Payment Glossary
[Confidential]

1. Payment Methods

1.1 Mail Order Telephone Order (MOTO) –

MOTO is a type of card-not-present transaction in which services or products are paid for and delivered via telephone, mail, fax or internet communication. Because MOTO transactions take place without the merchant or the card physically in the property, these transactions are at a higher risk for credit card fraud, than card-present transactions. Therefore, MOTO merchants will likely pay higher transaction rates to help offset the potential for disputed transactios and chargebacks. MOTO are manually entered into your payment gateway by means of a virtual terminal.

2. eCommerce –

An e-commerce payment system facilitates the acceptance of electronic payment for online transactions. e-commerce payment systems have become increasingly popular due to the widespread use of the internet-based shopping and banking

3.

eCommerce transactions are vulnerable to fraud, customer disputes and chargebacks to a much greater degree than card-present transactions. The main reason for why this is the case, is that the merchant can physically verify the validity of the card used for payment and the authen-ticity of the cardholder.

3.1 Chip & Pin

A Chip & PIN card is a card or debit card that contains data embedded in a microchip and requires the consumer to enter a personal identification number (PIN) to complete a purchase transaction.
Chip & PIN transactions are card-present transactions. Chip & PIN is a UK government-backed initiative to implement the EuroPay, MasterCard and VISA (EMV) standard for smart card payments.
The consumer enters a 4-digit PIN that is checked against the information embedded in the microchip on the card for the transaction to proceed.

3.2 Alternative Payments Methods –

An Alternative Payment Method (APM) is a way of paying for goods or services outside to the mainstream credit card schemes, such as VISA, MasterCard or American Express. Most APMs address a domestic economy or have been specifically developed for eCommerce and the payment systems are generally supported and operated by local banks. Each APM has its own unique application and settlement process, language and currency support, and is subject to domestic rules and regulations

3.3 Person to Person (P2P) –

P2P is an online technology that allows customers to transfer funds from their bank account or credit card to another individual's account via the Internet or a mobile phone.

There are 2 approaches for initiating a P2P payment:

1) Users establish secure accounts with a trusted 3rd party vendor, designating their bank account or credit card information to be used to transfer and accept funds. Using the 3rd party's website or mobile app, individuals can complete the process of sending or receiving funds. Users are generally identified by their email address and can send funds to anyone who is a member or the network.
2) Users use an online interface or mobile app (developed by their bank or financial institution) to designate the amount of funds to be transferred. The recipient is designated by their email address or phone number. Once the transfer has been initiated by the sender, the recipient receives a notification to use the online interface to input their banking information and routing number to accept the transfer of funds. Receipients do not need to have an account with financial institution of the sender in order to receive the money transfer.

3.4 Automated Clearing House (ACH) –

ACH payments are electronic payments that are created when an user gives the originating institution, corporation or other user (originator) authorization to debit directly from the user's checking or savings account for the purpose of payments in the US. The Automated Clearing House (ACH) Network is an electronic funds-transfer system run by NACHA (National Automated Clearing House Association). This payment system deals with payroll, direct deposit, customer bills, tax refunds, tax payments and payment services in the US.

3.5 Digital Wallet –

A digital wallet is a system that securely stores user's payment information and passwords for numerous payment methods and websites. By using a digital wallet, users can complete purchases easily and quickly with Near Field Communication (NFC) technology. Digital wallets can be used in conjunction with mobile payment systems, which allow consumers to pay for purchases with their smart phones. A digital wallet can also be used to store loyalty and digital coupons. A digital wallet is also known as an e-wallet.

3.6 Single Euro Payments Area (SEPA) –

SEPA is a payments system created by the European Union (EU) which enables cashless payments transactions between euro countries. European customers, businesses, and government agencies who make payment by direct debit, credit card or through credit transfers use the SEPA architecture. The single euro payment area is approved and regulated by European Commission.

The purpose of SEPA is to make cross border electronic payments as inexpensive and easy as payments within one country.

3.7 Bankers' Automated Clearing Services (BACS) –

Bacs Payment Schemes Limited (Bacs), previously known as Bankers' Automated Clearing Services, is the organisation responsible for the schemes behind the clearing and settlement of UK automated payment methods Direct Debit and Bacs Direct Credit, as well as the provision of managed services for third parties. Bacs became a subsidiary of Pay.UK on May 1, 2018 and as a result has the overall responsibility for the operations of Direct Debit, Basc Direct Credit, the Current Account Switch Service, Cash ISA Transfer Service and the Industry Sort Code Directory.

3.8 Transaction –

A transation is an agreement between a buyer and seller to exchange goods, services or financial instruments.

3.9 Payment –

A payment is the transfer of one form of good, service or financial asset in exchange for another form of good, service or financial asset in proportions that have been previously agreed upon all parties involved.

3.10 Refunds –

The most common chargebacks occur when a cardholder chooses to return an item. If the return is within the merchant's allowable timeframe the merchant can initiate a chargeback as a refund.

3.11 Chargeback –

A chargeback is a charge that is returned to a payment card after a customer successfully disputes an item on his account transactions report. A chargeback can be considered a refund since it returns specific funds taken frome an account through a prior purchase. Chargebacks are focused on charges that have been fully processed or settled. Chargebacks can be initiated by either the merchant or the cardholder's issuing bank. If initiated with a merchant the process is similar to a standard transaction however the funds are taken from a merchant's account and deposited with the cardholder's issuing bank.

For example a chargeback initiated by a merchant would begin with a request sent to the merchant's acquiring bank from the merchant. The acquiring bank would then contact the card's processing network to send payment from the ***merchant's account*** at the merchant bank to the cardholder's account at the issuing bank.

If a chargeback is initiated by the issuing bank then the issuing bank facilitates the chargeback through communication on their processing network. The merchant bank then receives the signal and authorizes the funds transfer with the confirmation of the merchant. In some cases, such as with fraudulent charges, the issuing bank may grant the cardholder with a chargeback while also sending the claim to a collection department. In this case a bank takes on the liability and expenses the chargeback through reserve funds while researching and resolving the claim.

Merchant acquiring banks will generally charge a fee to merchants for chargeback transactions. These fees are detailed in a merchant account agreement. Fees are typically charged per transaction to cover the costs by the processing network. Additional penalties for chargebacks may also apply.

3.12 Deposit/Advanced payment –

An advance payment is a type of payment made ahead of its normal schedule such as paying for a good or service before you actually receive it. The balance that is owed, if any, is paid once delivery is made.

3.13 Prepaid -

Unlike a debit card, a prepaid card is not linked to a bank account. Generally, when you use a prepaid card, you are spending money that you have already loaded onto the card.

4. Payment Intervenient

4.1 Payment Gateway –

A payment gateway refers to the front-end technology that reads payment cards and sends customer information to the merchant acquiring bank for processing. The payment gateway is an important aspect of all electronic payment card processing.

Payment gateway technology can vary for online merchants and brick and mortar businesses. The payment gateway will be constructed differently for an online company versus a brick and mortar business however the transaction process is still the same.

Websites will require application programming interfaces (APIs) that plug into the online system through programming that enables their functionality. For a brick and mortar business, the company will require a point of sale terminal that connects electronically through either a phone line or internet connection.

All payment gateways serve as the first step in an electronic payment transaction. The payment gateway technology transmits a customer's card information to the merchant acquiring bank. The merchant acquiring bank then facilitates the authorization of the transaction through communication with the processor and issuing bank.

4.2 Acquiring –

Acquiring is the process of obtaining funds from a cardholder using the Card Schemes. Acquiring is a licensed activity and approval is necessary from both the card scheme and the Financial Regulator of the region.

4.3 Sales Organization (ISO) –

"ISO" stands for "Independent Sales Organization" and is a formal designation that a company must have in order to sell Visa credit card processing services under its own company name. Visa displays its registered and approved ISOs on the Visa ISO List. In many cases, sales organizations operate as "ISOs" under a Visa-approved ISO in a sales partnership. In these cases the sales organization may have its own company name, but it sells merchant accounts branded under the actual Visa-approved ISO. Visa-approved ISOs represent an Acquiring Bank, or Processor, or both. ISOs are also allowed to set terms of their own merchant account contracts and mark up processing rates and fees. Although a Processor can also be an ISO, most ISOs are solely sales organizations that act as "middle men" that market point-of-sale solutions (terminals, payment gateways, mobile accessories, etc.) and pair them with acquirers and processors. MasterCard has a similar designation called an MSP.

4.4 Member Service Provider (MSP) –

See 2.3 above

4.5 Payment Facilitator –

A Payment Faciliator (PayFac) is a merchant service provider that simplieds the merchant account enrolment process. PayFacs operate on a sub-mercahnt platform where merchants no longer require their own MID, but are boarded directly under the PayFac's master MID Account.

4.6 Payment Processor –

Payment processors enable merchants to receive debit or credit card payments online by providing a connection to an acquiring bank. These processors perform many functions such as evaluating whether transactions are valid and approved, using anti-fraud measures to assure that a purchase transaction is initiated by the source it claims to be. Processors are held to standards and regulations organized by credit card associations. These standards include rules regarding fraud, chargebacks, and identity theft.

4.7 Issuing Bank –

The financial institution that grants debit or credit cards through the card associations is what is known as issuing bank. They offer card association branded payment cards directly to consumers.

4.8 Payment/Card Network –

The card network decides where their partnered, branded credit cards can be used. They also facilitate the payments made from each credit card user to the merchant through the bank. There are four major card networks – VISA, MasterCard, American Express and Discover. They are also known as card associations and schemes.

4.9 Merchant –

Merchant is defined as a person or company engaged in the business of selling or trading goods and services.

4.10 Merchant ID (MID) –

An MID or Merchant Identification Number is a unique code given to a business by payment processors before a merchants begin processing credit cards. ... In addition to a merchant identification number, a terminal identification number will also be used, in addition to a merchant account ID.

5. Commissions and Fees

5.1 Interchange fee

An interchange rate is a fee charged by banks that covers the cost of handling and credit risk inherent in a bank credit or debit card transaction. Interchange fees are usually paid to the bank funding a transaction and thus bearing the risk.

InterChange (IC) ++

Interchange++ is a type of pricing most commonly used in Europe and the United States. It's available for payments made through Visa and Mastercard, and offers more transparency than other pricing types by showing a more detailed breakdown of your costs.

When a card transaction is processed through an acquirer, there are three different cost components.

- The Interchange fee that goes to the card issuing bank,
- The scheme fee that goes to Visa or Mastercard (first +) , and
- The acquirer fee (second +)

Scheme fees and Interchange fees are driven by variables such as the card level (platinum / commercial), by country of merchant and the issuer, merchant segment, transaction type (online payments / POS payments) and many more.

The fees are set by the card schemes Visa and Mastercard and are regulated in some countries.

5.2 Blended rate -

Another word for bundled pricing, blended pricing is a pricing structure for credit card payment processors. It works by setting the same rate structure for all merchant account transactions into one flat level rate, usually a percentage of volume of sales.

5.3 Scheme fee –

Card scheme fees are a cost to the acquirer from the card schemes. Card acquirers typically pass these fees to the merchant.

5.4 Settlement commission –

Annual projected processing volume – The total value of all transactions a processor will allow a merchant to perform in credit card sales each year is known as its processing volume.

5.5

5.6 Average transaction value –

The average transaction value (ATV) is calculated by dividing the total value of all transactions by the number of transactions or sales. This can be calculated on a daily, monthly or annual basis.

6. Compliance

6.1 Payment Card Industry Data Security Standard (PCI DSS) -

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards from the major card schemes. ... The standard was created to increase controls around cardholder data to reduce credit card fraud.

6.1.1 Level 1

All merchants fall into one of the four merchant levels based on Visa transaction volume over a 12-month period. Transaction volume is based on the aggregate number of Visa transactions (inclusive of credit, debit and prepaid) from a merchant Doing Business As ('DBA'). In cases where a merchant corporation has more than one DBA, Visa acquirers must consider the aggregate volume of transactions stored, processed or transmitted by the corporate entity to determine the validation level. If data is not aggregated, such that the corporate entity does not store, process or transmit cardholder data on behalf of multiple DBAs, acquirers will continue to consider the DBA's individual transaction volume to determine the validation level.

Any merchant — regardless of acceptance channel — processing over 6M Visa transactions per year. Any merchant that Visa, at its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the Visa system.

6.1.2 PCI PTS V4.0

The Point Of Sale Pin Transaction Security Standard (PCI PTS) Overview: PCI PTS are technical and operational requirements set to protect cardholder data. The standards apply to all organizations that store, process or transmit cardholder data.

Version 4 was relevased in June, 2013. With V.4, PCI no longer maintains three separate security evaluation programs (point-of-sale PIN entry device (PED), encrypting PIN pad (EPP), and unattended payment terminal (UPT)). Instead PCI provides and supports one set of modular requirements, which covers all product options.

6. Compliance

6.1 Payment Card Industry Data Security Standard (PCI DSS) -

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards from the major card schemes. ... The standard was created to increase controls around cardholder data to reduce credit card fraud.

6.1.1 Level 1

All merchants fall into one of the four merchant levels based on Visa transaction volume over a 12-month period. Transaction volume is based on the aggregate number of Visa transactions (inclusive of credit, debit and prepaid) from a merchant Doing Business As ('DBA'). In cases where a merchant corporation has more than one DBA, Visa acquirers must consider the aggregate volume of transactions stored, processed or transmitted by the corporate entity to determine the validation level. If data is not aggregated, such that the corporate entity does not store, process or transmit cardholder data on behalf of multiple DBAs, acquirers will continue to consider the DBA's individual transaction volume to determine the validation level.

Any merchant — regardless of acceptance channel — processing over 6M Visa transactions per year. Any merchant that Visa, at its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the Visa system.

6.1.2 PCI PTS V4.0

The Point Of Sale Pin Transaction Security Standard (PCI PTS) Overview: PCI PTS are technical and operational requirements set to protect cardholder data. The standards apply to all organizations that store, process or transmit cardholder data.

Version 4 was relevased in June, 2013. With V.4, PCI no longer maintains three separate security evaluation programs (point-of-sale PIN entry device (PED), encrypting PIN pad (EPP), and unattended payment terminal (UPT)). Instead PCI provides and supports one set of modular requirements, which covers all product options.

In that process, the standard also dictates that software vendors develop payment applications that are compliant with the Payment Card Industry Data Security Standards (PCI DSS).

For a payment application to be deemed PA-DSS compliant, software vendors must ensure that their software includes the following fourteen protections:

1. Do not retain full track data, card verification code or value (CAV2, CID, CVC2, CVV2), or PIN block data.
2. Protect stored cardholder data.
3. Provide secure authentication features.
4. Log payment application activity.
5. Develop secure payment applications.
6. Protect wireless transmissions.
7. Test payment applications to address vulnerabilities and maintain payment application updates.
8. Facilitate secure network implementation.
9. Cardholder data must never be stored on a server connected to the Internet.
10. Facilitate secure remote access to payment application.
11. Encrypt sensitive traffic over public networks.
12. Secure all non-console administrative access.
13. Maintain a PA-DSS Implementation Guide for customers, resellers, and integrators.
14. Assign PA-DSS responsibilities for personnel, and maintain training programs for personnel, customers, resellers, and integrators.

6.3 Tokenisation –

The PCI Council defines tokenization as "a process by which the primary account number (PAN) is replaced with a surrogate value called a token. The encrypted card number is stored off-site in a Paymetric secure, PCI-compliant data vault. Tokenization frees merchants from having to keep credit card data within their payment systems. This helps to reduce their PCI scope and expense.

6.4 Encryption –

Encryption is the process of encoding payment data so that only authorized parties (with the right encryption key) can view it. Point to Point Encryption (P2PE) ensures that credit card data that must be collected and transmitted after a purchase is encrypted by a one time encryption key as soon as the card is swiped into the card reader. ... The decryption keys are stored in an isolated Hardware Security Module (or HSM) at the payment gateway.

6.5 Europay, MasterCard and Visa (EMV) –

EMV (Euvropay MasterCard Visa) is a worldwide standard for payment cards that provides global interoperability between all cards and the acceptance networks (Payment Terminals). The EMV standard is also applicable to mobile payment solutions such as mobile EMV with NFC (Near-field-communication).

EMV Payment is based on chip&PIN technology i.e. the use of a secure element (Certified Silicon chip) and a PIN code used by the cardholder to secure his/her payment transactions.

A vast majority of countries have already experienced a migration from their key financial institutions from an older technology based on cards using a magnetic stripe to store the cardholder credentials to the more secure, more interoperable EMV cards that can be used across the world.

The rationale and motivation for this motivation is threefold:

- First the level of fraud is drastically reduced in markets where EMV is deployed,
- second cardholders can use their payment cards when travelling abroad thanks to the ubiquity of service of the EMV global architecture, and
- third there is an incentive to migrate to EMV support for merchants who don't want to bear the financial liability of fraud such as markets that are supporting older magnetic stripe technology.

6.6 General Data Protection Regulation (GDPR) –

The General Data Protection Regulation (EU) 2016/679 ("GDPR") is a regulation in EU law on data protectionand privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). It also addresses the export of personal data outside the EU and EEA areas. The GDPR aims primarily to give control to individuals over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

6.7 Attestation of Compliance (AOC)

AOC (Attestation of Compliance) The AOC is a form used by merchants and service providers to attest to the results of a PCI DSS assessment.

6.8 Qualified Security Assessor (QSA)

Qualified Security Assessor (QSA) companies are independent security organizations that have been qualified by the PCI Security Standards Council to validate an entity's adherence to PCI DSS.

6.9 Card data environment (CDE)

A cardholder data environment (CDE) is a computer system or networked group of IT systems that processes, stores and/or transmits cardholder data or sensitive payment authentication data. A CDE also includes any component that directly connects to or supports this network.

6.10 Address Verification System (AVS)

The Address Verification System (AVS) is a system used to verify the address of a person claiming to own a credit card. The system will check the billing address of the credit card provided by the user with the address on file at the credit card company.

6.11 Card Verification Number (CVN)

Card verification number (CVN) is a three-digit security number that usually appears on the back of your credit or debit card. Sometimes called a card security code or card verification value, it provides extra protection against fraud.

6.12 Card Validation Code (CVV2)

CVV2 stands for “Card Verification Value 2”, CVV and CVV2 actually refer to the same thing: the security code printed on your credit card. The difference is that CVV2 technically describes the three-digit code on the back of Visa cards, in particular.

6.13 Cardholder ID (CID)

The Credit Card Identification Number is the 3-digit number located on the back of your card, usually at the top of the signature strip. For American Express, the CID is a 4-digit number printed on the front of the card.

6.14 Card Security Code (3CSC)

The Card Security Code is usually a 3- or 4-digit number, which is not part of the credit card number. The CSC is typically printed on the back of a credit card (usually in the signature field).

6.15 Triple DES Encryption (Batch processor)

Triple Data Encryption Standard (DES) is a type of computerized cryptography where block cipher algorithms are applied three times to each data block. The key size is increased in Triple DES to ensure additional security through encryption capabilities. Each block contains 64 bits of data. Three keys are referred to as bundle keys with 56 bits per key. There are three keying options in data encryption standards:

1. All keys being independent
2. Key 1 and key 2 being independent keys
3. All three keys being identical

Key option #3 is known as triple DES. The triple DES key length contains 168 bits but the key security falls to 112 bits.

Triple DES encrypts input data three times. The three keys are referred to as k1, k2 and k3.

6.16 Point to point encryption (P2PE)

Through a combination of secure devices, applications, and processes, businesses can encrypt data directly from the point of interaction to the point-to-point encryption solution provider's secure decryption environment. This means the data isn't decipherable to anyone who might steal it during the transaction process, and thus lacks value for thieves. Merchants using a PCI P2PE solution have the advantage of more simplified compliance efforts, because they are subject to fewer PCI DSS requirements.

6.17 Secure Sockets Layer (SSL)

SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral.

6.18 Transport Layer Security (TLS)

Transport Layer Security (TLS), and its now-deprecated predecessor, Secure Sockets Layer(SSL), are cryptographic protocols designed to provide communications security over a computer network. ... The TLS protocol aims primarily to provide privacy and data integrity between two or more communicating computer applications.

The differences between the two protocols are very minor and technical, but SSL and TLS are different standards. TLS uses stronger encryption algorithms and has the ability to work on different ports. Additionally, TLS version 1.0 does not interoperate with SSL version 3.0.

6.19 Hypertext Transfer Protocol Secure (HTTPS)

Hypertext Transfer Protocol Secure (HTTPS) is an extension of the Hypertext Transfer Protocol (HTTP). It is used for secure communication over a computer network, and is widely used on the Internet. In HTTPS, the communication protocol is encrypted using Transport Layer Security (TLS), or, formerly, its predecessor, Secure Sockets Layer (SSL). The protocol is therefore also often referred to as HTTP over TLS, or HTTP over SSL.

The principal motivation for HTTPS is authentication of the accessed website and protection of the privacy and integrity of the exchanged data while in transit. It protects against man-in-the-middle attacks.
The bidirectional encryption of communications between a client and server protects against eavesdropping and tampering of the communication. In practice, this provides a reasonable assurance that one is communicating without interference by attackers with the website that one intended to communicate with, as opposed to an impostor.

6.20 3D Secure v2.0

3-D Secure 2 is version 2 of 3D Secure. It will supports the transmission of rich data during transactions, making risk-based decisions possible on whether to authenticate or not. The consumer experience will also be simplified and enhanced, through the elimination of the initial enrolment process and removing the need for cardholders to remember static passwords. Non-payment authentication and native mobile support are also included in this version of the protocol.

6.21 PSD2

PSD2 is the second Payment Services Directive, designed by the countries of the European Union. The revised Payment Services Directive (PSD2) aims to better align payment regulation with the current state of the market and technology, and introduces security requirements for the initiation and processing of electronic payments, as well as for the protection of consumers' financial data.

6.22 Strong Customer Authentication (SCA)

Strong customer authentication (SCA) is defined as “an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is). Strong Customer Authentication (SCA) is a new European regulatory requirement to reduce fraud and make online payments more secure.

. To accept payments once SCA goes into effect, you will need to build additional authentication into your checkout flow. SCA requires authentication to use at least two of the following three elements.

- Something the customer knows (e.g., password or PIN)
- Something the customer has (e.g., phone or hardware token)
- Something the customer is (e.g., fingerprint or face recognition)

Starting 14 September 2019, banks will decline payments that require SCA and don't meet these criteria.

7. Hardware (POS Hardware)

7.1 PIN Entry Devices (PED) –

A PIN pad or PIN entry device is an electronic device used in a debit, credit or smart card-based transaction to accept and encrypt the cardholder's personal identification number (PIN). PED Security Requirements (managed by PCI SSC) are primarily concerned with device characteristics impacting the security of the PIN Entry Device used by the cardholder during a financial transaction.

7.2 Card Machine –

A Credit Card Terminal, also called an Electronic Data Capture Terminal or EDC Terminal for short, is an electronic device that enables merchants to accept credit cards at the point of sale.

7.3 Point of Sale (POS) –

A POS or point of sale purchase is the "point" where a transaction is finalized or the moment where a customer tenders payment in exchange for goods and services. Any form of payment can be used, such as cash, debit cards, credit cards, mobile payments, and even Bitcoin

7.4 Till -

In a store or other place of business, a till is a counter or cash register where money is kept, and where customers pay for what they have bought.

7.5 Terminal –

A payment terminal, also known as a Point of Sale (POS) terminal, credit card terminal, EFTPOS terminal (or by the older term as PDQ terminal which stands for "Process Data Quickly" or in common jargon as "Pretty Damn Quick"), is a device which interfaces with payment cards to make electronic funds transfers.

7.6 Near-field communication (NCF)

Near-field communication (NFC) is a set of communication protocols that enable two electronic devices, one of which is usually a portable device such as a smartphone, to establish communication by bringing them within 4 cm (1.6 in) of each other. NFC devices are used in contactless payment systems, similar to those used in credit cards and electronic ticket smart cards and allow mobile payment to replace or supplement these systems. This is sometimes referred to as NFC/CTLS (contactless) or CTLS NFC.

7.7 Leasing –

A lease is a contractual arrangement calling for the lessee (user) to pay the lessor (owner) for use of an asset. The lessor is the legal owner of the asset; the lessee obtains the right to use the asset in return for regular rental payments. The lessee also agrees to abide by various conditions regarding their use of the property or equipment.

7.8 Rent –

Rent is a fixed amount of money that you pay regularly for the use of tangible asset, that someone else owns.

8. Others

8.1 Underwriting –

Merchant underwriting is the process of evaluating the cost of assuming the risk of a merchant as a potential customer by a payment processor or lender.

8.2 Settlement –

Settlement is the exchange of funds between a card issuer and an acquiring bank to complete a cleared transaction and the reimbursement of a merchant for the amount of each card sale that has been submitted into the network..

8.3 Net settlement –

Merchant accounts are typically funded daily and the net settlement total is calculated as from the face amount of the submitted charges are subtracted all applicable deductions, which may include the following:

- Discount fees. These are the fees your processor charges you for each card transaction. They are specified in your merchant agreement.
- Amounts you may owe to your processor.
- Any chargeback amounts.
- Any credit amounts you may have submitted.

8.4 Gross settlement –

With Gross Settlement, the merchant is paid the full amount of the submitted charges, and then a second adjustment/invoice is applied to deduct the discount and other applicable amounts.

8.5 Multi-Currency Conversion (MCC)

Multi-currency pricing (MCP) is a financial service which allows businesses to price goods and services in a variety of foreign currencies, while continuing to receive settlement and reporting in their home currency.

8.6 Dynamic Currency Conversion (DCC)

Dynamic currency conversion (DCC) or cardholder preferred currency (CPC) is a process whereby the amount of a Visa or MasterCard transaction is converted by a merchant or ATM to the currency of the payment card's country of issue at the point of sale.

8.7 Reconciliation –

Reconciliation is an accounting process that uses two sets of records to ensure figures are correct and in agreement. It confirms whether the money leaving an account matches the amount that's been spent, and ensures the two are balanced at the end of the recording period.

9. Technology

9.1 Application Programming Interface (API)

An application programming interface, or API, is a "go-between" that enables a software program to interact with other software.

9.2 Software Development Kit (SDK) –

A software development kit (SDK or devkit) is typically a set of software development tools that allows the creation of applications