Venue Smart Pty Ltd

Credit Risk Policy

Document History (Version Number)	Date Modified	Author	Summary of Changes
V1.0	22nd August 2023	Franchesco Vorster	Initial Draft

Approved by the Board on: XXXX

Contents

1. **Definitions**
2. **Introduction**
3. **Management and maintenance**
4. **Monitoring and review process**
5. **Credit team**
6. **Credit analysis (customer (Merchant) screening and on-boarding)**
7. **Transaction, supply and settlement risk management**
8. **Approval process**
9. **Deviations from approval policy**
10. **General reserve for credit losses (GRCL)**
11. **Specific provisioning**
12. **Write-offs**
13. **Chargeback, Dispute, Refund/return risk management**
14. **Receivables risk management**
15. **Reporting and monitoring**
16. **Customer operational and financial review**
17. **Changes to Credit Risk Policy limits**

1. Definitions

Capitalised terms used in this document have the following meaning, unless the context otherwise requires:

Aggregator (Aggregation) means a payment aggregation service used to process BPay, Direct Entry and NPP transactions provided by a Service Provider to Venue Smart and on-supplied by Venue Smart to Merchants;

AML/CFT Act means the *Anti-Money Laundering and Countering Financing of Terrorism Act 2006* ;

AML/CFT Policy means the anti-money laundering and combating the financing of terrorism policy and processes developed by Venue Smart to detect ML and FT and manage and mitigate the risk of ML and FT;

AML/FT Risk Assessment means the document which records Venue Smart assessment of the risk of ML and FT as amended from time to time;

AML/CFT Risk Register means the register of risk maintained by the General Manager with oversight from the Payments Risk Committee.

Beneficial Owner means any individual (natural person) who, satisfies any one (or any combination) of the following three elements:

- Has Effective Control of a Merchant;
- Has Effective Control of the person on whose behalf a transaction is conducted; or
- Who owns a prescribed threshold (being more than 25%) of the Merchant or person on whose behalf a transaction is conducted,

and "Beneficial Ownership" will have a similar meaning;

Note: It is possible for ownership to be split into parcels of 25 percent or less but, if the Merchant's ownership structure is understood at each layer, it might become apparent that relationships between the parties may give an individual aggregate ownership of the Merchant that amounts to more than 25 percent.

Board means the Venue Smart board of directors from time to time;

BPay means that payment type, supplied by the banks, that allows a payer to pay a biller using a BPay biller reference and a payer customer reference;

Card Acquirer means a business that has the right (allocated to them by a card Association/Scheme) to acquire card payments from a Merchant and send that payment to the Issuer of that card. The Acquirer either utilises insourced or outsourced technologies to

perform this function. The Card Acquirer also means Global Payments and Fiserv or such other replacement or successor appointed by Venue Smart from time to time;

Chargebacks means the dispute process that results in the return of money or the reversal of a card transaction initiated by the Card Acquirer or a Merchant's customer's issuing bank;

Complaint means an expression of dissatisfaction made to Venue Smart by any person, related to its products or services, or the complaints handling process itself, and dispute has a corresponding meaning;

Complaints Policy means complaints and disputes policy including any schedules to it as amended from time to time;

Complaints Register means the register of Complaints maintained by the General Manager.

Compliance Manager means the staff member appointed by Venue Smart to manage compliance;

Credit Management Team means the group of staff appointed by Venue Smart to manage credit risk;

Credit Risk Policy means this credit risk policy as amended from time to time;

Direct Entry means that payments type, inclusive of direct debits and direct credits, supplied by a Service Provider that allows a payee to debit a bank account and a payer to credit a bank account overnight.

Dispute means the dispute process that results in the return of money or the reversal of a Direct Debit, NPP or BPay transaction initiated by the Service Provider or a Merchant's customer's bank;

Effective Control means to:

- any individual(s) with the ability to control the Merchant and/or dismiss or appoint those in senior management positions;
- any individual(s) holding more than 25 percent of the Merchant's voting rights;
- any individuals (for example, the CEO) who hold senior management positions; and
- trustees (where applicable);

Forward Dated Risk means the credit risk associated with the PayFac/Aggregation service being provided to the Merchant taking into account the risk of Chargebacks/Disputes in respect of payments received in advance before the Merchant provides the goods or services;

FT means financing of terrorism;

General Manager means a person who is appointed by the board of Venue Smart from time to time;

ISO means an entity that acts as an independent sales organisation on behalf of a Card Acquirer where the ISO resells the Card Acquirers payment service. The ISO typically has responsibility for signing up the Merchant to the Card Acquirers compliance and credit risk standards but does not underwrite the risk. The ISO typically receives the margin difference from the Card Acquirers ISO wholesale fee rate and the rate the ISO sells the payment service for;

Issuer means the issuing bank responsible for issuing the bank card (whether credit, debit or prepaid) to the cardholder;

Management Team means the General Manager , Chief Executive Officer, Chief financial officer who is appointed by the board of Venue Smart from time to time;

Merchant means a Venue Smart customer that is approved to use the PayFac, Aggregation or ISO service;

ML means money laundering;

NPP (New Payments Platform) means that payment type, supplied by the bank, that allows a payer to pay a payee real time or a payee to debit a payer in real time using an NPP payment identifier;

PayFac means a payment facilitation service used to process card transactions provided by the Card Acquirer to Venue Smart and on-supplied by Venue Smart to Merchants;

Payments Operations Team means the group of staff appointed by Venue Smart to manage payment operations.

PCI DSS means the Payment Card Industry Data Security Standard introduced by the Schemes for the protection of cardholder data and the associated transactions.

PEP (politically exposed person) means:

a An individual who holds, or has held at any time in the preceding 12 months, in any overseas country the prominent public function of:

- Head of State or head of a country or government; or
- government minister or equivalent senior politician; or
- Supreme Court Judge or equivalent senior Judge; or
- Governor of a central bank or any other position that has comparable influence to the Governor of the Reserve Bank of Australia; or

- Senior foreign representative, ambassador, or high commissioner; or
- high-ranking member of the armed forces; or
- board chair, chief executive, or chief financial officer of, or any other position that has comparable influence in, any State enterprise; and

b. An immediate family member of a person referred to in paragraph (a), including:

- a spouse; or
- a partner, being a person who is considered by the relevant national law as equivalent to a spouse; or
- a child and a child's spouse or partner; or
- a parent; and

c. Having regard to information that is public or readily available:

- any individual who is known to have joint Beneficial Ownership of a legal entity or legal arrangement, or any other close relationship, with a person referred to in paragraph a; or
- any individual who has sole Beneficial Ownership of a legal entity or legal arrangement that is known to exist for the benefit of a person described in paragraph a;

Venue Smart means Venue Smart (ABN 52 604 254 766);

Venue Smart Risk Committee means the risk committee, comprised of at least 2 Board directors or such other members who are appointed as comprising the risk committee from time to time;

Venue Smart CRM means a web-based, customer relationship management system used by Venue Smart to serve as a central repository for customer records and Complaint handling;

Venue Smart Risk Management Framework means the risk management plan developed by Venue Smart from time to time detailing Venue Smart's risk management process and which is adopted by Venue Smart it's risk management framework;

Prescribed Transaction means a transaction conducted through the PayFac or Aggregator service in respect of:

- a domestic (i.e. within Australia) physical cash transaction of AUS$10,000 and over;

Prohibited Industry means a Merchant that operates within an industry that is prohibited by Venue Smart, the Card Acquirer, the Service Provider, legislation, card scheme rules, regulations or otherwise;

Prohibited Merchant means a Merchant that is prohibited from using the PayFac or Aggregator service by Venue Smart, the Card Acquirer, the Service Provider, legislation, card scheme rules, regulations or otherwise (refer to the Credit Risk Policy for more information on "Prohibited Merchants");

Refund means the returning of customer funds or fees where the request may be as a result of one (but not limited to) overcharging, charging a fee not in an agreement, non supply of goods or services, faulty supply of goods or services, service level failure or a breach of an agreement;

Resellers means those parties that develop business management software for an industry and have embedded the PayFac's payment processing capabilities within their business software. The Reseller also has an agreement with the PayFac to resell their services.

Risk Register means the register of risk maintained by the General Manager Payments;

Scheme (also Association) means an organisation that has created a card product or Scheme with associated rules and regulations for the issuance, acquiring and use of that product. Also known as a card Scheme. Typical card Associations/Schemes include, Visa, MasterCard, China UnionPay, JCB, Diners, Discovery and EFTPOS; and

Service Provider means that business that has the ability to supply Aggregated Direct Entry, NPP or BPay payments services to Venue Smart.

2 Introduction

Venue Smart Pty Ltd (Venue Smart) is a multi-channel payments processor offering merchants the ability to accept both online and across the counter payments (via an EFTPOS device). The service is called Venue Smart.

Venue Smart supports the following payment types online:

- Card (Visa and MasterCard debit and credit cards)
- BPay
- Direct debit and NPP payments

Venue Smart supports the following payment types across the counter via an EFTPOS device:

- online and card (Visa and MasterCard debit and credit card)
- proprietary EFTPOS cards).

To support the above payment types Venue Smart is required to operate as follows:

- Online Cards processing as a Payment Facilitator (PayFac)
- Across the counter EFTPOS processing as an Independent Sales Organisation (ISO)
- Direct debit/NPP processing as a Direct Entry/NPP Sponsored User
- BPay processing as BPay Master Biller

As a PayFac Venue Smart is pre-issued card based Merchant ID's which are in-turn allocated by Venue Smart to a merchant. All funds are settled into the Card Acquirers owned and managed custodial account (in the name of Venue Smart) held at its bank. Venue Smart initiates disbursements from the custodial settlement account to the merchant's designated bank account.

As a Direct Entry/NPP and BPay Aggregator all funds are settled into a Venue Smart settlement account. Venue Smart initiates disbursements from the settlement account to the merchant's designated bank account.

As an ISO Venue Smart acts as a reseller of the Card Acquirer.

As a PayFac and Aggregator, Venue Smart absorbs the compliance and credit risks associated with servicing the merchant with a payment service.

As an ISO, the Card Acquirer absorbs the compliance and credit risks associated with servicing the merchant with a payment service.

Venue Smart has risks associated across the following broad areas:

- Regulatory
- Credit
- Financial and Market
- Strategic
- Operational
- Cyber Security & Privacy

This policy covers the area of credit risk.

Venue Smart incurs credit risk across its business from the following areas:

- On Call Bank deposits with an authorised deposit taking institution (i.e. a bank);
- Accounts receivables (i.e. debtors/customers who are invoiced and are required to make payments);
- Being a PayFac; and
- Being an Aggregator
- Being an ISO

Credit Risk of being a PayFac and Aggregator

Processing of payments for a Merchant can generate a dispute from a cardholder (Chargeback) or bank account holder (Dispute). This dispute could require Venue Smart to reverse a payment from the Merchant. If the Merchant does not have sufficient funds to cover the reversal, then this places a credit risk on Venue Smart (being the entity ultimately responsible for accepting payments on behalf of the Merchant) until the funds are recovered.

Disputes could typically arise as a result of:

- Non delivery of the goods and services;
- Faulty or sub-standard supply of goods and services that are returned; and
- Fraudulent use of the payment type by the payer.

The majority of credit risk is heavily weighted to disputes risk due to the potential for fraud and or Merchant bad debt.

To manage and monitor the credit risks associated with being a PayFac and Aggregator, Venue Smart must:

- Identify the relevant credit risks that may arise with processing payment transactions for Merchants and associated credit limits that Venue Smart wishes to operate in;
- Ensure timely on-boarding of customers – complicated or pro-longed on-boarding should be carefully assessed as it could be indicative of fraudulent behaviour;
- Implement prudent underwriting standards and procedures for approving Merchants to receive the PayFac and Aggregator service;
- Implement ongoing review processes for assessing the operational and financial condition of the Merchant;
- Operate adequate policies, systems and procedures for the monitoring of disputes and the ability for a Merchant to meet its dispute obligations if they arise;
- Implement adequate policies, systems and procedures to limit and monitor credit risk concentrations in specific geographies, industries and customers;
- Manage Forward Dated Risk. One of the considerations in assessing a Merchant is the time taken by the Merchant to deliver goods or services after receiving payment. The greater the lag between the delivery of goods and services after receiving payment, the greater the inherent Forward Dated Risk.

Credit Risk of being an ISO

Venue Smart does not incur credit risk from Chargebacks or Disputes associated with being an ISO as this is absorbed by the Acquirer.

Credit Risk from non payment of receivables

As a Payfac, Venue Smart incurs no receivables credit risk as all funds are settled net of fees.

As an Aggregator of Direct Entry and BPay payments, Venue Smart incurs no receivables credit risk as all funds are settled net of fees.

As an ISO of EFTPOS, Venue Smart only incurs receivables credit risk associated with the EFTPOS terminal rental or terminal damage/loss as this is debit manage outside the settlement cycle.

This document is the policy by which Venue Smart identifies and manages credit risk associated with supplying services to a Merchant.

Strict adherence to the procedures set out in this policy is expected from all Venue Smart staff and will be monitored to ensure that the credit risks associated with being a PayFac and Aggreator are managed and mitigated as far as possible.

Nothing within this policy is intended to render the policies and procedures it contains contractually binding. However, breaches of this policy by Venue Smart staff, contractors or operational service providers may constitute misconduct, serious misconduct or material breach of contract, which may result in disciplinary action culminating in termination of employment (including summary dismissal) or termination of contract.

Venue Smart may unilaterally amend this policy from time to time.

3. Management and maintenance

The Credit Risk Policy will be managed and maintained on a day to day basis by the company Compliance Manager.

4. Monitoring and review process

The Compliance Manager must:

- Provide the Credit Risk Policy to the Management Team 6 monthly for review; and

- Ensure that the Credit Risk Policy is reviewed and approved by the Board on an annual basis.

The General Manager Payments must:

- Ensure the Credit Risk Policy is operationally implemented, (i.e. that Merchants risk profiles are adequately assessed to ensure that the Merchant does not exceed the Credit Risk Policy limits detailed within this document);
- Report monthly to the Compliance Manager the company's status against the Credit Risk Policy limits. The report must take the form of updates to the Risk Register;
- Review the credit risks generated by the Merchant with the aim of recommending to the Compliance Manager new industry risk ratings and credit limits;
- Provide to the Compliance Manager an analysis of the payments processed (including refunds, declines, reversals, voids, disputes and Chargebacks) on a monthly basis highlighting any trends, emerging risks and any other issue; and
- Meet with the Compliance Manager on a monthly basis to ensure that appropriate actions are taken to mitigate any emerging risks.

5. Credit team

Venue Smart is required to operate a risk management function within its business which must be overseen by the Payments Operations Team.

The Payments Operations Team must:

- Manage the credit risk generated by a Merchant on a day to day basis;
- Manage Disputes/Chargeback requests; and
- Report, on a weekly basis, to the General Manager Payments.

All members of the Payments Operations Team should:

- Be reference checked;
- Be police checked every 2 years;
- Be appropriately experienced and trained;
- Have a job description with the appropriate risk mitigation key performance indicators;
- Be reviewed annually for performance; and
- Sign a register, at least annually, that they have received sufficient training on Venue Smart's credit risk management policies and procedures including this Credit Risk Policy.

6. Credit analysis (Merchant screening and on-boarding)

Venue Smart must ensure that it undertakes credit analysis of all prospective Merchants and that Venue Smart staff have an understanding of the credit risk associated with a prospective Merchant within the following key credit risk portfolios:

- Product portfolio risk;
- Merchant (customer) portfolio risk;
- Geography portfolio risk;
- Industry portfolio risk;
- Forward Dated risk; and
- Prohibited or restricted Merchant categories

6.1 Product portfolio risk

Venue Smart sells a multi-channel and multi-payment type payment processing service.

As Venue Smart is a new service provider therefore there is no product limit set in the first 12 months of operations,to be reviewed quarterly. After a full 12 months this limit will be reviewed.

6.2 Merchant portfolio risk

Venue Smart's business plan requires Venue Smart to sell its product/services to Merchants that require PayFac, Aggregation and ISO services.

It is expected that the Merchants will vary in size and complexity.

Venue Smart's policy is not to service Merchants that will negatively impact Venue Smart's overall business plan, strategic direction, risk appetite, brand, reputation or its financial stability.

The Merchants can be categorised as extreme, high, medium and low risk.

6.2.1 Extreme / High Risk Merchants

Extreme risk Merchants are defined as Merchants that have the following attributes:

- Supply prohibited products or have prohibited Merchant category codes (prohibited by legislation/rules/regulations established by Schemes (i.e. Visa/ Mastercard)/the Card Acquirer) and Service Providers;

- Operate within a prohibited industry (prohibited by legislation/rules/regulations established by Schemes (i.e. Visa/ Mastercard)/ the Card Acquirer) and Service Providers;
- Undertake activities that are inconsistent with Venue Smart's overall business plan, strategic direction and risk appetite;
- Have failed an AML/CTF check;
- Have failed a credit check;
- Assessed Merchant Prepayment Risk within the individual merchant risk limit as set by the Risk Committee from time to time (eg. $250k);
- Have unresolved chargebacks, disputes or claims (see section 13.3);
- Have a reputation for engaging in fraudulent activities and/or being associated, to a material extent, with failed businesses; and
- Have a returns/refunds that exceed 10% of their monthly turnover for more than 2 months in a row or 4 months over a 12 month period.
- Disputes or Chargebacks rate that exceed 0.50% of their monthly turnover for more than 2 months in a row.
- Or as defined by the acquirer from time to time.

6.2.2 High Risk Merchants

High risk Merchants are defined as Merchants that have one or more of the following attributes:

- Start up businesses with less than 6 months of operating history;
- Has a poor credit rating at a director, manager and/or business level;
- Has a poor reputation for supplying poor products/services that generates a substandard experience to the payer and hence are more likely to generate returns/refunds, Disputes or Chargebacks;
- Consistently high volumes of returns/refunds, Disputes or Chargebacks per month above the thresholds above;
- Have an increased risk of exposure to fraud and/or business failure.
- High brand risk merchants as defined by the card schemes or acquirer

Venue Smart will NOT sell its products and services to High Risk Merchants.

6.2.3 Medium Risk Merchants

Medium risk Merchants are defined as Merchants that have one or more of the following attributes:

- An early stage business with less than 24 months but more than 6 months of operating history;
- Have a average business process or have an average reputation of supplying products/services that is likely to generate confusion or a substandard experience to the cardholder/bank account holder and hence are more likely to generate returns/refunds, Disputes or Chargebacks; and
- Assessed Merchant Prepayment Risk limit above $25k;

Venue Smart has the following limits on medium risk Merchants

- No more than 10% of turnover from a single medium risk customer; and
- No more than 50% of turnover from all medium risk customers

6.2.4 Low Risk Merchants

Low risk Merchants are defined as Merchants that have all of the following attributes:

- Are businesses with greater than 24 months of operating history;
- Strong credit rating at a director, manager and/or business level;
- Have a reputation for the supply of a quality product/services to a cardholder/bank account holder
- Have a consistently low rate of returns/refunds, Disputes or Chargebacks;
- Assessed Merchant Prepayment Risk limit below $25k;
- Merchants who have their contractual obligations supported by 3rd party director/manager/owner guarantees
- Merchants that only use Venue Smart's EFTPOS services for across the counter payments.

No limits are allocated to low risk Merchants.

6.3 Geography Portfolio Risk

Venue Smart's business plan requires Venue Smart to sell its product/service to Australia Merchants only. In the longer term Venue Smart wishes to sell its product/services into other countries.

6.3.1 Geography Restrictions

Venue Smart will only sell it products/services to Australian based Merchants.

Venue Smart will sell its product/services to Merchants in all states and territories of Australia.

6.3.2 Geography Risk

Venue Smart has the policy to sell its products/services to Merchants across all states/territories within Australia and accordingly spread its revenue evenly across all states/territories.

For the first 12 months Venue Smart is prepared to concentrate its revenues and profit in a single or a limited number of states/territories.

6.4 Industry Portfolio Risk

Venue Smart's business plan requires Venue Smart to sell its product/service across many industries and spread industry concentrations appropriately. A review of industry concentration would occur quarterly.

6.5 Forward Dated Risk

Venue Smart has recognised that some of their Merchants may take payment upfront for products or services to be supplied.

It should be noted that insurance companies typically charge monthly insurance premiums hence reducing the risk of forward dated risk.

Venue Smart's Risk Appetite states that Prepayment Exposure can be no more than 30% of available capital/surplus liquidity.

Accordingly Venue Smart has the following Prepayment Risk limits:

- No Merchant is to be signed that requests deposits greater than 50% of the value of the goods/service sold before supply; and
- Total Prepayment Exposure across all Merchants can be no more than 30% of available capital/surplus liquidity.

6.6 Prohibited or Restricted Merchant Categories

Venue Smart will **NOT** sell its products or services to the following sectors/Merchant categories:

Merchants who offer Card based payments to its customers

- Merchants that sell illegal products or services;
- Merchants that in the Risk Committee's judgement are high Fraud, Forward Delivery or Reputational risk
- Merchants with a Merchant category code (MCC) that are prohibited or restricted by the rules/regulations established by the Schemes (i.e Visa/MasterCard) and or Venue Smart's Card Acquirers; and
- Merchants that are significantly impacted by prevailing negative market conditions of that time (i.e. Pandemic impacted businesses such as: suppliers to airlines, gyms, hotels etc), i.e.
    - A P and L and Balance Sheet that can not sustain high levels of refunds or chargebacks on non supply
    - High likelihood of cash flow issues caused by refunds/chargebacks
    - High likelihood of refunds being requested

Merchants who offer Direct Debit (Direct Entry) based payments to its customers

- Merchants that sell illegal products or services;
- Merchants that that are prohibited or restricted by the rules/regulations established by the Schemes (BEC's) and or Venue Smart's Direct Entry supplier;
- Merchants that are significantly impacted by prevailing market conditions of that time (i.e. Pandemic impacted businesses such as: suppliers to airlines, gyms, hotels etc).
    - A P and L and Balance Sheet that can not sustain high levels of refunds or disputes on non supply
    - High likelihood of cash flow issues caused by refunds/disputes
    - High likelihood of refunds being requested on non supply

Merchants who offer BPay based payments to its customers

- Merchants that sell illegal products or services;
- Merchants that in the Risk Committee's judgement are high Operational Fraud, or Reputational risk
- Merchants that that are prohibited or restricted by the rules/regulations established by the Schemes (BPay/Banks) and or Venue Smart's Direct Entry supplier;
- Merchants that are significantly impacted by prevailing market conditions of that time (i.e. Pandemic impacted businesses such as: suppliers to airlines, gyms, hotels etc).
    - A P and L and Balance Sheet that can not sustain high levels of refunds or disputes on non supply
    - High likelihood of cash flow issues caused by refunds/disputes
    - High likelihood of refunds being requested on non supply

Merchants who offer EFTPOS based payments to its customers

- Merchants that sell illegal products or services;
- Merchants that that are prohibited or restricted by the rules/regulations established by the Schemes (EFTPOS/Banks) and or Venue Smart's EFTPOS supplier;
- Merchants that are significantly impacted by prevailing market conditions of that time (i.e. Pandemic impacted businesses such as: suppliers to airlines, gyms, hotels etc).
    - A P and L and Balance Sheet that can not sustain high levels of refunds or disputes on non supply
    - High likelihood of cash flow issues caused by refunds/disputes
    - High likelihood of refunds being requested on non supply

7. Transaction, Supply and Settlement Risk Management

Venue Smart has the ability to further mitigate credit risk at three levels:

- Transactional;
- Supply; and
- Settlement.

7.1 Transactional Risk

Venue Smart is able to limit transactional credit risk associated returns/refunds, Disputes or Chargebacks caused by fraud or non supply of goods or services by setting limits on all payments made at a Merchant profile level. The limits are as follows:

- High risk business;
    - Maximum number of payments on a single card/bank account per day = 5
    - Maximum ticket size per payment = $1000
    - Turnover per month = $50,000
- Medium risk business;
    - Maximum number of payments on a single card/bank account per day = 5
    - Maximum ticket size per payment = $1000
    - Turnover per month = 100,000
- Low risk business;
    - Maximum number of payments on a single card/bank account per day = 5
    - Maximum ticket size per payment = $1000
    - Turnover per month = $500,000

7.2 Supply and Payment Risk (at an agreement level)

Venue Smart recognises that there is a risk that a Merchant could be fraudulent or may not supply goods or services paid for by the cardholder/bank account holder. This type of Merchant will generate returns/refunds, Disputes or Chargebacks. The level of returns/refunds, dispute or Chargebacks are likely to be larger where the payments are:

- Captured in advance of supply;
- The Merchants business processes create confusion or concern; and
- The product/services supplied are faulty or do not operate as advertised.

To mitigate the supply side risk that the cardholder/bank account holder holds Venue Smart directly responsible for non-supply of goods/services or supply of faulty goods by a Merchant, Venue Smart has implemented a Merchant agreement that provides that:

- Venue Smart is not responsible for the non-payment of good and services by the cardholder/bank account holder; and
- Where disbursements are Disputed/Charged back by the cardholder/bank account holder then Venue Smart will have the right to reverse these funds from the Merchants nominated settlement account. The Merchant in this case will need to recover these funds from the cardholder/bank account holder directly.

7.3 Settlement Risk

Venue Smart recognises that there is a risk that a Merchant could be fraudulent or may not supply goods or services paid for by the cardholder/bank account holder. To off-set the credit risk Venue Smart has implemented the following settlement based mitigations:

- Settlements that exceed the Merchant specific settlement profile of greater than 50% are blocked for review by the General Manager Payments;
- Only Merchant authorised users can supply a new settlement account;
- Changes to settlement accounts require 2 factor authentication; and
- Images of settlement account statements need to be supplied on sign up and on any changes.

8. Approval process

Venue Smart has the following Merchant approval processes that must be followed for each Merchant prior to on-boarding or being provided with a product or service:

- The Merchant application must be correctly completed and electronically signed/verified;
- The Merchant as part of the application must supply the following:
    - Registered business name
    - ABN or ACN
    - Date of business registration
    - Trading name
    - Trading address
    - Web site URL
    - All Beneficial Owners details (i.e. full name, residential address, DOB, place of birth and contact phone/mobile and email address)
    - All Director details (i.e. full name, residential address, DOB, place of birth and contact phone/mobile and email address)
    - Authorised signatories contact details (i.e full name, residential address, DOB place of birth, phone/mobile and email address)
    - Principle business contact details (i.e full name, phone/mobile and email address)
    - Settlement bank account (BSB/Account number)
- The Beneficial Owners must all pass Venue Smart's AML/CFT process. See AML/CFT policy;
- The Merchant must supply the following transactional details:
    - Industry serviced
    - Product/services supplied
    - Time in business
    - Total business turnover for last year
    - Estimated total payment turnover by channel and type (i.e. Terminal, Online, MOTO, Card, BPay, Direct Debit etc) for the next 3 years
    - Estimated ticket size by channel/type
    - Refund policy (i.e. all, some or none and by when)
    - Estimated refunds turnover/month
    - Estimated ticket size of refunds
    - Deposit policy (i.e. none, X% of payment)
    - Estimated average length of time of supply
- Check the prospective Merchant will not cause Venue Smart to exceed Credit Risk Policy limits (i.e this document); and
- Validate that the merchant's business processes and technologies are sufficiently robust that they will not create customer confusion or facilitate fraud by either a customer or merchant, i.e:

    - It is clear to the customer who they are buying from, i.e merchant name
    - Customers can contact them in some way shape or form
    - They are PCI compliant
    - They have customer payment terms and conditions
    - They have customer refund/return policies
    - If they are a online eCommerce merchant selling products to non account customers via a web site they also:
        - Use some type of tool to stop test transaction/surges
        - Use 3D Secure
        - Display their payment T and C's and refund/return policies
- The requirements for a standard ecommerce website.
    - Website must be valid and working. (i.e. not registered to GoDaddy or a Parked website)
    - Merchant contact information-providing a way for a customer to get in contact with the merchant.
    - Products & services, including pricing, that reflect the goods and services sold.
    - Terms & Conditions including:
        - Refund/Return policy
        - Delivery/Shipping policy
        - Cancellations policies (where applicable)
        - Exact dates of free trial periods (if offered)
- Prospective Merchants must be approved by the General Manager Payments after taking Venue Smart's overall business plan, strategic direction and risk appetite into account.

See attached for Merchant approval workflow here.

9. Deviations from approval policy and process

Any Merchant approvals that deviate from the above approval process and policy are required to be approved in writing by the Compliance Manager.

10. General reserve for credit losses (GRCL)

Venue Smart must maintain a general reserve for credit losses (GRCL) in its accounts.

The GRCL will include the following:

- Sufficient capital to cover 10% of debtors over 120 days (excluding those that have been specifically provisioned) representing the possibility of 10% of debtors not paying their debts for 120 days; and
- 0.05% of previous months payments turnover representing the possibility of:
    - a Merchant becoming insolvent without providing goods and services (i.e. Forward Dated Risk).
    - Dispute or Chargebacks due to fraudulent use of a card/bank account.

11. Specific Provisioning

As is standard practice, Venue Smart must maintain a specific provision for any debts where management is aware that the debtor is likely to be unable to pay its debt. As part of ensuring adequate specific provisions are maintained all debts over 90 days are to be reviewed on a monthly basis to identify any potential unrecoverable debts.

12. Write-offs

The General Manager Payments can write-off bad debts of up to $1000 after all efforts in recovering the debt have failed.

Write-offs above $1000 must be approved by the CEO.

13. Chargeback, Dispute and Refund/return risk management

Chargebacks are where the cardholder disputes a payment with their Issuing bank or financial institution.

Disputes are where the bank account holder disputes a bank account payment (via the Direct Entry, NPP or BPay channels) with their bank or financial institution.

If the Chargeback/Dispute is upheld (i.e. Venue Smart can not prove to the Card Acquirer or Service Provider that the payment was valid) then the Card Acquirer/Service Provider will then automatically reverse the payment from Venue Smart's custodial settlement account. Venue Smart then has to recover these funds from the Merchant.

Refunds are the returning of customer funds or fees where the request may be as a result of one (but not limited to) overcharging, charging a fee not in an agreement, non supply of goods or services, faulty supply of goods or services, service level failure or a breach of an agreement. Excessive refunds could impact the Merchant's cash flow/financial position to a point of insolvency.

To manage and monitor such risks Venue Smart must implement prudent underwriting standards and procedures for approving and monitoring Merchants.

See Section 7 for Venue Smart's monitoring processes and Section 8 for Venue Smart's approval processes.

13.1 Payments Operations Team - Dispute/Chargeback management

The Payments Operations Team is responsible for undertaking the following activities to manage Chargebacks/Disputes:

- Management of Card Acquirer/Service Provider relationships;
- Loading of Chargebacks/Disputes requests into Venue Smart's CRM as a "ticket";
- Distribution of Chargeback/Dispute notifications and requests for "proof of purchase" to Merchants;
- Collection of "proof of purchase" details from the Merchant;
- Distribution of Chargeback/Dispute "proof of purchase" details to the Card Acquirer/Service Provider before expiry of any SLA requested;
- Management and reporting of Chargebacks/Dispute statistics (i.e number, value, declined/approved per Merchant) to the General Manager Payments;
- Notification of declined Chargebacks/Disputes to Finance for recovery from the Merchant; and
- Management of any escalation of a declined Chargebacks/Disputes with the Card Acquirer/Schemes or the Service Provider.

13.2 Types of Chargebacks/Disputes

Chargebacks/Dispute by a cardholder/bank account holder are typically initiated as a result of the following:

- Non delivery of goods/services by the Merchant;
- Faulty or poor quality goods that are returned;
- Poor quality services that are disputed; and
- Fraudulent use of a credit or debit card or bank account by a cardholder/bank account holder.

In some cases cardholders/payers raise disputes to secure Chargebacks/Disputes on purpose so as to get free goods or services. This is called a "false" Chargeback or Dispute. These types of Chargebacks/Disputes will be reported to the Card Acquirer/Service Provider for them to report to the Scheme/Issuer or Police as fraud.

13.3 Chargeback, Disputes and Refunds Limits

Venue Smart operates the following Chargeback, Dispute and Refund thresholds:

- Merchants who have between 2% and 5% of their total monthly turnover for 3 consecutive months or greater than 5% for one month are to receive correspondence stating that they are on notice for continuous/excessive Chargebacks, Disputes or Refunds. These Merchants are to be monitored and educated on best practices to reduce Chargeback, Disputes and Refunds; and

- Merchants who have between 5% and 10% of their total monthly turnover for 3 consecutive months or greater than 10% for one month are to be placed on "stop-hold" immediately (i.e no settlements are not to be processed) pending review by the General Manager Payments.

  These Merchants are not to be made active again until:

  - they have satisfactorily explained why the Chargebacks, Disputes or Refunds have occurred
  - they have put in measures to fix the issue
  - The General Manager Payments is satisfied that the continued risk of excessive Chargebacks, Disputes or Refunds is mitigated

It is also Venue Smart's policy that Merchant Chargebacks, Disputes or Refunds across the full Merchant base should not exceed 2% of the total processed payments volume. If the total Chargeback, Dispute or Refund rate exceeds 2% then the Risk Committee/Board is to be informed and measures are to be put in place across all Merchants to reduce the rates.

13.4 Merchant fraud

Merchant fraud is where the Merchant knowingly processes payments with the aim of obtaining value by defrauding a cardholder/bank account holder.

Where a Merchant is proven to defraud a cardholder/bank account holder it is Venue Smart's policy to undertake the following steps:

- The Payments Operations Team must:
  - make the Merchant immediately inactive
  - stop all settlements relating to the Merchant
- The General Manager Payments must:
  - initiate a police complaint
  - report the fraud to the appropriate Card Acquirer or Service Provider
  - report the fraud to Venue Smart's Finance department to provision any likely bad debt from Chargebacks or Disputes

Merchant fraud across the whole customer base should not exceed 0.2% of total Merchant payment processing turnover. Where the Merchant fraud exceeds this limit the General Manager Payments must:

- Inform the Management Team and the Risk Committee/Board
- Merchant risks should be immediately audited/analysed with the aim of:
    - Improving Merchant risk assessment and monitoring practices
    - Reducing risk profiles for Merchants

13.5 Cardholder/Bank Account Holder Fraud

Cardholder/bank account holder fraud operates as follows:

- Cardholder/bank account holder knowingly (to gain advantage) initiates a dispute to generate a Chargeback or a Dispute and claims they did not receive goods or services (false Chargeback/Dispute)
- Cardholder/bank account holder data has been compromised and used by a third party to initiate an unauthorised payment

It is company policy to contact the Merchant and investigate the issue and ensure the Merchant is operating as per the Merchant terms and conditions.

The following steps will be undertaken to recover the Chargeback/Dispute:

- Where the cardholder/bank account holder is shown to be initiating a false Chargeback/Dispute the following actions must be undertaken:
    - The Payments Operations Team must
        - Contact the Merchant and inform them of the issue
        - Suspend the cardholder/bank account holder from the service by blocking the card number, bank account, BPay CRN or NPP PayID.
    - The General Manager Payments must:
        - Inform the Management Team
        - Contact the Card Acquirer or Service provider and inform them of the issue
        - Initiate a complaint to the police
- Where cardholder/bank account holder data is compromised which has resulted in an unauthorised payment being processed then the following actions must be undertaken:
    - The Payments Operations Team must:
        - Attempt to determine where the breach has occurred

        - Initiate any and all fixes necessary to stop the data compromise
        - Contact the Merchant informing them of the issue
    - The General Manager Payments must
        - Inform the Management Team and the Board
        - Contact the Card Acquirer/Service Provider informing them of the issue
        - Contact the Privacy Commission informing of the issue (if the breach is significant and the damage can not be stopped or reversed)

14. Receivables risk management

Venue Smart does not incur receivables credit risk with Merchants that are purely online as all fees are netted off settlements.

Venue Smart does incur receivables credit risk where a Merchant operates a terminal for EFTPOS payments. The receivables credit risk is from the following:

- Non payment of terminal rental; and
- Non payment of terminal value if the terminal is lost/stolen or damaged

To mitigate this risk the following processes are to be implemented:

- The merchant signs a direct debit (from either a bank account or card) for recovery of:
    - Monthly terminal rentals
    - Loss or damage of the terminal
    - The direct debit will be automatically re-presented on any decline after 3 days

Where a Merchants direct debit fails, the following steps are to be followed to recover these funds

- Notify the Merchant the direct debit has declined and it will be re-presented in 3 days.
- Re-present the direct debit after 3 days

If the direct debit declines a second time undertake the following process:

- Notify the Merchant the direct debit has declined a second time and it will be re-presented in 3 days;
- Inform them if the direct debit declines again their account could be suspended and they could be referred to a credit agency and debt collector; and
- Re-present the direct debit after 3 days.

Where a Merchant has **three failed** direct debits the Merchant is to be contacted by the credit department to determine the issue and seek payment of any outstanding monies. If the Merchant is uncontactable or does not pay the outstanding debit within agreed terms then:

- Suspend the account;

- Write off the debt if older than 90 days;
- Refer the Merchant to a credit agency; and
- Refer the debt to a Debt Collector if greater than $500.

15. Reporting and Monitoring

The following reports must be generated my the Payments Operations Team daily and reviewed by the Credit Management Team to ensure the credit risk limits have not been exceeded:

- Merchants on-boarded:
    - Merchant ID
    - Terminal ID
    - Registered name
    - Trading name
    - Address
    - MCC code
    - Industry name
    - KYC check - yes/no
    - Credit Check - yes/no
    - Expected monthly turnover
    - Expected ticket
    - Expected refund turnover
    - Expected ticket
    - Forward date %
    - Supply period
    - MSF
    - Risk level - High, Medium or Low
- Merchants off-boarded;
- Merchant daily turnover with the following details per transaction:
    - Merchant ID
    - Terminal ID
    - Register name
    - Trading name
    - Register address
    - MCC
    - Industry name
    - Risk Level (High/Medium/Low)
    - Value of payment
    - UUID

    - Payment type (proprietary EFTPOS, Scheme, Direct Debit, PayTo, BPay)
    - Transaction types - purchase, refund, void, decline and chargebacks
    - Card type - visa, mastercard, proprietary eftpos
    - Card category - debit or credit
    - Card sub category - standard, premium, commercial
    - Issuer
    - Issuer country
    - Interchange cost
    - Scheme cost
    - EFTPOS cost
    - BPay cost
    - Direct Debit cost
    - Retails Fee generated
- Chargebacks
    - All chargebacks
    - Merchants who have exceeded 2% of daily turnover
- Disputes (by payment type)
    - All Disputes
    - Merchants who have exceeded 2% of daily turnover
- Fees
    - All fees generated
    - Declined direct debits for the day
    - Merchants with unpaid fees

16. Customer Operational and Financial Review

Merchants must be regularly reviewed to ensure that their business is operating within the terms and conditions of their agreement.

All Merchants must be contacted by the Payments Operations Team by telephone (and to have their web sites reviewed and their management team vetted where relevant) at least every 12 months.

The following questions must be asked of the Merchant and validated via the Merchants web site and public registers (i.e. ASIC,) where possible by the Payments Operations Team:

- Has your business ownership structure changed in the last 12 months?;
- Have your directors changed in the last 12 months?;
- Has your principal trading address changed in the last 12 months?;

- Are you still selling the same product/service - if changed what are the differences?;
- Have you changed your business operations significantly since last reviewed?;
- Have you changed your refund or deposit policies/processes in the last 12 months?; and
- Is your business still financially sound?

All Merchants must receive a site visit at least every 24 months. The site visit is to be carried out by an account manager. The account manager is to enquire at the site visit (and seek evidence where appropriate) of the following:

- Has your business ownership structure changed since the last review?;
- Have your directors changed since the last review?;
- Has your principal trading address changed since the last review?;
- Are you still selling the same product/service since the last review? - if changed what are the differences?;
- Have you changed your business operations significantly since last reviewed?;
- Have you changed your refund or deposit policies/processes since the last review?; and
- Is your business still financially sound?

Where a Merchant does not meet the terms and conditions of their agreement the following steps are to be taken by the Payments Operations Team:

- Where the breach of terms and conditions is considered material (i.e. high risk) - make the Merchant facility inactive while the Merchant seeks to adhere to the terms and conditions;
- Where the breach of terms and conditions is considered immaterial (i.e low risk) - negotiate for the Merchant facility to remain open while the Merchant seeks to adhere to the terms and conditions
- Always check the nature of the breach against the contractual terms (i.e. Venue Smart's rights, powers and remedies under the Merchant agreement) and take appropriate action based on the level of risk; and
- Where the Merchant changes are deemed acceptable re-negotiate new fees and new risk profile to cater for change in the Merchant risk profile

17. Changes to Credit Risk Policy Limits

If the Merchant wishes to exceed the Credit Risk Policy limits loaded within the risk profile relating to the Merchant the Merchant must contact the General Manager Payments who must seek approval from the Compliance Manager in writing before the limit is increased.

Limits should only be increased where the Merchant has at least a 12 month history of trade with Venue Smart without any reported issues.