to time

**"Business Day"** means a day (other than Saturday, Sunday or public holidays) on which the banks are open in [\*\*\*insert jurisdiction within which the TPSP operates\*\*\*] for the settlement of interbank operations and the setting of market indices;

**"****Charges"** has the meaning given to it in Clause 6 below;

**"Confidential Information"** means in relation to either the DFS Provider or the TPSP, all information used in or otherwise related to that disclosing Party's business, customers or financial or other affairs, in each case whether or not marked "Confidential", and any and all other information clearly designated as "Confidential" by the disclosing person, in each case existing in any form;

“Control” and derivatives thereof means, with respect to any entity,

(a) the direct or indirect ownership or control of more than 50 per cent. (%) of the (i) ownership interests or (ii) voting power at the general meeting or a similar body, of that person, or

(b) the right or ability to (i) appoint or remove or (ii) direct the appointment or removal of, such number of the members of the management board or a similar body of that person with decisive voting power in such body;

**"****Customer"** meansan individual who has an account with the DFS Provider and who has signed up to terms and conditions with the TPSP for use of the TPSP Services;

**"Customer Complaints"** means any complaint by a Customer of the TPSP Services with regards to the TPSP Services that is either lodged directly with the TPSP or directed to the TPSP by the DFS Provider or any Third Party;

**"DFS Provider's Services"** means the services provided by the DFS Provider to a Customer in accordance with its terms and conditions in place with that Customer outside of this API Contract;

**"Effective Date**" meansthe date on which the TPSP [provides a signed copy of this API Contract to the DFS Provider] OR [accepts this API Contract electronically by way of an electronic signature] OR [registers as a TPSP on the DFS Provider's website and receives confirmation from the DFS Provider that an account has been set up] OR [installs, copies or otherwise uses the API and therefore acknowledges that it has read, understood and agreed to be bound by this API Contract];

(NB: *DFS Provider should consider the method by which the TPSP will enter into this contract.)*

**"Eligibility Criteria"** meansthe specific criteria set out in the DFS Provider's onboarding process which tests 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, including but not limited to:

* + 1. the technicalities of the TPSP's solution;
    2. the TPSP's financial soundness;
    3. the TPSP's compliance with anti-money laundering regulation and that it is not named on any financial crime sanctions lists;
    4. whether the TPSP holds all necessary permissions or authorisations for the activities which it intends to carry out;
    5. the TPSP's security measures and operation and risk management controls, particularly in relation to personal data, including its cybersecurity policy, what monitoring it has in place and its data retention and destruction practices; and
    6. the TPSP's business continuity and disaster plans.

(NB: *The extent and scope of the due diligence carried out in relation to any TPSP should be proportionate to the risk attached to the relationship with the TPSP. The following factors should be considered in assessing the depth and scope of the process: the nature of the services to be carried out by the TPSP; how long the TPSP has been operating in the market; how and where the TPSP will be processing personal data; whether the TPSP's activities will be regulated within its market; and whether the TPSP will be sending messages via a* *Third Party's system.)*

**"Group"** means, in relation to a Party, that Party and any person which is from time to time a subsidiary undertaking of that Party, a parent undertaking of that Party and any other subsidiary undertaking of such parent undertaking;

**"****Intellectual Property Rights"** means

* + 1. copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in Internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information;
    2. applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction; and
    3. all other rights having equivalent or similar effect in any country or jurisdiction;

**"****Malware"** means any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence;

**"Maximum Session Time"** means [\*\* minutes]; (NB: *The length of time included here should reflect the maximum length of time for which the DFS Provider is comfortable allowing the TPSP to access Customer data. Local law and regulation should be checked to ensure there are no strict requirements related to this time period*.)

**"****Security Breach"** meansany unauthorised access, attempted unauthorised access or indication that there is a risk of unauthorised access to or interference with the systems or data owned, held or managed by either the DFS Provider or the TPSP by any Third Party or by a Party in breach of the terms of this API Contract;

**"****Security Requirements"** meansthose requirements listed at Schedule 1;

**"****Service Levels"** has the meaning given to it in Schedule 2;

"Supervisory Authority" means any local, national or multinational agency, department, official, parliament, public or statutory person or any government or professional body, regulatory or supervisory authority (including a supervisory authority under Applicable Data Protection Law), board or other body responsible (in the context in which such term is used) for regulating a Party and/or any matters relating to the performance by any Party of its obligations under this Agreement or for collecting, assessing or administrating Tax;

Tax" or "Taxation" means:

* + 1. all forms of taxation and statutory, governmental, state, federal, provincial, local government or municipal charges, duties, stamp taxes, imposts, contributions (but excluding social security contributions), levies, VAT, withholdings or liabilities wherever chargeable and whether in [\*\*\*insert jurisdiction in which the TPSP operates\*\*\*] or any other jurisdiction; and
    2. any penalty, fine, surcharge, interest, charges or costs payable in connection with any taxation within (a) above;

(NB: *The definition of* *Tax or Taxation should be checked with local counsel in the jurisdiction in which the TPSP is operating.)*

**"****Term"** has the meaning given to it by Clause 3.1;

"Third Party" means any person other than a Party to this API Contract, an employee, director, officer or agent of a Party to this API Contract or any tax authority;

**"TPSP Services**" meansthe services detailed by the TPSP during its onboarding process, which the TPSP intends to provide to Customers using the data or services accessed by the TPSP through the APIs; and

**"****TPSP's System"** meansthe hardware or software operated by TPSP in offering the TPSP Services.

# [Onboarding/Registration

*(NB: this Clause is only required if the API Contract is entered into before the TPSP has been accepted/has met the Eligibility Criteria.)*

* 1. As part of the TPSP's registration onboarding process with the DFS Provider, the TPSP will provide the following information to the DFS Provider on its request:
     1. [ ];
     2. [ ] (*NB: include documentation/information which the TPSP will need to provide – in some jurisdictions this will include evidence that the TPSP is regulated in its own right)*.
  2. The TPSP warrants and represents that all information and documentation it provides to the DFS Provider in respect of this Clause 2 will be complete and accurate in all material respects.
  3. On the basis of this information, the DFS Provider is satisfied that the TPSP has satisfied the Eligibility Criteria.
  4. If at any time the TPSP becomes aware of any change to the information or documentation it provided, any change to its status as a TPSP or ability to meet the Eligibility Criteria it must immediately inform the DFS Provider who may take any action it considers to be reasonably necessary which may include suspension or termination of the API Contract under Clause 15.]

# Access

* 1. Subject to Clause 2 above, the DFS Provider will provide the APIs to the TPSP in accordance with the terms of this API Contract from the Effective Date [for [\*\*\*] months] OR [until otherwise terminated in accordance with Clause 15 below] (the "**Term**") provided that:
     1. Unless otherwise stipulated in this API Contract, the TPSP will make the arrangements it requires to access the APIs;
     2. the TPSP continues to satisfy the Eligibility Criteria; and
     3. the TPSP will contract directly with the Customers with regards to the provision of the TPSP Services.
  2. The TPSP will during the Term make available to the Customers the TPSP Services.

# Availability/Service Levels

[The DFS Provider will provide access to the APIs on an 'as is' basis. The DFS Provider does not warrant that the APIs will be uninterrupted, timely, error-free or virus-free, nor does it make any warranty as to the results that may be obtained from using the APIs. [Subject to the foregoing, the DFS Provider will use its reasonable endeavours to prevent interruption to the access to the APIs as is reasonably practicable for it to do so.] The DFS Provider reserves the right to limit access to and/or use any API by various means and using various criteria.]

OR

[The DFS Provider agrees to provide access to the APIs at the Service Levels set out in Schedule 2 to this API Contract.]

(NB: *Each DFS Provider will need to consider if it can 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.*)

# Customer authentication and consent

* 1. On each occasion that it receives a call from the TPSP for Customer's data, the DFS Provider will authenticate each Customer and authenticate the TPSP.
  2. Once satisfied as to the identity of both the Customer and the TPSP, the DFS Provider will then provide the TPSP with the Customer data it requires in order to carry out the Customer's request for TPSP Services solely for the purposes of providing the Customer with the TPSP Services.
  3. When the TPSP receives the Customer data, it will provide the Customer with the TPSP Services the Customer requested.

# Charges

[To be completed by DFS Providers.] ***(****NB: any fees, royalties or other financial remuneration and risk on each side will need to be included in these Terms.****)***

# Data access

* 1. The DFS Provider will obtain the express consent of the Customer that the Customer's data will be disclosed to the TPSP through the APIs when required by the TPSP so that it can operate the TPSP Services.
  2. The DFS Provider will provide Customer data to the TPSP via the APIs in accordance with 7.3 and 7.4 below.
  3. The TPSP will [only] have access to Customer data during an Active Session. The TPSP will only be provided with the Customer data which is necessary in order to provide that Customer with the TPSP Services being requested via the APIs.
  4. [The TPSP will also have access to Customer data outside of an Active Session provided that:
     1. the Customer was informed of the data to which the TPSP would have access at the point that it entered into a contract with the TPSP;
     2. the TPSP will only access Customer data a maximum of [four (4)] times in any twenty-four (24) hour period;
     3. the amount of any transaction authorised by the TPSP outside of an Active Session must be notified to the Customer in advance and confirmed to the Customer afterwards, and if the amount of the transaction exceeds the amount notified to the Customer, the TPSP will be liable to refund the amount to the Customer;
     4. the maximum amount of any one transaction authorised by the TPSP outside of an Active Session is [\*\*\*] and the maximum aggregate amount of any transactions authorised by the TPSP outside of an Active Session and in any one 24 hour period is [\*\*\*]; and
     5. the TPSP will not change any feature of a variable recurring payment without the prior consent of the Customer.]

# Data Obligations

* 1. [The Customer data provided by the DFS Provider to the TPSP is provided on an 'as is' basis and no assurance is given by the DFS Provider as to its accuracy or completeness.] OR [The DFS Provider will endeavour to ensure that the Customer data provided by the DFS Provider to the TPSP under this Clause 8, will be the data that was requested by the TPSP and will be as far as possible without material error.]
  2. The DFS Provider and the TPSP will only process Customer data in compliance with Applicable Data Protection Law.
     1. The TPSP will use and secure all data provided by the DFS Provider in compliance with the Security Requirements.
     2. 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 providing the TPSP Services to the Customer.
     3. Any data transmitted to or accessed by the TPSP for the purposes of providing the TPSP Services to the Customer, is licensed to the TPSP on a non-exclusive, non-transferrable basis and only for the purposes for which the TPSP requires the data under the API Contract.

(NB: *As law and best practices on the protection of personal data vary considerably between jurisdictions, and the law will impact what must be included in the API Contract to protect* *Customers, the API Contract deals with data protection only at a principles level.*)

(NB: *Further to the above* *terms, if the TPSP 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 data is being provided and that the DFS Provider takes no responsibility for the aggregation of that data or any outputs which stem from it.*)

# Intellectual Property

* 1. Except as expressly set out in these Terms or as otherwise agreed in writing between the Parties:
     1. the TPSP shall not acquire any right, title or interest in or to the Intellectual Property Rights of the DFS Provider or its licensors; and
     2. the DFS Provider shall not acquire any right, title or interest in or to the Intellectual Property Rights of the TPSP.

# Licences

* 1. The DFS Provider grants a non-exclusive, non-transferable licence to the APIs to the TPSP to the extent required for the TPSP to provide the TPSP Services to the Customers on the basis that the TPSP complies with any restrictions placed on its use of the APIs under this API Contract. (NB: *If the DFS Provider is receiving the API by way of a licence from a* *Third Party, this licence should not go further than that originating licence.*)
  2. The DFS Provider grants to the TPSP a non-exclusive, non-transferable licence to the data it provides to the TPSP for the purposes of providing the TPSP Services under this API Contract, on the basis that the TPSP complies with any restrictions placed upon its use of the data under this API Contract.
  3. [The DFS Provider grants to the TPSP a non-exclusive, non-transferable licence to the DFS Provider's brand, including [\*\*\*state details of any specific logos, trade marks, names, domain names, imagery etc.\*\*\*] for the purposes of providing the TPSP Services to the Customers [and only in line with the DFS Provider's brand guidelines available at [\*\*\*]] and seeking sign-off on the use of the brand before live use.]
  4. Where the API Contract is terminated or suspended either under Clause 15 of this API Contract or otherwise, the licences contained within this Clause 10 will be similarly terminated or suspended.

# Confidential information

* 1. Both Parties will use at least the same degree of care, to safeguard the Confidential Information of the other Party as it employs with respect to its own Confidential Information of a similar nature.
  2. Neither Party will disclose or use any such Confidential Information other than in connection with, and only to the extent necessary for the performance of its obligations under, or to exercise any rights of licences granted by, this API Contract.
  3. Subject to Clause 11.4, neither Party will disclose any of the terms of this API Contract which are Confidential Information to any other person without the prior written consent of the other Party.
  4. Both Parties may disclose Confidential Information:
     1. if and to the extent required by Applicable Law or for the purpose of any judicial proceedings;
     2. if and to the extent required in referring a dispute for resolution pursuant to Clause 21;
     3. to its professional advisers, auditors (and their advisers) and lawyers; and
     4. if and to the extent the information has come into the public domain through no fault of that Party.
  5. Notwithstanding the expiry or early termination of this API Contract, the provisions of this Clause 11 will continue to apply to each Party without limit in time.
  6. The text of any press release or other communication made by either Party to be published by or in the media concerning the subject matter of these Terms will require the approval of both Parties.

# Security

* 1. Both Parties will:
     1. be responsible for the security of its own system;
     2. not knowingly transmit any Malware through the use of the APIs or introduce Malware into any data or message sent to the other Party or into the other Party's system;
     3. use commercially available and current scanning tools (in line with good industry practice) to scan for Malware.
  2. The TPSP is responsible for putting in place measures to ensure the security of Customer data and of the TPSP Services, including by complying with the Security Requirements at all times during the Term and for not allowing unauthorised individuals to access and use the DFS Provider's APIs and data via the TPSP's System.
  3. On request from either Party, the non-requesting Party will provide information evidencing its compliance with this Clause 12.
  4. On the occurrence of a Security Breach, the TPSP must notify the DFS Provider as soon as reasonably practicable and in any case within forty-eight (48) hours of the TPSP becoming aware of the Security Breach and provide the DFS Provider with all the information it has available to it regarding the data affected by the Security Breach.

(NB: *We have not included a business continuity plan within these security provisions but there may be circumstances in which such a plan is required by the TPSP under its regulatory obligations. In this instance we would recommend consulting with local counsel to assess what is required to fulfil these requirements. Please also refer to section 9.3 of the Guidance Note which advises on the use of 'screen-scraping' as a method of business contingency planning and the risks which the DFS Provider should mitigate where 'screen-scraping' is allowed under the API Contract.)*]

# Technical standards

[ NB: *Refer to a schedule or to the DFS Provider's technical specifications*.]

# Liability

* 1. The TPSP will be responsible for the TPSP Services that it provides to the Customers and for its use of the Customer data provided to it by 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.
  2. The TPSP will be responsible for using the APIs and the Customer's data in accordance with this API Contract, the scope of the Customer's consent, and Applicable Data Protection Law. This will include:
     1. only using data for the purposes disclosed to the DFS Provider and permitted by this API Contract and the scope of the Customer's consent; and
     2. only accessing (and attempting to access) those resources which are within the scope of the Customer's consent and to which it has been granted access permission.
  3. The DFS Provider will be responsible for authenticating the TPSP when it makes a call for Customer data, enforcing any access permissions, and ensuring that it only provides the TPSP with the data and access requested and no more.
  4. The DFS Provider will be responsible for authenticating Customers in accordance with Clause 5 above, ensuring that payments are only processed when they have been instructed by the Customer and that payment instructions issued by users which have failed the authentication process are rejected.
  5. 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 misconduct of the TPSP's personnel.
  6. The DFS Provider will be responsible for a deficiency in the execution of a payment transaction due to its fault or negligence. The TPSP will be responsible for a deficiency in the execution of a payment transaction due to its fault or negligence.
  7. 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 but not limited to fraud, misuse of the APIs, any misrepresentation of the DFS Provider's products and services, any Security Breach, or persistent poor service to Customers.
  8. The TPSP will ensure that it has in place adequate insurance to cover its entire liability under the API Contract at all times during the Term.
  9. Nothing in this Agreement will exclude or limit the liability of:
     1. either Party for death or personal injury resulting from the negligence of that Party or any of its officers, employees or agents;
     2. either Party for fraud, gross negligence or wilful misconduct; or
     3. the TPSP in respect of sums payable under Clause 6.
  10. Subject to this Clause 14, no Party will be liable to any other Party under or in connection with this API Contract (whether in contract, tort (including negligence) or breach of statutory duty or otherwise) for:
      1. any loss of profit, interest, goodwill, production, business opportunity, business (including loss of contracts), revenue and/or anticipated savings; and/or
      2. indirect, special, punitive or consequential losses,

even if such losses were foreseeable and notwithstanding that a Party had been advised of the possibility that such losses were in the contemplation of the other Party or any Third Party.

* 1. The total aggregate liability of the TPSP to the DFS Provider (whether in contract, tort (including negligence) or breach of statutory duty or otherwise) for any event of series of connected events under or in connection with this API Contract, in each year of the Term, for any loss or damage of whatsoever nature and howsoever caused will be limited to and in no circumstances will exceed [100% of the total Charges paid or payable by the TPSP to the DFS Provider in such year of the Term].
  2. The DFS Provider will not be liable or in breach of this Agreement for:
     1. any breach by the DFS Provider of this API Contract or failure by the DFS Provider to provide the APIs to the extent that such failure is caused by any failure of the TPSP to comply with the TPSP's obligations under this API Contract;
     2. any loss or damage whatsoever caused directly or indirectly by the acts or omissions of any TPSP personnel or any Third Party engaged by the TPSP to receive services under this API Contract; or
     3. any loss of access to the APIs or inability to provide the TPSP Services caused by any incompatibility between the TPSP's System and the APIs.

[NB: *Local law may influence what losses can and cannot be recoverable under a contract and there may be specific types of loss that cannot be excluded or limited. The clauses above reflect the English law position with regards exclusion of losses. Liability will also depend on who is responsible for what activity and this may differ across agreements. DFS Providers need local counsel advice and to consider the specific use in their circumstances.*]

# Termination and Suspension of the Services

* 1. The DFS Provider has the right to terminate the TPSP's access to the APIs if it has reason to believe that:
     1. the TPSP no longer fulfils the Eligibility Criteria;
     2. the TPSP has breached any of the conditions of Clause 5;
     3. the TPSP is using the APIs for purposes not disclosed to the DFS Provider during the onboarding process;
     4. the TPSP declares or acknowledges that it is insolvent or unable to pay its debts as they become due or upon the filing of any proceeding for bankruptcy;
     5. the TPSP introduces Malware into, or otherwise disrupts or attempts to disrupt the DFS Provider's systems;
     6. [there is a change in Control of the TPSP in favour of a competitor of the DFS Provider;]
     7. the TPSP offers the TPSP Service or conducts itself in a manner that causes damage to the DFS Provider's reputation, either with the Customers or with the market more widely, including but not limited to regulators; or
     8. the TPSP has used the APIs other than as permitted by Clause 3 or the Customer data other than as permitted by Clause 7;
  2. The DFS Provider has the right to suspend the TPSP's access to the APIs in circumstances where:
     1. it has the right to terminate the APIs under Clause 15.1 of this API Contract;
     2. emergency maintenance needs to be carried out;
     3. there is an actual or suspected Security Breach by the TPSP;
     4. there is an actual or suspected breach of this API Contract by the TPSP;
     5. the TPSP suffers a Security Breach or other unauthorised access to the systems through which either the APIs are accessed or the Customers use the TPSP Services;
     6. 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 Breach; or
     7. where the DFS Provider has any other reasonable grounds for such suspension.
  3. The DFS Provider will notify the TPSP of its intention to terminate access to the APIs in accordance with 15.1 or suspend access to the APIs in accordance with 15.2, [\*\*\*] Business Days before the respective termination or suspension (**a "Notice of Intention**"). Should the TPSP remedy the grievances of the DFS Provider before the expiry of the Notice of Intention, the DFS Provider at its own discretion may withdraw the Notice of Intention and continue to provide access to the APIs.
  4. If a Notice of Intention to suspend the API Contract expires without adequate remedy, the DFS Provider will suspend access to the APIs by the TPSP and the TPSP will not be entitled to exercise any of its rights under this API Contract and the licences granted in Clause 10 will also be suspended.
  5. Once a period of suspension begins, the DFS Provider will as soon as reasonably practicable send a further notice to the TPSP detailing the reason for suspension, whether it deems the TPSP to be at fault, and, if it does consider the TPSP to be at fault, a reasonable time period for correction by the TPSP. If the TPSP does not remedy the situation to a standard sufficient to the DFS Provider, the DFS Provider may at its own discretion terminate the API Contract in accordance with 15.1 and 15.3 above. If the reason for the suspension either ceases to exist or is sufficiently remedied by the TPSP, the DFS Provider will reinstate the APIs as soon as reasonably practicable henceforth.
  6. The DFS Provider has the right to refuse to action an instruction, such as a payment instruction, which reasonably causes the DFS Provider to be suspect a fraudulent transaction or to be concerned about the security of the APIs or the Customer data. In such a case, the DFS Provider should as soon as reasonably possible after the action is requested, provide notice to the TPSP that it will not carry out such an action.
  7. Notwithstanding term in this Clause 15, the DFS Provider's obligation to provide notice shall not apply in any case of security incidents, data breaches, emergency incidents or where the DFS Provider reasonably considers that any delay in suspending the APIs would cause the DFS Provider to be in breach of Applicable Law.

# Consequences of Termination

* 1. On termination or suspension of this API Contract, the TPSP will no longer have any rights to access the APIs or the Customer data.

# Warranties

* 1. The TPSP warrants, represents and undertake to the DFS Provider that:
     1. it has the necessary rights to perform its obligations under the API Contract;
     2. it has full legal authority to enter into the API Contract;
     3. it will maintain all legal or regulatory permission or authorisations it needs in order for it to provide the TPSP Services to the Customers;
     4. it will notify the DFS Provider if its circumstances change such that it does not or in the future will not fulfil the Eligibility Criteria;
     5. all information provided by or on behalf of the TPSP to DFS Provider is accurate and complete; and
     6. each representative of its operational team, and each representative of its senior management to whom disputes are to be referred pursuant to the dispute resolution procedure under Clause 21 has full authority to bind such TPSP in relation to any dispute referred to such representative.
  2. The DFS Provider warrants, represents and undertakes to the TPSP that:
     1. it has the necessary rights to perform its obligations under the API Contract; and
     2. it has full legal authority to enter into the API Contract.
  3. To the fullest extent permitted by law, and unless expressly set out to the contrary in the API Contract, all warranties and terms which would otherwise be implied by law, custom or usage are excluded from the API Contract.
  4. [All access to the APIs is made available to TPSPs by the DFS Provider on a continuous basis and all Customer data provided through the APIs shall be as accurate, comprehensive and up to date as reasonably practicable.] OR
  5. [The DFS Provider does not guarantee that access to the APIs will be continuously available for use or without inaccuracy or defect. The TPSP agrees that access to the APIs is at its sole risk.]

# Indemnities

* 1. The TPSP agrees to indemnify the DFS Provider and hold it harmless from and against any and all claims, losses, demands, actions, suits, proceedings, damages and costs arising directly or indirectly out of or in connection with:
     1. a material breach of the TPSP under this API Contract;
     2. a breach by the TPSP of the data protection provisions;
     3. any failure to provide the TPSP Services or any claims made by Customers in relation to the TPSP Services;
     4. any payment error or duplication error made by any bank;
     5. fraudulent, negligent or improper actions wholly or partially attributable to the act or acts of the TPSP; and
     6. any taxes, duties, or other charges which are or may be imposed in the DFS Provider in connection with this API Contract.

# Sub-Contracting

* 1. The API Contract is personal to each of the Parties. No Party other than the DFS Provider may assign, novate or transfer in any way, or charge the benefit of, any of its rights, liabilities or obligations under the API Contract on a temporary or permanent basis to any Third Party.

# Variations

* 1. Any changes which the DFS Provider will make to the APIs or their specifications will be communicated to the TPSP [directly by email to the TPSP's Service Manager] OR [via the DFS Provider's [website]/[API Portal] which can be found at [\*\*\*]].
  2. The DFS Provider will give the TPSP [\*\*\*] Business Days' notice prior to making any changes to the APIs or their specifications, save in any case of security incidents, data breaches, emergency incidents or where the DFS Provider reasonably considers that any delay in suspending the APIs would cause the DFS Provider to be in breach of Applicable Law.

# Service Managers and Dispute Resolution Procedure

* 1. The DFS Provider and the TPSP will each appoint appropriate representatives who will be the key points of contact for any matters relating to this API Contract or the provision of the APIs (the "**Service Managers**").
  2. The Service Managers will meet regularly to discuss any Customer Complaints as received by the TPSP. The DFS Provider's Service Manager will have the right to request any further information about the Customer Complaints or their handling by the TPSP. Should the TPSP consider that a Customer Complaint is the result of an act or omission by the DFS Provider, the Service Manager for the TPSP should share this with the Service Manager for the DFS Provider as soon as reasonably practicable.
  3. If a dispute arises between the Parties in relation to the performance of their respective obligations under this API Contract, [including in regards to the provision of the APIs in line with the Service Levels,] the Service Managers will discuss the dispute, in good faith, and each use their respective reasonable efforts to resolve the matter in dispute within [\*\*\*] days. Either Party may request a copy of the data held by the other for the purposes of resolving the dispute. If the dispute cannot be resolved between the Service Managers, either Party may escalate the dispute to [\*\*\*] for the DFS Provider and [\*\*\*] for the TPSP who shall meet to try to resolve the matter within [\*\*\*] days.
  4. Failing resolution under 21.3 above, the Parties will be required to refer the dispute to an alternative dispute resolution forum, the specific procedure to be decided between the Parties.
  5. For the purposes of this API Contract the Service Managers are as follows:

|  |  |
| --- | --- |
| DFS Provider | |
| Name: |  |
| Address: |  |
| For the attention of: |  |
| Email: |  |
| TPSP | |
| Name: |  |
| Address: |  |
| For the attention of: |  |
| Email: |  |

# Force Majeure

* 1. A Party will not be responsible for any delay in performing or failure to perform any of its obligations under the API Contract if and to the extent that the delay or failure directly results from a failure of another Party to perform its obligations in accordance with the API Contract.
  2. The DFS Provider shall not be in breach of the API Contract if such delay or failure results from events, circumstances or causes beyond its reasonable control.

# Governing Law

# Each Party agrees that the API Contract and relationship between the Parties will be exclusively governed by and interpreted in accordance with [\*\*\*] law and that all disputes arising out of or in connection with the API Contract and/or the DFS Provider's APIs and/or the relationship between the Parties in relation to the subject matter of the API Contract (in each case whether or not regarded as contractual claims) will be exclusively governed by and determined in accordance with [\*\*\*] law and (subject to the dispute resolution procedure) each Party expressly and irrevocably submits to the exclusive jurisdiction of the [\*\*\*] Courts in relation to all such disputes and any other claim or matter arising under or in connection with the API Contract.

# Entire Agreement

* 1. Notwithstanding any entire agreement provisions in any (current or future) agreement between any two or more of the Parties, the API Contract constitutes the entire agreement and understanding between the Parties in respect of the matters dealt with in it and supersedes any previous agreement between the Parties or any of them relating to such matters notwithstanding the terms of any previous agreement or arrangement expressed to survive termination.
  2. Each of the Parties represents and agrees that in entering into the API Contract it does not rely on, and will have no remedy in respect of, any statement, representation, warranty or understanding (whether negligently or innocently made) of any person (whether a Party or not) except as expressly set out in the API Contract. The only remedy available to any Party for breach of the warranties will be for breach of contract under the terms of the API Contract. No Party will be entitled to rescind the API Contract (except for fraudulent misrepresentation).

(*NB: these* *terms and conditions will replace any existing* *terms and conditions between the Parties relating to the same subject matter (e.g., if the Parties have already signed* *terms and conditions relating to the sandbox, or already have an agreement under which the TPSP passes payment instructions to the DFS Provider). Parties should consider the interaction with any existing agreements between the Parties. If any existing agreements need to remain in force, the Parties can either delete this clause or state that the existing agreements are excluded from the clause.*)

Signed by )

[\*\*\* NAME OF TPSP \*\*\*] )

)

Acting through Name:…………………………………………………

Job title:………………………………………………

Schedule 1

Security Requirements

(NB: *DFS Provider to include a list of* *security requirements or reference to its specific security policy. At a minimum we recommend that the following are required:*

* *a secure connection must be established before data is transferred;*
* *each Party will be responsible for the security of its own system;*
* *each Party will agreed not to 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;*
* *each* *Party will use commercially available and current scanning tools (in line with good industry practice) to scan for* *Malware;*
* *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*
* *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 System.*

*Local law and regulation may impose* *security requirements on the Parties and these should be considered when completing this Schedule.)*

[Schedule 2

* 1. Service Levels

(NB: *DFS Provider to provide the levels of service it intends to meet in providing access to the APIs. Service Levels can be measured by:*

* *a minimum level of uptime (e.g. 95%)/maximum level of downtime per day across all interfaces;*
* *a daily error response rate;*
* *the daily average time 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. (e.g. compliance 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 APIs.)*

*When calculating Service Levels, the DFS Provider should take into account any 'allowed downtime' or other situations in which the DFS Provider has to suspend access without being in breach of the Service Levels.*

*The DFS Provider should also consider how service will be monitored and how frequently. It should further consider whether the TPSP will have a remedy where the Service Levels are not met and what that remedy should be.)*]

1. Schedule 3
   1. Application Performance Interfaces

[DFS Provider to include details of the APIs being offered to the TPSP.]