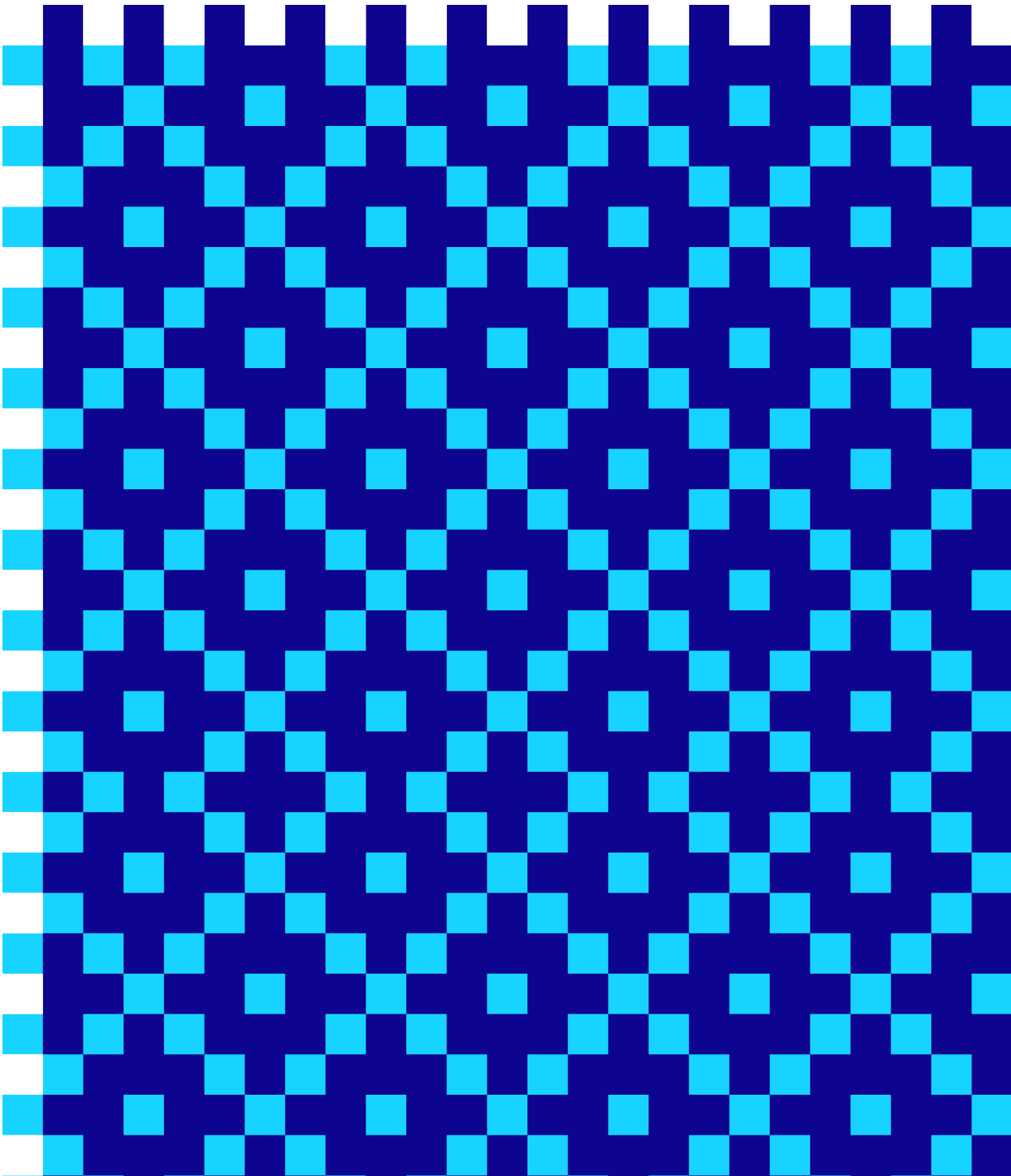
Card Processing Agreement

Schedule 5 – Enhanced Fraud Transaction Monitoring and Fraud Transaction Monitoring



The terms below supplement the Card Processing Agreement and relate to Enhanced Fraud Transaction Monitoring and Fraud Transaction Monitoring only. The applicability of the terms 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.

BASE SOFTWARE: means the proprietary software programs of Featurespace known as ARIC which is provided on the SaaS;

ENHANCED FRAUD TRANSACTION MONITORING: means the enhanced version of the product which may be supplied to the Client under this Schedule, which includes the Client's specific implementation of the Base Software, the ongoing provision of the Base Software and its outputs (i.e. adaptive behaviour profiling of authorisations for potential fraud risk, sandbox replay & advanced analytics) as a service within THREDD provision of issuer processing services;

FRAUD TRANSACTION MONITORING: means the essential version of the product which may be supplied to the Client under this Schedule, which includes the Client's specific implementation of the Base Software, the ongoing provision of the Base Software and its outputs (i.e. assessment of authorisations for potential fraud risk) as a service within THREDD provision of issuer processing services;

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;

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.

1. **Use of the SaaS:**

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.

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. **Use of User Interface and Case Manager:**

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.

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. **Creating, Modifying Rules, Models, and Configurations:**

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.

THREDD do 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. Service Levels

The Client acknowledges and agrees that the Service Levels in Schedule 4 do not apply to Enhanced Fraud Transaction Monitoring or Fraud Transaction Monitoring