Card Processing Agreement

**Schedule 7 – Fraud Transaction Monitoring and Scam Transaction Monitoring**



**This Schedule 7 is incorporated into the Card Processing Agreement and applies to Fraud Services and Scam Transaction Monitoring only. The applicability of the terms of this Schedule 7 is dependent on the Client’s use of SaaS (including but not limited to whether the Client is permitted by THREDD to use UI, create rules, and change configurations). For the purpose of this Schedule, references to THREDD shall include its authorized subcontractor Featurespace.**

**This Schedule is incorporated into the Card Processing Agreement and does not replace or amend the Card Processing Agreement,** **which shall continue in effect according to its terms. Terms that are not defined in this Schedule have the meaning given to them in the Card Processing Agreement.**

**Part 1 – Fraud Transaction Monitoring**

Part 1 of this Schedule shall apply to the services set out in clause 1.3 of Part 1 only unless explicitly stated.

**Agreed Terms**

1. **Definitions and interpretation**
	1. In this Schedule the following definitions apply:
		1. **BASE SOFTWARE** means the proprietary software programs of Featurespace known as ARIC which is provided on the SaaS;
		2. **CARD PROCESSING AGREEMENT** means the agreement entered into by the Client and THREDD, as amended by the parties from time to time.
		3. **CUSTOMER FRAUD ALERT** means a communication sent from THREDD to the most recent phone number or email address held on THREDD database for the relevant Cardholder, as further described in Schedule 2.
		4. **ENHANCED FRAUD TRANSACTION MONITORING** means the enhanced version of the product which may be supplied to the Client under this Schedule, as further described in Schedule 2.
		5. **ENHANCED FRAUD TRANSACTION MONITORING MANAGED SERVICE** means the service inclusive of Customer Fraud Alerts, Sandbox Replay and Enhanced Fraud Transaction Monitoring, which is managed by Thredd, as further described in Schedule 2.
		6. **FRAUD ALERT** means an alert triggered by the Fraud Rules, which may result in a Customer Fraud Alert being sent by THREDD.
		7. **FRAUD RULES** has the meaning given to it in clause 2.2.
		8. **FRAUD TRANSACTION MONITORING** means the baseline version of the product which may be supplied to the Client under this Schedule, as further described in Schedule 2.
		9. **FRAUD TRANSACTION MONITORING MANAGED SERVICE** means service inclusive of Customer Fraud Alerts, Sandbox Replay and Fraud Transaction Monitoring, which is managed by Thredd, as further described in Schedule 2.
		10. **HOSTING SERVICES** means the SaaS and associated services related to Featurespace’s provision of the SaaS for Client access to and use of the SaaS.
		11. **LOCAL RESTRICTIONS** has the meaning given to it in clause 3.3.
		12. **REGULATIONS** means all relevant laws, statutes, statutory instruments, acts, regulations, orders, and directives issued by government agencies, self-regulatory bodies, trade associations or industry bodies (whether or not having the force of law) applicable to the conduct of the business of the Client or THREDD or in connection with their rights and obligations under this Schedule.
		13. **REPRESENTATIVE** means all employees, temporary staff, independent contractors, part-time staff, call centre operatives, marketing and sales personnel, agents, representatives and all other people, in each case retained by or otherwise working under the direction of any member of either Party.
		14. **SAAS** means the Base Software, hardware, third party software, networks, and peripherals used by Featurespace, or its third-party cloud platform provider AWS, to provide the Hosting Services.
		15. **SANDBOX REPLAY** means the feature which allows users to test the effects of changes made to analytics in the staging environment, as further described in Schedule 2.
		16. **FRAUD SERVICES** has the meaning given to it in clause 1.3.
	2. This Schedule is incorporated into the Card Processing Agreement and does not replace or amend the Card Processing Agreement, which shall continue in effect according to its terms. Terms that are not defined in this Schedule have the meaning given to them in the Card Processing Agreement.
	3. The services governed by this Schedule are as follows (“Fraud Services”):
		1. Fraud Transaction Monitoring
		2. Fraud Transaction Monitoring Service
		3. Enhanced Fraud Transaction Monitoring
		4. Enhanced Fraud Transaction Monitoring Service
		5. Sandbox Replay
		6. Customer Fraud Alerts
2. **Fraud Transaction Monitoring Service and Enhanced Fraud Transaction Monitoring Service**
	1. The provision by THREDD of the Fraud Services is dependent upon the Client providing such details to THREDD as THREDD may reasonably require in order to provide the Service, including but not limited to Cardholder contact details (including but not limited to most recent mobile phone number and/or email address).
	2. The Client is solely responsible for providing and approving its fraud monitoring rules to increase fraud monitoring efficiency (“Fraud Rules”). THREDD shall configure and test Fraud Rules before submitting to the Client for approval.
	3. The Client is solely responsible for its choice of Fraud Rules and shall review and update its Fraud Rules from time to time at its discretion. The Client shall ensure that any changes to Fraud Rules are communicated to THREDD via the THREDD jira application. THREDD is not responsible for any delay or result of Client’s failure to correctly configure Fraud Rules.
	4. Subject to Client providing notice of changes in Fraud Rules in accordance with clause 2.3, THREDD shall update the Fraud Rules within 48 hours of receipt. THREDD shall only carry out Customer Fraud Alert based on the Fraud Rules provided and configured by the Thredd in accordance with clause 2.3.
	5. Where it is reasonably necessary to enable THREDD to deliver, provide or maintain the Fraud Services (including any associated equipment or infrastructure) in accordance with this Agreement, the Client will allow or arrange for THREDD and THREDD Representatives to have access to any systems, networks or other facilities of the Client’s or that are operated on the Client’s behalf with the Client’s consent. This access will be subject to the Client’s normal security and access procedures as notified to THREDD.
	6. THREDD reserves the right to implement changes to Fraud Services at any time at its sole discretion. In such circumstances, THREDD will use reasonable endeavours to provide as much advance notice as possible of any such changes but is not bound to do so if to do so is not reasonably practicable.
	7. Except to the extent expressly set out in this Schedule, no conditions, warranties or other terms apply to the Fraud Services.
	8. Without prejudice to any of THREDD’s other rights under this Schedule, the Client agrees that THREDD may, at any time for the purposes of transaction monitoring, capacity planning and for analytical purposes, monitor any and all data that relates to the Client’s use of the Fraud Services.
3. **Customer Fraud Alerts**
	1. The Client acknowledges that if a valid mobile phone number or email address is not provided to THREDD for Cardholders it will not be possible for THREDD to send the relevant Customer Fraud Alert.
	2. The Client shall work with THREDD to populate predefined templates for Customer Fraud Alerts.
	3. The Client acknowledges that where countries have local restrictions on 2-way SMS or a country is sanctioned (“Local Restrictions”) it will not be possible for THREDD to send the relevant Customer Fraud Alert. THREDD shall not be liable for any failure to send a Customer Fraud Alert to a Cardholder affected by Local Restrictions.
	4. The Client shall use best endeavours to assist THREDD in the delivery of the Fraud Services and will respond to all requests for assistance in a timely and professional manner.
	5. With the exception of anything that is expressly specified in this Schedule as being supplied, provided, installed or implemented by THREDD in relation to the Fraud Services, the Client will supply, provide, install and implement (or arrange for the supply, provision, installation or implementation) any hardware, software, network and telecommunications systems, cards and any other facilities or services that might be necessary to enable the provision of the Fraud Services.
4. **Use of the Fraud Services**
	1. The following clauses relate to use of the SaaS:
		1. The Client consents to the use of its data and outputs on the SaaS to be used by THREDD for the delivery of SaaS for the Client and Client’s Affiliates, including for support, testing, and development of patches, fixes, improvements, and functionality to be used within SaaS during the Term. The Client is responsible for promptly obtaining and providing to THREDD all required consents necessary so that THREDD can provide access, use, and/or modify your data for the operation and improvement of the SaaS.
		2. THREDD may monitor the Client’s use of the SaaS and collect and compile aggregated statistics. The Client acknowledges that THREDD may compile aggregated statistics based on the Client’s data input into the SaaS. The Client agrees that THREDD may use aggregated statistics to the extent and in the manner permitted under applicable law; provided that such aggregated statistics do not identify the Client or the Client’s Confidential Information or personal data.
	2. The following clauses relate to use of user Interface and case manager:
		1. The Client is responsible for ensuring that all access credentials provided to the Client are kept confidential. Access credentials are for the Client’s internal use only and may not be shared, sold, disclosed, transferred or sublicensed to any other entity or person. The Client will be deemed to have taken any action that the Client or the Client’s authorised users permits, assists or facilitates any person or entity to take related to use of or access to the SaaS using the access credentials. The Client is responsible for authorized users’ use. If any authorized user no longer requires access to the system or violates the Client’s obligations, the Client must immediately notify THREDD so that THREDD may suspend such user’s access rights.
		2. THREDD may temporarily suspend any authorized user’s access to any portion or all of the SaaS if: (i) THREDD reasonably determines that (A) there is a threat or attack on any Intellectual Property Rights of the system; (B) any authorized user’s use of the system disrupts or poses a security risk to the system or hosted environment; (C) authorized user is using the system for fraudulent or illegal activities; THREDD will use commercially reasonable efforts to provide written notice of any service suspension to an authorised user and to provide updates regarding resumption of access to the SaaS following any service suspension. THREDD shall use commercially reasonable efforts to resume providing access to the SaaS as soon as reasonably possible after the event giving rise to the service suspension is cured. THREDD will have no liability for any damage, liabilities, losses, or any other consequences that you or any authorized user may incur as a result of a service suspension.
	3. The following clauses relate to creating, modifying rules, models, and configurations:
		1. Legal remedies for failure to meet THREDD’ obligations and service levels do not apply to any customizations or changes the Client makes, including new rules, decorations, third party call-outs, and configurations. The usage of this ability to customize functionality may impact the performance or results of the SaaS. Support for customizing functionality, rules, and models created by THREDD may be provided on a time and materials basis, and only after prior written agreement by each of THREDD.
		2. THREDD does not warrant the performance of your custom configurations, rules, third-party call-outs, decorations, and/or models, nor that such additions or configurations will be fit for any particular purpose.  The Client is responsible for the security and integrity of any items uploaded into the SaaS, and any changes to the SaaS the Client make, unless it is provided by THREDD. THREDD highly recommends the Client shall have appropriate anti-virus and malicious code scanning tools in place for models and third party content uploaded or connected to the SaaS.
	4. The Client acknowledges and agrees that the Service Levels in Schedule 4 of the Card Processing Agreement do not apply to Fraud Services provided under this Schedule.
	5. Sandbox Replay shall only allow the Client to test rules, aggregators based on rules, and PMML models. Sandbox Replay does not allow the Client to test models developed by Featurespace, or aggregators or risk thresholds based on those models.
	6. Fraud Transaction Monitoring Service and Enhanced Transaction Monitoring Service are subject to the fair usage policy set out in Annex 2.
5. **Eligibility Criteria**
	1. The Client acknowledges and agrees that the provision of Enhanced Fraud Monitoring Service is conditional on the criteria set out in Annex 1 (“Eligibility Criteria”). If the Client data does not meet the Eligibility Criteria, whole or part of the Fraud Services may not be provided.
	2. Featurespace may share examples of the Eligibility Criteria that are identified during a data health check within one month following the go-live date of the Fraud Services, which shall include a description of the checks performed.
	3. Thredd shall not be liable for any failure to provide whole or part of the Fraud Services where the Client data fails to meet the Eligibility Criteria.
6. **Additional Obligations**
	1. The Client is responsible for ensuring that it provides THREDD with the latest contact details for its business, Representatives and Cardholders.
	2. The Client is solely responsible for complaint handling and shall ensure that all complaints and communications with Cardholders are handled in accordance with the Regulations (including but not limited to any regulations for territories the Cardholder’s Card is issued in).
	3. The Client must at all times comply and continue to comply with the Regulations, the requirements of the Scheme, and must not do or omit to do anything which may lead to the failure to honour any responsibilities to Cardholders or others in connection with or relation to the Fraud Services.
	4. Each Party shall comply with all applicable Regulations, including but not limited to reporting requirements under the Regulations. The Client shall indemnify THREDD against all liabilities, costs, expenses, damages and losses suffered or incurred by THREDD arising out of or in connection with the Client’s breach of this clause 6.4.
7. **Limitation of Liability**
	1. Any liability that THREDD may have under or in relation to the Fraud Services is not excluded or limited to the extent that it arises from any claim for:
		1. death or personal injury caused by THREDD’s negligence or that of THREDD’s Representatives;
		2. fraud or fraudulent misrepresentation by THREDD or THREDD’s Representatives; and
		3. any liability that cannot lawfully be excluded under any applicable Regulations.
	2. Subject to clause 7.1, THREDD shall not be liable to the Client in any way whatsoever (whether due to breach of contract, negligence, misrepresentation or for any other reason and whether or not we have been informed or are aware of the possibility of such loss arising) for any:
		1. indirect or consequential loss;
		2. loss of revenue;
		3. loss of profits;
		4. loss of goodwill;
		5. loss of anticipated savings;
		6. loss of customers;
		7. loss of business;
		8. loss under or liability in relation to any other contract (including any contract with a Cardholder);
		9. loss incurred by or in relation to any Cardholder;
		10. loss incurred as a result of THREDD’ failure to respond to Fraud Alert and/or Customer Fraud Alert;
		11. loss incurred as a result of the Client data failing to meet the Eligibility Criteria; and/or
		12. loss incurred as a result of the Client’s failure to comply with the provisions of Clause 2 and 6 of this Schedule.
	3. Subject to Conditions 7.1 and 7.2, and excluding any indemnities provided in this Schedule, THREDD’s aggregate liability under or in relation to this Schedule and the provision of the Fraud Services (whether due to breach of contract, negligence, misrepresentation or for any other reason and including liability to repay any sums already paid to THREDD under this Schedule) shall be limited to £25,000.
	4. Without affecting any other express exclusions or limitations in this Schedule, THREDD’s delivery of the Fraud Services and all obligations under this Schedule is subject to the Client complying in a timely manner with its obligations as set out in this Schedule and Cardholder’s timely response to each Customer Fraud Alert. THREDD will not be liable for any breach of this Schedule to the extent that it arises from a failure by the Client to respond to a reasonable request or comply in a timely manner with its obligations as set out in this Schedule or Cardholder’s failure or delay in responding to Customer Fraud Alert.
	5. Except in respect of any fraudulent or illegitimate Transactions being committed by its Representatives, THREDD shall have no liability for any loss or damage whatsoever arising from or related to any fraudulent or illegitimate Transactions and the Client shall fully indemnify THREDD in respect of any actions, proceedings, costs, losses and damages arising from such fraudulent Transaction.
	6. The Client acknowledges that fraud may occur where the status is changed by the Client or the Cardholder in contradiction of the Fraud Services, and THREDD shall have no liability for any loss incurred as a result.
	7. Each Party shall bear its own costs incurred in respect of compliance with their obligations under this Schedule.
	8. The Parties agree that liability relating to Fraud Services is set out in this Schedule only. For the avoidance of doubt, this clause 7 supersedes the liability provisions set out in the Card Processing Agreement in relation to the Fraud Services only.
8. **Assignment**
	1. The Client shall not without the written consent of THREDD assign, transfer, charge or deal in any other manner with this Schedule or any of its rights under it, nor purport to do any of the same, nor sub-contract the whole or any part of its rights or obligations under this Schedule without THREDD’s prior written authority which shall not be unreasonably withheld or delayed.
	2. THREDD may at any time assign, mortgage, charge, subcontract, delegate, declare a trust over or deal in any other manner with any or all of its rights and obligations under this Agreement.

**Part 2 – Scam Transaction Monitoring**

Part 2 of this Schedule 7 shall apply to Scam Transaction Monitoring only.

1. **Definitions and interpretation**
	1. In this Schedule the following definitions apply:
		1. **SCAM TRANSACTION MONITORING** has the meaning given to it in the Service Schedule (schedule 2).
2. **Client obligations**
	1. The Client shall at all times comply with any instructions or requests provided by THREDD in relation to Scam Transaction Monitoring, including but not limited to any manuals, process documentation or specifications provided from time to time to the Client by THREDD. THREDD accepts no liability for issues resulting from the Client’s non-compliance with such instructions or requests.
	2. The Client shall be solely responsible for:
		1. any required reimbursements determined using Scam Transaction Monitoring to its customers or other entities;
		2. ensuring the rules are created and deployed within their risk appetite, as determined by the Client.
	3. The provision by THREDD of Scam Transaction Monitoring is dependent upon the Client providing such details to THREDD as THREDD may reasonably require in order to provide the service, including but not limited to**:**
		1. payment data in real-time once payments have been initiated by Client to THREDD via REST API in the requested format (as determined by THREDD) including all the mandatory datafields;
		2. all payments related to their customer, both inbound and outbound, to THREDD to analyse for scam behaviour (which for the avoidance of doubt shall assist with the scam transaction monitoring machine learning model which shall learn and provide a risk score);
		3. provide feedback whenever a payment was proven to be related to scam (authorised push payment fraud) or fraud (un-authorised fraud).
	4. The Client acknowledges that additional optional payment fields may assist with better decisioning based on agreed schema (as available in API docs) and shall provide information to THREDD or Featurespace as reasonably requested in order to improve the machine learning model.
	5. The Client shall comply with any obligations, instructions or requirements set out in the API documents provided by THREDD to the Client from time to time.
	6. Retrains will be performed by Featurespace at intervals periodically calibrated at Featurespace’s recommendation; retrains are performed by aggregating data from all customers within the same geographical area.
	7. Thredd is not liable for the actions taken or not taken off the back of the risk score, or, if, highly unlikely, there is an outage and a risk score is not provided OR due to technical error OR due to feedback given via both API and Portal resulting in double-counted event.
	8. The Client acknowledges and agrees that the Service Levels in Schedule 4 of the Card Processing Agreement do not apply to Scam Transaction Monitoring provided under this Schedule.
	9. The Client is solely responsible for complaint handling and shall ensure that all complaints and communications with Cardholders are handled in accordance with the Regulations (including but not limited to any regulations for territories the Cardholder’s Card is issued in).
	10. The Client must at all times comply and continue to comply with the Regulations, the requirements of the Scheme, and must not do or omit to do anything which may lead to the failure to honour any responsibilities to Cardholders or others in connection with or relation to Scam Transaction Monitoring.
	11. Each Party shall comply with all applicable Regulations, including but not limited to reporting requirements under the Regulations. The Client shall indemnify THREDD against all liabilities, costs, expenses, damages and losses suffered or incurred by THREDD arising out of or in connection with the Client’s breach of this clause.
3. **Liability**
	1. Any liability that THREDD may have under or in relation to Scam Transaction Monitoring is not excluded or limited to the extent that it arises from any claim for:
		1. death or personal injury caused by THREDD’s negligence or that of THREDD’s Representatives;
		2. fraud or fraudulent misrepresentation by THREDD or THREDD’s Representatives; and
		3. any liability that cannot lawfully be excluded under any applicable Regulations.
	2. Subject to clause 3.1, THREDD shall not be liable to the Client in any way whatsoever (whether due to breach of contract, negligence, misrepresentation or for any other reason and whether or not we have been informed or are aware of the possibility of such loss arising) for any:
		1. indirect or consequential loss;
		2. loss of revenue;
		3. loss of profits;
		4. loss of goodwill;
		5. loss of anticipated savings;
		6. loss of customers;
		7. loss of business;
		8. loss under or liability in relation to any other contract (including any contract with a Cardholder);
		9. loss incurred by or in relation to any Cardholder;
		10. loss incurred as a result of THREDD’ failure to send an API response in relation to Scam Transaction Monitoring;
		11. loss incurred as a result of the Client data failing to comply with THREDD’s reasonable instructions; and/or
		12. loss incurred as a result of the Client’s failure to comply with the provisions of Clause 2 this Schedule.
	3. Subject to Conditions 3.1 and 3.2, and excluding any indemnities provided in this Schedule, THREDD’s aggregate liability under or in relation to this Schedule and the provision of the Scam Transaction Monitoring (whether due to breach of contract, negligence, misrepresentation or for any other reason and including liability to repay any sums already paid to THREDD under this Schedule) shall be limited to £25,000.
	4. Without affecting any other express exclusions or limitations in this Schedule, THREDD’s delivery of Scam Transaction Monitoring and all obligations under this Schedule is subject to the Client complying in a timely manner with its obligations as set out in this Schedule and Cardholder’s timely response to each request. THREDD will not be liable for any breach of this Schedule to the extent that it arises from a failure by the Client to respond to a reasonable request or comply in a timely manner with its obligations as set out in this Schedule or Cardholder’s failure or delay in responding to any alerts.
	5. Except in respect of any fraudulent or illegitimate Transactions being committed by its Representatives, THREDD shall have no liability for any loss or damage whatsoever arising from or related to any fraudulent or illegitimate Transactions and the Client shall fully indemnify THREDD in respect of any actions, proceedings, costs, losses and damages arising from such fraudulent Transaction.
	6. Each Party shall bear its own costs incurred in respect of compliance with their obligations under this Schedule.
	7. The Parties agree that liability relating to Scam Transaction Monitoring is set out in this Schedule only. For the avoidance of doubt, this clause 3 supersedes the liability provisions set out in the Card Processing Agreement in relation to the Scam Transaction Monitoring only.
4. **Assignment**
	1. The Client shall not without the written consent of THREDD assign, transfer, charge or deal in any other manner with this Schedule or any of its rights under it, nor purport to do any of the same, nor sub-contract the whole or any part of its rights or obligations under this Schedule without THREDD’s prior written authority which shall not be unreasonably withheld or delayed.
	2. THREDD may at any time assign, mortgage, charge, subcontract, delegate, declare a trust over or deal in any other manner with any or all of its rights and obligations under this Agreement.

**ANNEX 1 – ELIGIBILITY CRITERIA**

Eligibility criteria for joining the consortium model

A tenant should be considered to join the consortium model if its data meets the following criteria:

* Fraud label events must be able to be linked back to the original transaction using a unique Id (lifecycleId) and this method must be at least 90% accurate.
* ARIC must receive the majority of fraud label events (recommended 90%) within 30 days of the original transaction.
* Thredd must be able to obtain fraud data (or mark in the ARIC UI) fraud cases for both:
	+ Fraud alerted by ARIC
	+ Fraud missed by ARIC but reported by the Client
* There are not segments of the transaction data (e.g. card-present transactions) that are missing labels.
* There is an identifier for the card that is unique across the consortium and consistent over time (i.e. hashing is not changed periodically).
* Merchant and MCC identifiers are consistent with the consortium (sourced from VISA/Mastercard) and consistent over time.
* Transaction data does not dramatically deviate from all other transaction data in the consortium. For example, if a small tenant is onboarded which only contains single-use PANs and no other tenant does then its card and model scores will be very divergent and performance likely poor.

The Client acknowledges that the above list not exhaustive and data may be subject to additional requirements.

**ANNEX 2 – FAIR USAGE POLICY**

Fair usage policy

* Thredd shall provide the Client with a maximum of 4 bespoke reports per month (to be agreed between the Parties in advance).
* The Client may request configuration (in accordance with the terms of this Schedule) of up to 20 Fraud Rules updates per month.