Payment Facilitator

Operational Guidelines & Procedures

-March 2016-

Table of Contents

1. Introduction

The Netpay Ltd. Operational Guidelines and Procedures booklet, “Payment Facilitator,” provides guidance for the organization - Netpay Ltd. -managers, employees and examiners on merchant processing activities. For purposes of this booklet, a merchant processing activity is the settlement of credit and debit card payment transactions by the organization for merchants through various card associations. This booklet focuses on card payment-related processing.

2. Background

Consumers

Consumers are individuals or organizations that intend to make a purchase. Consumers may be motivated to select a particular merchant by several things: price, service, selection or preference.

Merchants

Merchants are entities looking to sell their goods and services to consumers.

Issuing Banks

Consumers get their credit cards from a bank or a credit union, called the “issuing bank” or “issuer”. These are branded credit cards like MasterCard, Visa, American Express but also credit cards called “Private Label Credit Cards” such Target cards.

The purpose of the issuing bank is to grant credit directly to a consumer, gaining on the interest the consumer pays on outstanding balances from previous purchases and getting a part of every purchase a consumer makes with the card from a merchant.

Acquiring bank (acquirer)

A bank that contracts with merchants for the settlement of payment card transactions is an acquiring bank.

Acquiring banks contract directly with merchants, or indirectly through agent banks or other third-party organizations, to process card transactions.

The acquiring bank generally provides all backroom operations to the agent bank and owns the bank identification number (BIN)/Interbank Card Association (ICA) number through which settlement takes place.

Payment Facilitator (PF) or Payment Service Provider (PSP)

MasterCard defines a payment facilitator as a merchant that is registered by an acquirer to facilitate transactions on behalf of sub-merchants.

Under Visa’s rules, a payment service provider is an organization that contracts with an acquirer to provide payment services to sponsored merchants.

The payment facilitator and the payment service provider (collectively, PSP) are operationally similar. In both cases, the acquirer is responsible for the actions of its PSP and the PSP’s sponsored merchants.

Card Associations

Card associations are entities like MasterCard, Visa, America Express and more.

They are responsible for setting up the guidelines on how transactions, services and disputes are handled and interface with national banking laws. Each card association has is own network of systems, policies for use and payment processing.

3. Operations

This section summarizes how card transactions are processed. The intricacies may vary significantly for each bank, but the basic principles are the same.

Authenticating Transactions

The first step in authorizing payment card transactions is to verify the identity of the individual cardholder. Card association rules address cardholder authentication and vary based on the type of card transaction, the merchant category, the amount of the transaction and how the cardholder initiates the transaction. This ensures that the person presenting the card for payment is authorized to use the card. Transactions can be authenticated by using a signature code (a three- or four-digit code located typically on the back of the card) or other methods.

Authorizing Transactions

Authorization is the process of approving or declining a transaction before a purchase is finalized or cash is disbursed. After authentication, the merchant obtains approval from the card-issuing bank or from a third party acting on behalf of the card-issuing bank.

Figure 1 illustrates the authorization process.

This authorization process is structured to prevent transactions from being approved for cardholders who have not satisfactorily maintained their card accounts or who are over their credit limits, and to protect against the unauthorized use of cards that have been reported as stolen or as fraudulent. Authorization systems may include internally or externally developed platforms, or a combination of both.

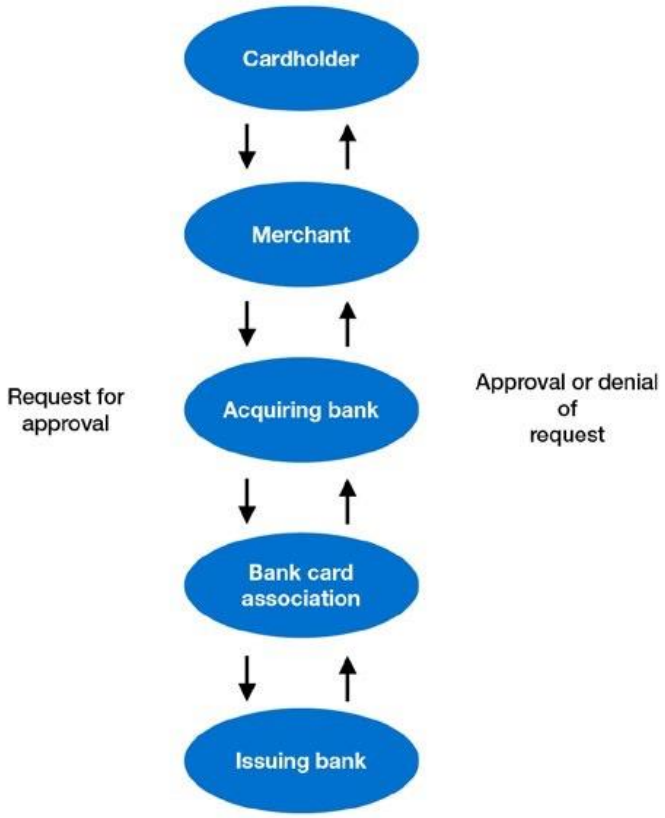

Figure 1. Authorization Process

Typically, the clerk or cardholder swipes the card through a terminal at the point of sale to obtain the information stored on the magnetic stripe on the back of the card, and then inputs the amount of the transaction. This information is transmitted to the acquiring bank or the acquiring bank's processor, which captures the transaction and forwards the information to the card-issuing bank through the bank card association network. Depending on the status of the cardholder's account, the transaction is approved or declined, and this decision is transmitted back through the bank card association network to the point of sale.

Bank card associations have implemented simpler rules for some in-person card transactions. For example, customer signatures or personal identification numbers are not required for transactions

meeting certain low-dollar criteria and where the merchant's business falls into certain business code categories; authentication, however, is required. The threshold for low dollar transactions varies depending on the particular bank card association and the approved merchant category code allowed by the bank card association.

Acquiring banks require authorizations for all paper-based transactions. Ensuring that each paper-based transaction is authorized and helps protect merchants against fraudulent transactions. While paper-based transactions still occur, most transactions are now processed electronically.

Clearing and Settlement

Clearing is the process of delivering final transaction data from acquirers to issuers for posting to the cardholder's account. Clearing also includes the calculation of certain fees and charges that apply to the issuer and acquirer involved in the transaction, as well as the conversion of transaction amounts to the appropriate settlement currencies.

Settlement is the process of transmitting sales information to the card-issuing bank for collection and reimbursement of funds to the merchant. Settlement also refers to the process of calculating, determining, and reporting the net financial position of issuers and acquirers for all transactions that are cleared.

Figure 2 illustrates the clearing and settlement process.

A typical transaction flows from the merchant to the acquirer (or acquirer's processor), then to the bank card association, and finally to the card-issuing bank (or its processor), which bills the cardholder.

Funds flow in the opposite direction, or from the card-issuing bank to the bank card association, then to the acquirer, and finally to the merchant.

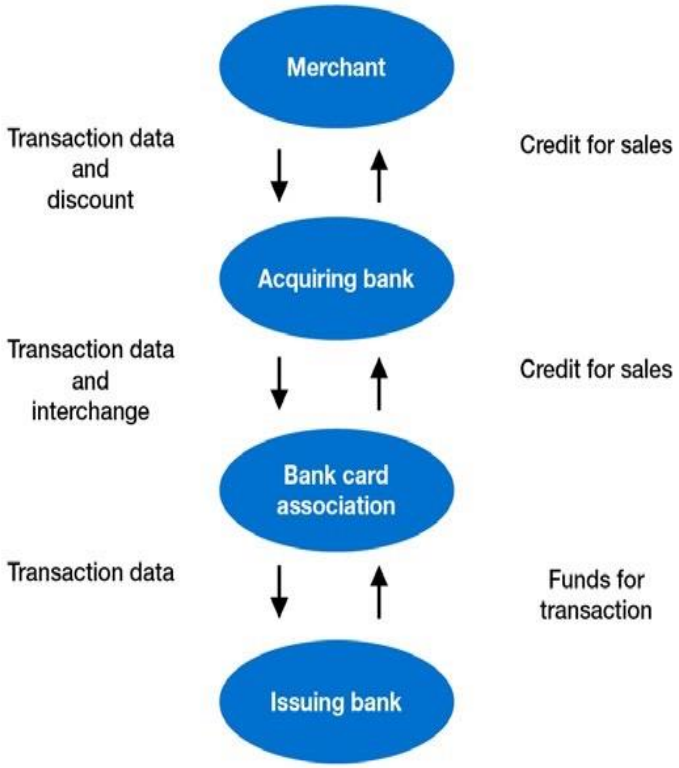

Figure 2. Clearing and Settlement Process

Note: This figure does not illustrate the added complexities associated with using third-party organizations as PF or PSP.

Large merchants often transmit data directly to the acquirer or third-party organization. Smaller merchants usually submit data to a third-party organization that collects data from several merchants. The third-party organization then transmits transactions to the acquirers.

The acquiring bank transmits the information through an interchange to the issuing bank. The issuer remits funds, through the bank card association, to the acquirer and posts the charges to the cardholders' accounts. After the acquirer receives the proceeds, it pays the individual merchants. Most third-party processors net settle with their clients. That is, the bank receives, or pays, the net of merchant and cardholder activity for each day of business.

The acquiring bank may pay select merchants before receiving funds through interchange, thereby increasing the bank's credit and liquidity exposure. The timing of the payments to the merchants is specified in the agreement between the acquiring bank and the merchants.

The agreement should always allow the bank to review the transaction for fraud before releasing funds.

The acquiring bank should not become reliant on the merchant's deposits to fund other bank activities.

An acquiring bank is potentially liable for losses caused by merchant fraud, including merchants engaged in deceptive or misleading practices.

A merchant can also directly defraud banks by such means as factoring and laundering. Factoring, also called credit card factoring, is used to launder money via credit cards, essentially by processing transactions through a merchant account for a business or entity other than the specific business that was screened and set up for the merchant account.

Charge-Back Processing

Charge-backs are common in the merchant processing business, and a merchant must be capable of paying them.

Charge-backs fall into four categories.

- Technical: Expired authorization, nonsufficient funds, or bank processing error.
- Clerical: Duplicate billing, incorrect amount billed, or refund never issued.
- Quality: Consumer claims to have never received the goods as promised at the time of purchase.
- Fraud: Consumer claims not to have authorized the purchase, or identity theft.

The consumer's rights and responsibilities vary by the type of payment method used.

For a credit card, the consumer must first try resolving a payment dispute with the merchant. If unsuccessful, the consumer informs the card-issuing bank of the dispute, and then the card issuing bank posts a temporary credit to the cardholder's account. The card-issuing bank requests documentation from the merchant that authenticates the transaction and possibly resolves the dispute. If the charge-back is upheld by the card-issuing bank, the amount is charged back to the merchant's account, and the consumer does not pay for the disputed charge. The customer has 60 days from the day the card statement is received to report a dispute to the card-issuing bank.

The charge-back processing and time frames between the bank and its merchant are generally addressed contractually via the merchant processing agreement.

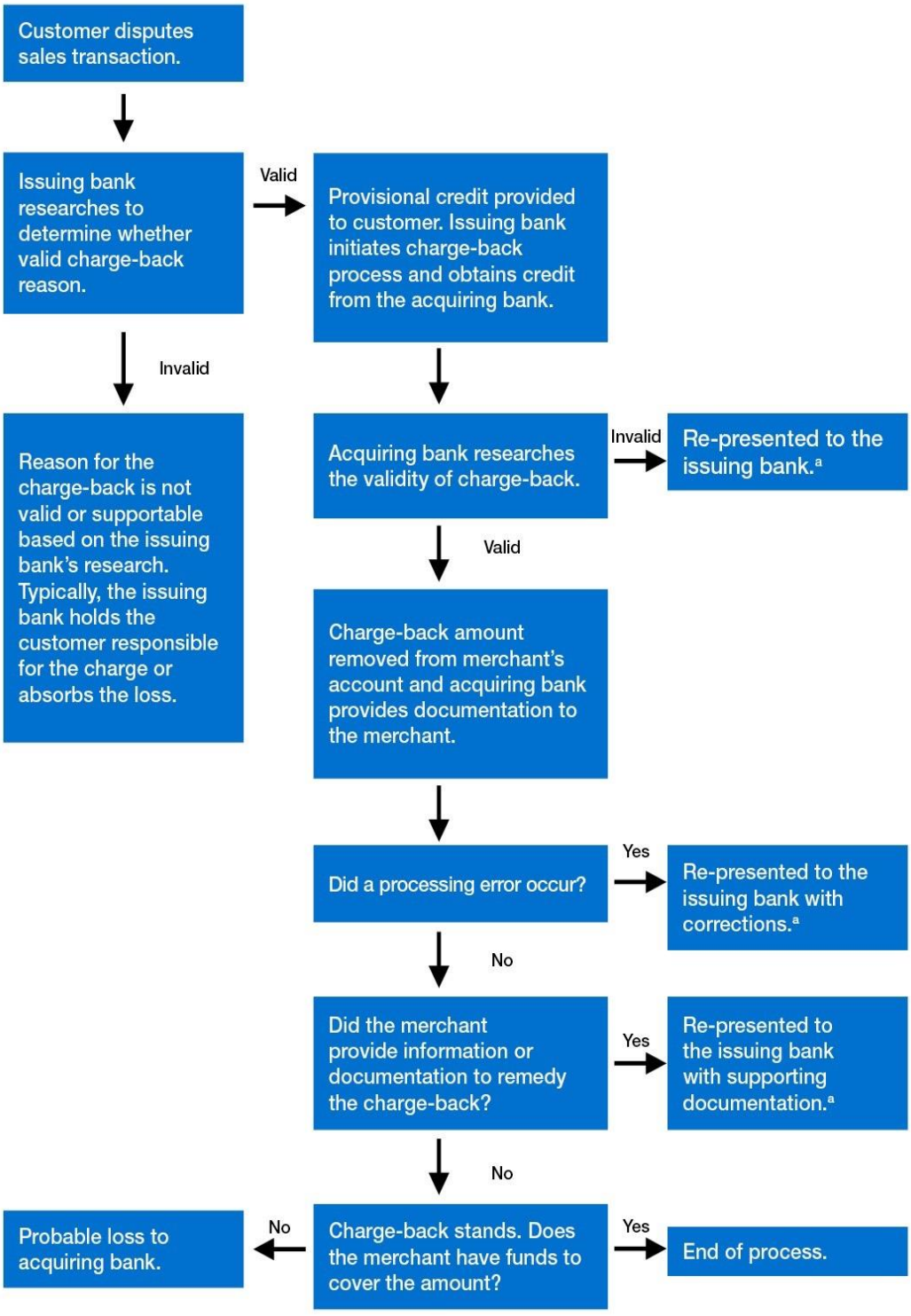

Figure 3. Charge-Back Process for credit transactions

Card-issuing banks can also initiate charge-backs when the merchant does not follow proper card acceptance and authorization procedures (e.g., no authorization obtained or card used after expiration date). The acquirer incurs contingent liability for as long as 180 days.

Bank card associations have strict charge-back processing rules.

For example, an association allows a bank to charge a transaction back to a merchant when the merchant fails to provide copies of the requested sales ticket. If the merchant does not provide a copy of the sales ticket within a prescribed time, the merchant will lose the charge-back dispute.

A retrieval request is used by bank card associations to request items from the merchant. The merchant must have a process to respond to retrieval requests and charge-back investigations in a timely manner.

4. Risk Associated With Merchant Processing

Operational Risk

Payment Facilitators are faced with operational risk daily as they process card transactions for their merchants.

This risk arises primarily from the settlement process.

Settlement is the process of transmitting sales information to the card-issuing bank for collection and reimbursement of funds to the merchant.

Operational risk can also arise from a payment facilitator and bank's failure to process a transaction properly, inadequate controls, employee error or malfeasance, a breakdown in the bank's computer system, or a natural catastrophe.

Among the operational risk exposures are processing risks. A failure anywhere in the transaction process can result in risks to the payment facilitator.

Operational risk exposures arise from the hardware and software used for processing, if there are intrusions or negative alterations, internally or externally.

The same is true for the transaction data that is handled in processing.

Risk also arises if the data is not accessible for necessary monitoring and reports.

Operational and compliance risks arise if personally identifiable information emerges from the merchant processor as a result of social engineering or a cyber attack.

Although data may not be expropriated, cyber attacks can cause degradation or even complete disruption of services to customers, alteration of customer data, and in the worst case, they could lead to the destruction of systems and customer data.

Data stored or data in transmission is at risk.

Fraud risk is another operational risk.

Fraud can exist in any part of the payment transaction and thus creates a risk exposure for the merchant processor.

Fraud at the authentication level is often referred to as identity theft.

Fraud at the authorization level may be caused by cyber attacks or complicity with a merchant or merchant employee.

Compliance Risk

Compliance risk may occur in various parts of offering and providing the merchant processing activity.

While the risk may occur at the payment facilitator level, when products, services, or systems associated with the processing are not properly reviewed for compliance, or when the operations are not consistent with law, ethical standards, or the card scheme's policies and procedures.

The potential for serious, frequent violations or noncompliance is heightened when the payment facilitator oversight program does not include appropriate audit and control features, particularly when the organization is implementing new activities or expanding existing ones.

Compliance risk also increases when the privacy of consumer and customer records is not adequately protected, when conflicts of interest between the organization and third parties are not appropriately managed, and when the payment facilitator or its service providers have not implemented an appropriate information security program.

The payment facilitator should involve his compliance management function in the due diligence and monitoring process.

5. Risk Management and Controls

Management Supervision

The management must ensure the organization has a comprehensive risk management framework in place commensurate with the payment facilitator complexity and risk profile.

The framework should enable the organization to assess, measure, monitor and control the various individual risks associated with the payment facilitator's merchant processing activities or risks within lines of business or by function.

The importance and need for a comprehensive and integrated approach to risk management has increased in an environment that has become more complex in last years.

The payment facilitator's risk management process should include written procedures appropriate to the size and complexity of operations.

Risk management must include a system for approving merchants and an ongoing program to monitor their credit quality and guard against merchant fraud or sanctioned activity.

The management must establish a sound internal control environment and audit culture.

In addition, the CEO is ultimately responsible for ensuring that the organization maintains an effective internal control structure that includes suspicious activity monitoring and reporting.

Management and staff should have knowledge and skills appropriate for the type and level of the risk the payment facilitator takes.

Staffing levels should be commensurate with the workload.

Risk measurement technology systems must be in place to operate, monitor, and control the activity effectively.

The management should regularly receive reports that enable them to gauge the department's risk. Key management reports should detail new account acquisitions, portfolio composition, sales volumes, charge-back volumes, fraud, suspicious activity reporting and department profitability.

PCI Security Standards

The PCI Security Standards are technical and operational requirements the council sets to protect cardholder data.

The standards are global and govern all merchants and organizations that store, process, or transmit payment data, and include specific requirements for software developers and manufacturers of applications and devices used in the transaction process.

Compliance with the standards is enforced by the major payment card brands that established the council.

PCI Data Security Standard for Processors and Merchants

The PCI Data Security Standard (PCI DSS) for processors and merchants is the global data security standard that a payment facilitator or payment service provider or merchant must adhere to in order to accept payment cards. The standard includes the following six goals and twelve requirements:

- Build and maintain a secure network.
    - Requirement #1: Install and maintain a firewall configuration to protect cardholder data.
    - Requirement #2: Do not use vendor-supplied defaults for system passwords and other security parameters.
- Protect cardholder data.
    - Requirement #3: Protect stored data.
    - Requirement #4: Encrypt transmission of cardholder data across open, public networks.
- Maintain a vulnerability management program.
    - Requirement #5: Use and regularly update antivirus software or programs.
    - Requirement #6: Develop and maintain secure systems and applications.
- Implement strong access control measures.
    - Requirement #7: Restrict access to cardholder data by business need-to-know.
    - Requirement #8: Assign a unique ID to each person with computer access.
    - Requirement #9: Restrict physical access to cardholder data.
- Regularly monitor and test networks.
    - Requirement #10: Track and monitor all access to network resources and cardholder data.
    - Requirement #11: Regularly test security systems and processes.
- Maintain an information security policy.
    - Requirement #12: Maintain a policy that addresses information security for all personnel.

PCI DSS attempts to establish essential practices for securing cardholder data.

If security control requirements are not properly implemented, data breaches may occur. Significant deviations from PCI DSS may result in security breaches.

PCI DSS compliance is not, however, a guarantee that breaches will not occur.

Merchant Underwriting and Review

Management should implement a formal merchant underwriting and approval policy to control credit risk.

The policy should designate the types of merchants with which the organization is willing to conduct business.

Further, the organization policy should define what information each application should contain, such as type of business, location and identification number for the business entity or principal owners.

The policy should also stipulate what information is required in the merchant agreement.

The merchant agreement should disclose all fees, define what the merchant is required to do and ask notification of ownership changes or substantive marketing and product changes.

The policy also should outline the procedures for the periodic reviews of the existing merchant base.

Underwriting Standards

The underwriting policy should require a background check of the merchant to support the validity of the business, creditworthiness of the merchant, and sales history.

The organization's underwriting standards should require, at a minimum:

- Signed application.
- Signed processing agreement.
- Signed corporate resolution, if applicable.
- Adequate understanding of the merchant's business to ensure that it is classified under the merchant category code.
- Processing history if available.
- Bank references.
- Licenses, if applicable.

Review and Approval of Merchants

In the initial review of a merchant application, the organization should reject a merchant with a history of substantial charge-back volumes, weak financial condition, or failure to operate a valid business.

The organization should establish who can approve new accounts.

To approve a merchant with a high sales volume, a senior officer's authorization should be required.

The policy should address documentation requirements.

Prohibited or Restricted Merchants

When evaluating merchants' credit quality, the organization must consider the business lines and any products the merchants offer.

The bank card association's segment businesses by activity, and payment facilitators should analyze merchants along similar lines on an ongoing basis.

Most payment facilitators compile lists of prohibited or restricted merchants, describing the types of merchants they are unwilling to sign or are willing to sign only under certain circumstances.

Certain types of businesses are inherently risky than others, for example: mail order and telemarketing merchants (often called MO/TO or MOTO), or if the merchant sells goods or services for future/delayed delivery, such as airline tickets, furnitures or memberships.

Many payment facilitators use holdback or reserve accounts to mitigate credit risk on higher-risk merchants.

Card Present (CP) Verus Card Not Present (CNP)

Merchants that swipe credit cards and examine each card at a point of sale location generally present far less risk than those who accept telephone or internet card payments where the card is not presented by the cardholder in person.

Merchant exposure varies significantly depending on whether or not the transaction is CP or CNP.

Merchants under CP category are basically lower risk than merchants under CNP category which are at higher risk of chargebacks and fraud as the cardholder will not see the quality of the products at the time of the payment and the merchant cannot check the signature of the cardholder against the card and make a judgment as to the card's legitimacy when they take a payment.

Internet Merchants

The Internet gives fraudulent businesses and businesses with minimal financial resources ready access to the public.

Payment facilitators should conduct thorough underwriting reviews of internet merchants using bank and trade verifications.

During the underwriting process, credit analysts should determine whether heightened fraud and charge-back risks warrant the use of additional risk mitigation techniques, such as delaying settlement or establishing reserves.

Electronic commerce and the use of the Internet pose privacy and security concerns that should be addressed in the initial underwriting.

The payment facilitator should ensure the security of transactions as well as stored data.

Secured servers and data encryption technologies help to protect data and transaction integrity.

For Internet merchants, underwriting standards should stipulate that at least the following information must appear on the Web site:

- Customer service number.
- If the web site or merchant uses an alias, the actual name of the entity that operates or controls the merchant.
- E-mail address to contact the company.
- Statement on security controls.
- Delivery methods and timing.

- Refund and return policies.
- Privacy statements.

Pricing Structure Versus Product Type

Does the merchant sell a product that has appropriate value to the price being charged?

Certain type of business offer products and services that are more prone to costumer dissatisfaction or buyer's complain.

This can result in excessive chargebacks or credits then if the business goes bankrupt or closes the payment facilitator may be liable for the payment of the returned charges and any resultant fines by the credit card schemes.

Average Transaction Amount (Ticket) & Monthly Volume

Large ticket amounts present higher risk exposure because they represent a concentration of risk.

One or two sales that are charged back may be very costly. Small tickets amounts are less likely to be contested by consumers and any chargeback that does come through represents less financial impact to the merchant. If the ticket is high, consumers are more likely to initiate a dispute when they are dissatisfied and the merchant may not be able to absorb the financial impact of the chargebacks leaving the liability to the payment facilitator.

Order Fulfillment

Merchants that sell products or services that are fulfilled and delivered immediately or within a few days from the sale represent less risk than merchants providing the service over a course of many weeks or months as travel, tourism and furniture verticals.

If the merchant does not ultimately fulfill orders already paid, he may not be able to absorb the financial impact of the chargebacks leaving the liability to the payment facilitator.

Recurring Transactions

Merchant's business model utilizing recurring transactions such as memberships, subscriptions, pre-payments etc. are subject to increased chargeback periods. The payment facilitator has to ensure that the business model is clear to the consumer and that the merchants maintain a liberal refund policy and an easy membership cancelation even if the consumer calls 30 days after the transaction has been done.

Seasonal Merchants

Seasonal merchants create additional risk to the payment facilitator as their processing volume is sporadic.

At the end of their busy season they will have fewer or zero transactions and this means there may be insufficient funds to cover any refund or chargeback at there times.

Seasonal merchants are also more prone to insolvency that others are.

Charities

Charities are sometimes a cover for fraud and money laundering. Payment facilitators have to require during the onboarding process specific charity registration certificates and documentation.

Merchant Credit-Worthiness

Depending on the type of merchant and the volume processed the Payment Facilitator should examine the financial viability of the merchant through credit bureau enquiries and examination of financial statements and other documentation.

Whether possible and available the latest financial accounts should be required from the merchant.

For existing and established companies, it's possible to obtain the above information from public records.

The payment facilitator must be confident that the merchant can financially support the amount of credit card volume and the potential risks that may be associated with its business.

Periodic Review

The financial condition of high-volume and high-risk merchants should be regularly monitored. The payment facilitator's policy should stipulate the frequency of reviews and the size of merchants requiring reviews.

In determining the threshold for periodic reviews, the payment facilitator should consider volume, concentrations, high-risk industries, and charge-back history.

Depending on the composition of the organization's portfolio, it may not be necessary for the payment facilitator to review smaller merchants periodically; the payment facilitator may be able to rely on sound underwriting guidelines at acquisition.

Whether or not a merchant's credit is reviewed periodically, its transactions—and those of every merchant—should be monitored rigorously for such events as fraud, charge-backs, suspicious activity, and sanctioned activity.

To screen portfolios periodically for troubled accounts, many payment facilitators now use information databases (e.g., databases of risk scores, bankruptcy filings, and fraud data).

By implementing effective and appropriate controls over its clients, a payment facilitator should be able to identify those merchants that process fraudulent transactions and to ensure that it's not facilitating these transactions.

In the event that a payment facilitator identifies fraudulent or other improper activity with a specific merchant, it should take immediate steps to address the problem including terminating the relationship with the merchant and requiring the acquirer bank to cease processing for that specific merchant.

Member Alert to Control High-Risk Merchants

MATCH is an identification system that logs merchants and principals (the owners of the merchant business) terminated for specific reasons.

When acquiring banks and transaction processors terminate contracts with merchants for certain risk-related reasons, the merchant businesses and their owners should be placed on MATCH.

The listing on MATCH indicates that the merchant committed one or more specific acts that convinced the acquiring bank or processor that the acceptable level of risk had been exceeded.

The specific reasons or types of acts that would warrant the merchant being placed on

MATCH include:

- Excessive charge-backs due to merchant business practices or procedures.
- Excessive deposits for transactions unauthorized by cardholders.
- Credit or debit card fraud conviction.
- Excessive deposits for counterfeit transactions.
- Deposits for transactions involving sales of goods or services generated by another merchant (laundering or factoring).
- Suspicion that the merchant is conducting fraudulent activity.

It is not uncommon for merchants to be placed on the list for technical violations of their merchant agreements, which would not be considered risk-related reasons, or possibly for several charge-backs that did not cause the processor a loss, or that may not have exceeded an acceptable level of risk.

Fraud Monitoring

Fraud analysts should not rely exclusively on excess charge-back activity to identify fraud.

The primary tool for detecting merchant fraud is an exception report that details variances from parameters established at account setup.

Basic parameters may include daily sales volume, average ticket size, multiple purchases of the same dollar amount, multiple use of the same cardholder number, and charge-back activity.

A daily exception report lists the merchants that breach these parameters.

Most large-volume processors and payment facilitators have exception parameters by industry or merchant type.

To maximize the efficiency of staff and monitoring reports, the organization should periodically review and update parameters as necessary.

Internet merchants may require a higher level of monitoring because of heightened fraud and charge-back risks associated with this sales channel.

Charge-Back Monitoring

A payment facilitator must have strong controls in place to accurately process charge-backs and retrieval requests in a timely manner.

The payment facilitator may lose a charge-back dispute (and lose the money involved) if it does not adhere to strict bank card association rules.

The bank card associations notify acquirers which notifies payment facilitators of merchants having excessive charge-backs, which may be based on volume, amount, or both.

The associations may fine banks that have high levels of charge-backs or that do not handle charge-backs properly.

Management can limit the chargeback compliance risk by establishing a structured charge-back processing system to monitor and handle merchant charge-backs.

A payment facilitator's risk management practices should detect merchants having high levels of charge-backs.

Numerous charge-backs may indicate an unscrupulous merchant, or the merchant's need for additional training.

Employees that monitor charge-backs should be alert for merchants with excessive retrieval requests or charge-backs.

Risk Mitigation

To protect themselves from merchants that pose high risk or that have a history of chargebacks, many payment facilitators establish merchant reserve accounts or holdback reserves.

Holdback reserves are also used to limit a payment facilitator's credit risk when the merchant's product or service involves future/delayed delivery.

A payment facilitator can fund the reserve by setting aside a lump sum or by withholding a portion of each day's proceeds until a specific balance has been reached.

Settlement Controls

Payment facilitators must understand and assess the risk regarding payments and settlement controls from merchant processing activities.

An assessment of payments and settlement controls should help management to understand the risks to the organization; to establish policies, procedures, and controls appropriate to these risks.

Agreements

A written contract should clearly set out the responsibilities of each party, compensation and liability arrangements, allowable uses of the payment facilitator ‘s name, and reasons the contract can be terminated.

Pricing

In general, merchant pricing is extremely competitive, especially for large and national-scale merchants that generate high transaction volumes.

The payment facilitator may use various methods to price the merchant account.

Smaller merchants are frequently priced with a single discount rate, rather than a range of discount rates, based on merchant volume and average sales ticket.

Payment facilitators frequently use unbundled pricing for their medium-size and large merchants.

When pricing is unbundled, a fee is charged separately for each service.

Fees as discount rate, transaction fee, authorizations and charge-backs may be unbundled.

Banks also may unbundle fees for application, customer service, membership, maintenance, and penalty fees (for violation of association rules or for fraud loss recovery due to a data compromise).

The pricing method chosen for a specific merchant should take into account the level of risk the merchant poses.

Pricing for higher-risk merchants may be set higher than for lower-risk merchants.

Many payment facilitators use pricing models to determine their target discount rates.

Payment facilitators may also maintain several pricing models.

The model used depends on criteria in the organization’s pricing policy, such as the merchant’s sales volume or type of business.

Pricing models allow payment facilitators to input different variables for different sales volumes, average sales tickets, revenue, or expenses, and such adjustments are designed to produce desired profit margins.

The pricing model should include all direct and indirect expenses.

The accuracy of any pricing model depends on reasonable assumptions for revenue and expenses.

6. Netpay Procedures

1. Organization and Staffing

Refer to Appendix 3- Chart Organization.

The normal hours of staffing of the risk department are Sunday to Thursday 9 AM - 6 PM, Friday from 9 am to 5 PM.

During weekends and holidays there is a staffing rotation vigilance in case of emergency; the risk department staff, the IT staff and the managers have remote access to the system.

Every user enters the system with his own password and all the logs and changes done in the system are registered.

High level managers are available 24/7.

In case of risk detection, the risk officer will receive alerts notifications to his email and proceed as follow:

- Level risk 1- pass thresholds 1 – alert to the risk officer. Risk officer call.
- Level risk 2- pass thresholds 2 – the transaction is blocked by the system. Risk officer call.
- Level risk 3- pass thresholds 3 – the merchant is blocked by the system and the call is escalated to a higher level manager following the escalation procedures.

2. Escalations

The company considers “serious fraud problems” as: Fraud Attacks, Account Generation, ADC or Disaster.

In case of serious fraud problems, the risk department block the merchant account/s and its or their reopening will be defined and eventually authorized following the below escalation tier categories of the merchant account:

- Credit Tier 1 merchant: monthly sales from 0 USD to 50K USD- Risk Officer.
- Credit tier 2: monthly sales from 50K USD to 500K USD- Head of Risk.
- Credit tier 3: monthly sales from 500K USD to 1M - CFO/CEO.

The merchant will not be re-opened unless a retain decision will be taken by the due manager and logged in the system.

The escalation procedures are reviewed once a year of per case.

3. Anti-Money Laundering

Refer to appendix 4- Anti-Money Laundering Policy and Procedure.

4. MATCH (Member Alert to Control High-Risk Merchants)

All our acquirers are connected to the MATCH system and complete MATCH checks on our mutual merchants.

The organization does not enter into a new business relationship or agreement with merchants listed on MATCH.

Refer to Appendix 8: Emails confirmation from acquirers.

5. MRP (MasterCard Registration Program)

MasterCard requires costumers (acquirers including sub-merchants and other entities) to register the following merchant types using the MRP system, available via MasterCard Connect:

- Non-face-to-face adult content and services merchants- MCCs 5967 and 7841;
- Non-face-to-face gambling merchants- MCCs 7995, 7801 and 7802;
- Non-face-to-face pharmaceutical merchants- MCCs 5122 and 5912;
- Non-face-to-face tobacco product merchants- MCC 5993;
- State lottery merchants (US region only) MCC 7800;
- Skill games merchants (US region only)- MCC 7994.

The organization sponsors high risk merchants within the card schemes organization rules and regulations.

The organization's acquirers register all our high risk sub-merchants to the MRP.

Refer to Appendix 8: Email confirmations from acquirers.

6. Merchant Application Processing

Submission of Applications

Accepted merchants: only e-commerce merchants from low, medium and high risk levels.

Accepted verticals: retail, services, forex, binary options, gambling, lottery, adult, dating, charity.

Required documents and compliance checks:

- Merchant Application Form- Refer to Appendix 6- Merchant Application Form.
- Company registration confirmation or equivalent document.

- Certificate of incorporation.
- Share certificate.
- Official documents showing owners and directors.
- Memorandum of associations.
- Utility bills of owners and directors.
- Passports copies of owners and directors.
- First minute meeting document: official letter stating who is the authorized signatory for the company.
- Bank statement and financial statements.
- Processing history.
- If there is a Mother / Daughter/ Nominee company involved, all of the above documentations as well.
- What is the service policy, time/days the service given (appear on the web site).
- PCI yes/no.
- Data security policy.
- If it's a consisting merchant, what is the track record related to CHB and fraud reporting.
- SLA (service-level agreement)

For Gambling/Lottery /Forex/Binary Options/ Charities Merchants:

- Evidence of legal authority, license that authorize the merchant to engage in the specific activity.
- Legal opinion if required by the acquirer.

URL checks:

- About us.
- Contact us/costumer service policy.
- Costumer phone number and email.
- Company name and registration address.
- Term & Condition.
- Delivery methods and timeframes.
- Refunds and return policy.
- Privacy policy.
- URL registration.
- Payment page flow and compliance with SSL.

Adult website extra checks:

- Compliance with 2257 and disclaimer.

- Check if there are any illegal contents, brand damaging sale of images and or non-consensual adult and child pornography which are illegal.

Gambling website extra checks:

- Notice on website before the account information is requested stating that assertions have been made that gambling is lawful in some jurisdictions including the United States and suggesting the cardholder check whether Internet gambling is lawful under applicable law.
- Check the merchant does not sell chips or other value that can be used to gamble.
- Check the merchant is not crediting winnings to credit card account holders.
- When opening the merchant in the system CVC2 field requirement is mandatory.

Signed Merchant Service Agreement

Refer to Appendix 9: Business case- Boursotrade Ltd.

Prohibited and Restricted Verticals

Gaming, gambling in jurisdictions where its illegal, Pharmaceutical, Tobacco, Cyberlocker (file sharing, hosting services, virtual storage, remote backup), sales of counterfeits goods, sales of goods or services in violation of intellectual property rights, illegal sales of any products or services, travel and seasonal goods and services.

Approval Criteria

The compliance department is responsible for ensuring the merchant applications are submitted correctly. The approval on each new merchant application will be given upon the below credit tier criteria:

- Credit Tier 1: monthly sales from 0 USD to 50K USD - approved by compliance officer.
- Credit tier 2: monthly sales from 50K USD to 500K USD- approved by senior officer or head of risk.
- Credit tier 3: monthly sales from 500K USD to 1M - approved by CFO.
- Credit tier 4: monthly sales more than 1M- approved by CEO.

The organization shall use as a part of its KYC, financial and bona-fide checks on new merchants, reports by DBI and D&B.

Application Acceptance

Upon approval is given the compliance officer opens a new merchant account in the system filling in the related details.

Each detail is checked upon the company data base to find details in common.

- If no matches are found: he will open the new merchant in “integration status”.
  - ✓ The integration has to be approved by the tech department.
  - ✓ The signed merchant agreement has to be submitted and approved by the compliance officer.
  - ✓ The risk officer sets up the MID and merchant risk profile.
  - ✓ The risk officer changes the status of the merchant from “integration” to “processing”.

- If matches are found: the compliance officer will check the matching details and investigate the reasons of the duplicate application.
  - ✓ If the merchant has been blacklisted due to risk and fraud reasons, the application will be denied and registered in the merchant blacklist database.
  - ✓ If the merchant has been blacklisted due to underwriting incompliance the application may be approved upon the above described compliance and approval criteria.

Approved applications are stored both in soft and hard secured files.

Application Rejection

When an application is rejected the compliance officer will notify the merchant by email with the reason of the rejection.

If the nature of the rejection is not risk or fraud, the merchant shall resubmit his application which will be reconsidered if further required documentation and explications are applicable by the compliance officer.

Rejected application are stored both in the system under “merchant black list” category and in hard files.

Merchant Screening

The organization shall use as a part of its KYC, financial and bona-fide checks on new merchants, reports and scoring by DBI and D&B.

The organization checks the validity of the merchant address by visiting its facilities if it’s a local merchant and if it’s an international merchant by validating phone numbers, domain registrations, company address vs. company registration address, DBI and B&D if needed, terms and conditions of making transaction, and SLA.

Applications are stored in both secured soft and hard files.

The organization’s compliance and risk department execute monthly periodic reviews on all the merchant urls to:

- Determinate if after the onboarding they continue to be in compliance with the organization standards and requirements.

- Determine if any change has been detected in the merchant activity business model.
- Make sure the correct MCC code is utilized.

If a minor change is detected the compliance or risk officer will immediately issue a notification to the merchant, ask for an explanation and correction action.

If a major change is detected like illegal content or MCC misuse the merchant will be immediately closed.

The organization used in the past the services of G2 to monitor the merchant's urls for illegal, brand damaging content and aggregation detection and it's now renegotiating a new agreement.

7.Term and Conditions

The organization requires a signed "Merchant Service Agreement" as mandatory document to be supplied as a part of the onboarding procedure of a new merchant.

The Merchant Service Agreement is reviewed on a yearly basis or when risk issues rises.

The risk department contribution in establishing or changing terms and conditions of the agreement is high.

Refer to Appendix 10: Merchant Service Agreement.

Merchant Termination

A merchant may be terminated immediately by the organization based on the following circumstances:

- If a risk threshold is reached.
- If a serious fraud problem has been detected.
- If there are damaging changes in the merchant's credit records.
- It the merchant goes bankrupt.
- If the merchant is in any violation of the card schemes.
- If a merchant is in breach with any of the terms of the merchant agreement.
- It the acquire or card association requires so.
- If the merchant is found to have been dishonest or inaccurate in the information supplied.
- If the merchant changes its business model without prior written notice and approval.
- If any other event or series of events whether related or not occurs which in our opinion may affect the ability of the merchant to comply with all his obligations and liabilities under the card schemes rules and laws.

The organization will give the merchant up to 30 days written notice as per the risk department decision.

The termination letter contains the legal name of the merchant, the date of the termination, the reason of the termination, the signature of an authorized signatory.

Refer to Appendix 11- Termination Letter.

The immediate decision to terminate a merchant is taken by risk. The final decision will involve the CEO.

The organization will then notify the acquirer; hold up to 180 days' rolling reserves and settle payments according to the agreement and on a case by case review done in collaboration between the risk department, CFO and CEO.

8.Sales Force

The organization has internal sales managers and accept leads from third-party vendors.

Every single lead arrives to the organization's sales department and is managed internally by the organization.

If the organization receives several times bad performances leads from third-party vendors the business relationship with the vendor will be stopped.

The organization has NDA/ third-party vendor's agreement in place with all of his sub-contractors.

Refer to Appendix 16: Facilitator Agreement.

9.Merchant Education and Support

The compliance and risk department shall provide to the merchant operational highlights related to their day by day business activity.

Refer to Appendix 12: Managing Merchant & Operational Procedures.

10.Merchant Compliance Programs

GMAP (Global Merchant Audit Program)

The GMAP uses a rolling of six month of data to identify MasterCard merchants that, in any calendar month, meets the criteria set forth in the following table:

Fraud Criteria for Global Merchant Audit Tier Classification

The MasterCard location is classified in the following GMAP tier	**If in any calendar month, the MasterCard merchant location meets the following fraud criteria**
Tier 1- Informational Fraud Alert	• 3 fraudulent transactions • at least 3K USD in fraudulent transactions • a fraud to sales USD volume ratio minimum of 3% and not exceeding 4.99%
Tier 2- Suggested Training Fraud Alert	• 4 fraudulent transactions • at least 4K USD in fraudulent transactions • a fraud to sales USD volume ratio minimum of 5% and not exceeding 7.99%
Tier 3- High Fraud Alert	• 5 fraudulent transactions • at least 5K USD in fraudulent transactions • a fraud to sales USD volume ratio minimum of 8%

The payment facilitator responsibilities are to evaluate the fraud control measures and merchant training procedures in place for the merchant.

When GMAP identifies a merchant location in tier 3, MasterCard will determinate whether to initiate an audit on the merchant.

The actions taken by the organization if there is a breach of this program are:

- Tier 1- The merchant will be flagged by the risk department for a closer monitoring, notified accordingly, asked to take care and called to explain the situation.

- Tier 2- The merchant will be notified, educated and trained accordingly by the risk department to ensure that he is familiar with the requirements of MC.
  The merchant will also be questioned on the risk system he uses and asked to increase the level of intercepting possibly fraud.
- Tier 3- Enforcement actions will be applied, like hold the activity or even stop the relationship with the organization.

The organization will take corrective actions through merchant education as communication, assistance in analyzing the results of the risk engine or damage control enforcing only type of transactions, minimizing the ticket amount and limiting the monthly volume.

The organization receives on a daily and weekly basis from its acquires SAFE and TC40 reports.

The risk department synchronizes the data to the system and calculates the fraud values. If needed takes action accordingly.

The merchants identified with the above fraud tiers continues to be monitored as long as they are active in the system's organization.

Refer to Appendix 12: Fraud Thresholds Master Card and Visa Breach Notification

ECP (Excessive Chargeback Program)

MasterCard designed the ECP to encourage each acquirer to closely monitor, on an ongoing basis, its chargebacks performance at the merchant level and to determine promptly when a MasterCard merchant has exceeded or is likely to exceed monthly chargebacks thresholds.

Definitions:

- **CTR (Chargeback to Transaction Ratio):** is the number of MasterCard chargebacks received by the acquirer for a merchant in a calendar month divided by the number of the merchant MasterCard sales transactions in the preceding month acquired by the acquirer. A CTR of 1% equals to 100 basis points and a CTR of 1.5% equals 150 basis point.

- **CMM (Chargeback-Monitored Merchant):** is a merchant that has a CTR in excess of 1% and at least 100 chargebacks in a calendar month.

- **ECM (Excessive Chargeback Merchant):** is a merchant that in each of two consecutive calendar months (the trigger months) has a minimum of CTR 1.5% and at least 100 chargebacks in each month. This designation is maintained until the ECM's CTR is below 1.5% for two consecutive months.

The payment facilitator responsibilities are to monitor on an ongoing basis each of its merchants in accordance with the standards and thresholds and to calculate for each calendar month the CTR for each of its merchants and report to the acquirer/MasterCard any merchant that is a CMM or ECM as defined above.

The actions taken by the organization if there is a breach of this programs are:

- CMM- The merchant will be inquired, notified and trained accordingly by the risk department. The organization will limit the monthly volume to achieve better results of the risk engine.

- ECM- The merchant will be terminated at the time he reaches the CHB card organizations thresholds then a program will be built together with the merchant as not to be above the CMM.

The organization will take corrective actions through communication, education, analyzing the results of the risk engine as to make them more powerful, damage control and enforcement.

The organization produces specific batch reports and online alerts that monitors merchants identified with a breach in the CHB internal thresholds.

The merchants identified with such breach will be either terminated or stay monitored as long as they are active in the system's organization.

Refer to Appendix 12: Chargebacks Thresholds-VISA/MC Breach Notification.

11.Fraud Loss Control Program

In order to identify, measure, monitor and control the fraud levels the organization uses is own system based on a table of parameter's thresholds set for each activated merchant to monitor his transactions and overall processing activity.

For each parameter's threshold reached, the system will issue an alert directed to the risk officer in charge to take care it accordingly.

11.1 Authorization Monitoring

The parameters used are:

- ✓ Number of authorizations per hour.
- ✓ Number of authorization per day.
- ✓ Number of authorization per week.
- ✓ Number of authorization per month.

The risk officer receives real time alert any time a threshold is reached.

The alert contains the following information: rule detection, threshold detection, threshold type, threshold value, the parameter value vs. the threshold value and the action taken.

The risk officer will run an investigation to analyze the nature of the breach and the reason behind the occurrence of the alert; then take action accordingly to the procedures.

11.2 Fraud Monitoring

The parameters used are:

- ✓ Deposit volumes per rolling 24 hours.
- ✓ Deposit volumes per rolling 7 days.
- ✓ Deposit volumes per rolling 30 days.

- ✓ Average ticket size.
- ✓ Number of transactions per rolling 24 hours.
- ✓ Number of transactions per rolling 7 days.
- ✓ Number of transactions per rolling 30 days.
- ✓ Credit amounts on the same period of time.
- ✓ Credit counts on the same period of time.
- ✓ Maximum credit amount per single refund.

The risk officer receives real time alert any time a threshold is reached.

The alert contains the following information: rule detection, threshold detection, threshold type, threshold value, the parameter value vs. the threshold value and the action taken.

The risk officer will run an investigation to analyze the nature of the breach and the reason behind the occurrence of the alert; then take action accordingly to the procedures.

*** credit/refunds-will be processed only after** the risk officer checks that there isn't any breach of the parameters and there is balance in the merchant account; if there is not enough balance the refund won't be executed.

11.3 Fraud Detection

The parameters used are:

- ✓ Multiple tickets in the same dollar amount.
- ✓ Multiple uses of same cardholder number (velocity check).
- ✓ Credits amounts.
- ✓ Credits counts.
- ✓ Reinsertions from same IP for different cards within short period of time.
- ✓ Transactions from inactive accounts.
- ✓ Number of declined transactions (rate=decline /decline + approved (count) per day.
- ✓ Number of declined transactions (rate=decline /decline + approved (count) per week.
- ✓ Number of declined transactions (rate=decline /decline + approved (count) per month.
- ✓ Fraud counts.
- ✓ Fraud amounts.

The risk officer receives real time alert any time a threshold is reached.

The alert contains the following information: rule detection, threshold detection, threshold type, threshold value, the parameter value vs. the threshold value and the action taken.

The risk officer will run an investigation to analyze the nature of the breach and the reason behind the occurrence of the alert; then take action accordingly to the procedures.

11.4 Fraud Detection Administration

For risk and fraud data monitoring the organization's system generate both online alerts and batch alerts/reports.

The parameters are established by the head of risk.

The parameters for exceptions and parameters changes are authorized (logged by passcode and user name), by the Head of Risk/CFO/CEO accordingly to the escalation procedures and logged in the system.

The parameters changes may be done in real time.

The parameters effectiveness are reviewed once a quarter by running a log of all the alerts and rules that have been issued and analyzed.

If there are zero or few alerts it means that it is not effective. If there are too many alerts it means that it is not effective as well and the system is overcharged, however there will be another filter of checks when actual fraud will be compared to the fraud system and defined if it can be intercepted by the system as well.

11.5 New Merchant Monitoring

The risk department manages parameters for the monitoring of new merchants differently and firmer than for old-time merchants.

A new merchant activity is evaluated following his processing history if available. Parameters are established as per the merchant business model, risk related, industry and MCC.

A new merchant is considered new during the first 3-4 months of processing within the organization.

When an unusual activity is identified at a new merchant the risk department practices the same procedures as set for all the organization's merchants: communication, analysis, education, damage control and enforcement if needed.

11.6 Seasonal Merchant Monitoring

The organization will not accept and sign any seasonal merchants, this is a restricted vertical, thus up to know a seasonal merchant monitoring is N/A.

11.7 Inactive Merchant Monitoring

A merchant is considered inactive when during the last 21 days (3 weeks) no transactions have been processed in its account.

When an inactive merchant is detected the account is blocked and an alert is sent to the risk officer who will further investigate the reasons of the alert and eventually reactivate the account manually by following the procedures. The reactivation is logged in the system.

11.8 Fraud Investigation

When the risk officer receives an alert from the system he runs an investigation to analyze the nature of the breach and the reason behind the occurrence of the alert. Then he takes action accordingly to the procedures as for example implementing more control on such merchant and/or even blocking the merchant from any further activities with the company.

The risk officer will document an investigation summery with the following details in a dedicated folder:

- ✓ The details of the investigator.
- ✓ The time of receiving the alert.
- ✓ The reason for the alert and the investigation.
- ✓ The action being taken.

11.9 Chargebacks

The parameters used are:

- ✓ Chargeback amounts for MasterCard.
- ✓ Chargeback counts for MasterCard.
- ✓ Chargeback amounts for Visa.
- ✓ Chargeback amounts for Visa.

The risk department is in charge to monitor chargeback's levels on a daily basis and following the below card schemes thresholds:

VISA-Chargeback Thresholds:

2% and 200 count chargebacks within the same calendar month.

The ratio is calculated vs. the Visa transactions count of the same month.

MASTERCARD- Chargeback Thresholds:

1% and 100 count chargebacks within the same calendar month.

The ratio is calculated vs. the MC transactions count of the previous full calendar month.

11.10 Fraud- TC40 and SAFE

The parameters used are:

- ✓ Fraud amounts for MasterCard.
- ✓ Fraud counts for MasterCard.
- ✓ Fraud amounts for Visa.
- ✓ Fraud amounts for Visa.
- ✓ The internal parameters will be lower that the international brands and/or the acquirer parameters.

The organization receives on a daily or weekly basis (depending on the acquirer) the TC40 and SAFE reports relevant to its merchants.

The risk department is in charge to update the information in the system and monitor fraud levels following the card schemes thresholds.

MasterCard Fraud Criteria Tier Classification:

The MasterCard location is classified in the following tier	If in any calendar month, the MasterCard merchant location meets the following fraud criteria
Tier 1- Informational Fraud Alert	3 fraudulent transactions at least 3K USD in fraudulent transactions a fraud to sales USD volume ratio minimum of 3% and not exceeding 4.99%
Tier 2- Suggested Training Fraud Alert	4 fraudulent transactions at least 4K USD in fraudulent transactions a fraud to sales USD volume ratio minimum of 5% and not exceeding 7.99%
Tier 3- High Fraud Alert	5 fraudulent transactions at least 5K USD in fraudulent transactions a fraud to sales USD volume ratio minimum of 8%

Visa Fraud Criteria

Actually is as follow:

- 2% and 200 count fraud transactions within the same calendar month.
- The ratio is calculated vs. the Visa transactions count of the same month.

But it will be changed on July 2016

11.11 Merchant Settlement

Funds are settled to the merchants bank accounts of their choice once a week from the moment the organization receives the funds from the acquirer, through bank wire transfers.

As the organization keeps rolling reserve up to 180 days from the date of the transaction, in case of merchant account termination, or detection of high fraud activity the organization may use the reserve if there will be a need according to the merchant service agreement.

11.12 Pricing

The organization sets his pricing method as a percentage (%) of the processing volume with a scaling model and additional services fee, as per the below example:

Discount Rate	**Processing Volume**
6.00% -5.25%	$ 0-150 K
5.25% - 4.95%	$ 151-500 K
4.95% - 4.75%	$ 501k-1M
4.75% - 4.50%	$ 1M and above

A flat rate may be provided when the processing volumes are higher.

Services Fee:

Transaction Fee	$ 0.55-0.66
Chargeback Fee	$ 55-70
Refund Fee	$ 5

The organization holds a rolling reserve of minimum 10% of the processing volume for 6 months.

The discount rate shall mean a percentage of gross settled sales volume.

Transaction fee shall mean a fee charged on each sale and each credit transaction and each declined transaction.

The CFO and CEO are permitted to change/fix a price for merchant account out of the pricing guidelines.

Refer to Appendix 10: Merchant Service Agreement, Exhibit A

11.13 Reserves

Reserves are funds collected by the organizations from each merchant account to ensure the covering of possible loss encountered during the processing activity.

The organization holds a rolling reserve for each merchant account based on a percentage deducted from daily processing settlements and normally released after 6 full months of processing.

After the 180 days the money used as rolling reserve is being paid back to the merchant.

The organization may also require a security deposit where a determination is made that a gradual accrual of reserves does not protect adequately the potential risk of losses.

12.Account Data Compromise Standards and Programs

In case an Account Data Compromise event happens our system react as follows in terms of PCI:

• Internet connections originating from non–business-related IP addresses1; inbound Internet connections originating from countries without a business relationship to the potentially compromised entity; outbound Internet connections to non–business-related IP addresses; countries, or both:
System - CC issued countries can be blocked. IP can be blocked.
Network (Incapsula) – block & alert countries and IP's.

• Log-in activity from unknown or inactive user IDs, or excessive or unusual login activity from user IDs:
PCI policy, block after 3 failed tries / block after 3 months of no activity / force complex password / keep history of login tries.

• Presence (in network systems or environments) of malware, suspicious files, or executables and programs, or presence of unusual activity or volume in same:
Using FIM to monitor unnecessary file changes (Netwrix) / ESET File security / Microsoft OM for change Auditing.

• SQL injection or other suspicious activity on Web-facing systems:
System - Secured coding procedures, we filter tries in our code.
Network (Incapsula) – Traffic go thru Incapsula and comes to us filtered (WAF/DDoS /SQL Injection/Cross Site Scripting).

• POS terminals and ATM devices showing signs of tampering: N/A

• Key-logger found: N/A.

• Card-skimming devices found: N/A.

• Lost, stolen, or misplaced sales receipt: N/A.

• Lost, stolen, or misplaced payment card data:
ADC procedure, stop service/s, report to top managers check logs, find security hole and fix, run restore if necessary, fill a writing report.

• Lost, stolen, or misplaced computers, laptops, hard drives, or other devices that contain MasterCard payment card data: We don't keep payment data outside production database.

• Files containing MasterCard account data mistakenly transmitted to an unauthorized party and suspicious e-mail or File Transfer Protocol (FTP) activity occurring on network systems:
ADC procedure, stop service/s, report to top managers check logs, find security hole and fix, run restore if necessary, fill a writing report.

13.Site Data Protection and PCI Compliance

Netpay ltd is a PCI DSS Level 1 certified service provider.

Refer to Appendix 14: PCI Certificate.

The organization's staff is mandatory required to follow the site data protection PCI's procedures.

Educational sessions from qualified entities are provided annually to maintain up-to-date on site awareness.

Refer to Appendix 13: PCI Password Procedure; PCI Incident Response Procedure.

14.Disaster Recovery

The ensure business continuity the organizations keeps at least 2 of each server types (web/data/dc etc.) for redundancy.

The company databases run under SQL Server Always-On setup.

Backup of database as well as server's images are done on a regularly basis.

During the disaster event there is no involvement of the risk department, but from the moment the system is back the risk department will check the fraud monitoring and detection system is working correctly.

15.Senior Management Level Reporting

The head of risk provides a monthly summery report to the organization's management at the beginning of each month,

The 3rd degree alerts are reported immediately base on the escalation procedures to the CEO/CFO.

The data reported will include:

- The name of the rule.
- The alert level.

- The number of alerts.
- The merchant's name with all types of alerts and numbers.
- A list of all type's of merchant's alerts.

7. Examination Procedures

These examination procedures apply to Netpay Ltd. ("The Organization").

Overall objective: To assess the quantity and direction of risks in the organization's merchant processing activity; understand management's risk tolerance levels; gain an understanding of products offered or planned; assess policies, procedures, and practices used in merchant processing; and assess compliance with regulations and regulatory guidance.

Management Planning

Objective: To assess the adequacy of the strategic plan, business plan, and the overall planning process, including management's methodology for setting merchant processing growth and profitability targets, and the processes to ensure appropriate expertise and sufficient staffing within the line of business.

- Review the organization's strategic plan and determine whether management's plans for the departments are clear and represent the current direction of the departments.
- Obtain information about the overall portfolio. Significant changes from the prior examination should be reviewed to understand how the changes have affected the portfolio's risk profile.
- Evaluate any new programs the organization is pursuing and what effect the programs may have on the merchant operation.
- Determine the risk profile of the portfolio. Evaluate the methods the organization uses to rate the risk in its merchant accounts, as well as the frequency and timing of adjusting the ratings of its merchant accounts.
- Review the résumés of the principals in the merchant processing department. Determine whether the staff has adequate experience in merchant processing and if is adequately trained.
- Review the organizational chart for the department to determine whether the organizational structure is appropriate.
- Determine whether current staffing levels fit the organization's short-term and long-term requirements. Determine whether:
  - ✓ Staffing levels are adequate for the volume of merchant accounts, the number of applications reviewed daily, processing needs, and the need to oversee third parties;
  - ✓ Personnel reviewing merchant applications are qualified;
  - ✓ Staffing levels are sufficient to handle resolution of costumer service and support;
  - ✓ Staffing levels are sufficient to investigate daily fraud exception reports in a timely manner;
  - ✓ Staff turnover is reasonable;

- Evaluate the overall adequacy of written policies for merchant processing by considering whether the policy:
  - ✓ Establishes clear lines of authority and responsibility;
  - ✓ Identifies the risks the organization is willing to accept, as well as limits on the amount of those risks in relation to capital, earnings, or sales volumes, as appropriate;
  - ✓ Limits the individual and aggregate volume of the organization's merchant activity;
  - ✓ Provides for adequate and knowledgeable staff;
  - ✓ Requires written contracts between all third parties;
  - ✓ Establishes criteria for the acceptance of merchants;
  - ✓ Requires the development of procedures to monitor each merchant's activity;
  - ✓ Establishes when merchant reserve accounts are appropriate;
  - ✓ Establishes risk-based guidelines for the periodic review of merchant creditworthiness;
  - ✓ Establishes guidelines for handling exceptions to policy;
  - ✓ Requires review of all contracts and applications by legal counsel familiar with merchant processing.
- Determine whether the CEO evaluates policies for changing market and business conditions at least annually and whether the policies are in line with the overall strategic plan for this activity.
- Determine whether the organization policy addresses the approval process for new merchant accounts. In that regard, and from an underwriting perspective, determine whether the policy addresses the following issues and points:
  - ✓ Types of merchants for which the organization does not want to provide merchant processing services (prohibited and restricted lists);
  - ✓ Documentation requirements for merchant files;
  - ✓ Location of original contracts for merchants and requirement to be maintained in a secure, fire-protected area;
  - ✓ Merchant contracts have the appropriate party signatures;
  - ✓ Underwriting guidelines for merchant accounts;
  - ✓ Termination procedures for merchant accounts;
  - ✓ Type of derogatory information that is acceptable on credit reports;
  - ✓ Criteria for approving processing for additional merchant locations;
  - ✓ Personnel in the organization who are responsible for approving merchants;
  - ✓ Handling of exceptions to the merchant approval policy.

Settlement and Charge-Backs

Objective: To evaluate the effectiveness of the settlement and charge-back function, including strategies and programs employed.

- Determine types and adequacy of information on merchant charge-backs and on the organization's monitoring for fraud.

- Determine whether the organization maintains any merchant holdback reserves to mitigate risk.
- Determine whether the organization has incurred any significant charge-back or fraud losses in the past year.
- Review the settlement flow chart. Identify all parties involved, each party's responsibilities, and the estimated time that it takes funds and transaction data to flow from party to party during the settlement process.

Risk Management and Control Systems

Objective: To assess adequacy of the organization's processes for identifying, measuring, monitoring, and controlling risk by reviewing the effectiveness of risk management and other control functions.

- Determine the internal/external auditor's knowledge of the merchant processing department and whether the auditor's knowledge is adequate to perform effective reviews.
- Determine whether management has established parameters for monitoring Internet transactions.
- Determine how the organization establishes parameters for exceptions.
- Determine who in the organization can set fraud parameters and what documentation is required to change the parameters.
- Determine the organization's course of action when it detects suspicious activity.
- Review monitoring parameters for exceptions that are available to the organization. Commonly used parameters are:
  - ✓ Large average ticket size.
  - ✓ Large daily or weekly volume.
  - ✓ Multiple tickets in the same dollar amount.
  - ✓ Multiple uses of same cardholder number.
  - ✓ High charge-back activity.
  - ✓ Excessive return volumes.
  - ✓ Declined authorizations.
  - ✓ Authorizations not matched to sales and vice versa.
  - ✓ Transactions from inactive or closed accounts.
- Set periodic review of the parameters that have been set.
- Consider performing verification procedures if the reports contain unusual information or information that cannot be readily explained.

Third-Party Vendor Management

Objective: To determine the extent of all third-party arrangements in merchant processing and evaluate the effectiveness of management's oversight and risk management processes.

- Determine what third-party vendors the organization uses for merchant processing services and the activities or services the third party performs.
- Obtain a report that shows merchant sales volume for each third-party vendor. Review vendors that have significant volume or growth.
- Determine whether contracts are on file for each third-party vendor.
- Review major contracts to assess the following information:
  - ✓ Terms specifying financial compensation, payment arrangements, and price changes.
  - ✓ Specific work to be performed by the third-party servicer.
  - ✓ Requirements for the confidential treatment of records.
  - ✓ Whether contractual penalties for terminating the contract seem reasonable.

Profitability - Pricing

Objective: To assess the quantity, quality and sustainability of earnings from merchant processing activities.

- For organizations that retain loss liability and if the organization sets pricing variables, determine what pricing variable method is used (e.g., matrix, formula, or pricing model).
- Consider whether:
  - ✓ Pricing system takes into account all of the organization's costs.
  - ✓ Pricing on the organization's largest merchant accounts (e.g., top 10) is profitable.

Determine who has the authority to price a merchant account outside the pricing guidelines.

8. Industry Glossary

Acquiring bank (acquirer): a bank that contracts with merchants for the settlement of payment card transactions is an acquiring bank. Acquiring banks contract directly with merchants, or indirectly through agent banks or other third-party organizations, to process card transactions. The acquiring bank generally provides all backroom operations to the agent bank and owns the bank identification number (BIN)/Interbank Card Association (ICA) number through which settlement takes place.

Authorization: an issuing bank's approval of a card transaction in a specific amount. If a merchant complies with bank card association rules in obtaining an authorization, by telephone or electronic terminal, payment to the merchant is guaranteed.

Automated clearing house (ACH): ACH is an electronic network for financial transactions in the United States, which processes large volumes of credit and debit transactions in batches.

Bank card association: a bank card association is an organization, owned by financial institutions, that licenses a bank card program. Visa USA and MasterCard International are bank card associations. Banks must be members of an association to offer the association's card services. Membership rights and obligations are specifically defined by the associations. Both Visa and MasterCard require all members of their organization to be banks.

Bank identification number/Interbank Card Association (BIN/ICA) number: a series of unique numbers used to identify the settling bank for both acquiring and issuing transactions.

Chargeback: a chargeback is generated when a cardholder disputes a transaction or when the merchant does not follow proper procedures. The issuer and acquirer research the facts to determine which party is responsible for the transaction. Strict card association rules must be followed.

Clearing: clearing is the process of delivering final transaction data from acquirers to issuers for posting to the cardholder's account. Clearing also includes the calculation of certain fees and charges that apply to the issuer and acquirer involved in the transaction, as well as the conversion of transaction amounts to the appropriate settlement currencies.

Cyber attack: an intentional maneuver to exploit, steal, alter, degrade, destroy, or disrupt computer information systems, networks, software, or infrastructure, or the information that the system processes, stores, or transmits.

Debit card: a card that customers use to pay for a merchant's goods and services. A debit card also enables a user to transact business at an automated teller machine (ATM). In a debit card transaction, the cardholder is accessing funds from a personal checking or savings account.

Discount rate: the fee, as a percent of sales volume, an acquirer or PSP or PF charges a merchant for processing sales transactions.

E-commerce: the term used for electronic commerce, which refers to buying and selling products or services using the Internet.

Electronic data capture: process used when the merchant "swipes" the card through an electronic card reader or terminal. The information on the card's magnetic stripe is entered into the processor's database electronically.

EMV: EMV is a technology that embeds a microprocessor chip on credit cards and debit cards to encrypt transaction data. The technology was jointly developed by Europay, MasterCard, and Visa, and the technology is named for the original developers. EMV technology is widely used in other countries, but not in the United States.

Factoring (credit card factoring): factoring is used as a method to launder money via credit cards. Factoring, also referred to as credit card factoring, is essentially processing transactions through a merchant account for a business or entity other than the specific business that was screened and set up for the merchant account. Factoring is a form of fraud in which a merchant creates false sales transactions, inflates the sales amount, or alters the sales drafts to receive funds from the issuer. The merchant's intentions could be to obtain additional money to cover charge-backs or cash flow problems, or the merchant may have ceased operations and plans to abscond with the sales proceeds. If the merchant ceases to operate or disappears, the acquirer would be responsible for any remaining charge-backs.

Future or delayed delivery: sales transactions on products or services that are delivered in the future. Examples of such products or services include airline tickets, concert tickets, travel/tour packages and furniture.

High-risk merchant account: a high-risk merchant account poses increased risk to banks through fraud, high charge-back rates, or poor credit history. Examples of merchant account categories that may be deemed high-risk include: businesses where the products incur a high likelihood of consumer fraud; businesses with historically high refund and charge-back rates; businesses that have an elevated risk of bankruptcy; and businesses that sell products or services against the local laws.

Holdback: a percentage of the merchant's sales deposits that the acquirer holds back to serve as a reserve against future exposure or to cover existing charge-backs.

Independent sales organization (ISO): an organization that provides merchant processing functions on behalf of the acquirer. These functions may include soliciting new merchant accounts, arranging for terminal purchases or leases, and providing backroom services. An ISO and an MSP are functionally similar. The acquirer must register all ISOs/MSPs with the bank card associations. Also, see the definition of MSP.

Interchange: the electronic infrastructure that processes financial and nonfinancial transactions between financial institutions.

Interchange fee: a fee paid by one bank to another to cover handling costs and credit risk in a bank card transaction. The interchange fee, a percentage of the transaction amount, is derived from a formula that takes into account authorization costs, fraud and credit losses, and the average bank cost of funds.

Laundering: a form of fraud in which a merchant that holds an account with an acquirer submits drafts for a merchant that does not. This is sometimes called draft laundering. The authorized merchant typically receives a percentage of the unauthorized merchant's sales volume. Several states' criminal statutes prohibit laundering.

Member Alert to Control High Risk Merchants (MATCH): the MATCH file is maintained by the bank card associations based on information reported by acquirers. By checking this file before approving a merchant, an acquirer determines whether the merchant has a history of poor operating practices.

Member service provider (MSP): A nonmember of MasterCard who markets bank card merchant acceptance on behalf of MasterCard financial institutions. An MSP is functionally similar to an ISO. Also, see the definition of ISO.

Bank account: A bank account opened by a merchant through a bank or other financial institution that is a member of a major card network.

Merchant account: a merchant account is an account that provides merchant's processing.

Merchant processing: the settlement of credit card or debit card payment transactions by banks for merchants. Merchant processing activity, which is off-balance-sheet, involves gathering sales information from the merchant, collecting funds from the issuing bank, and paying the merchant. Various types of third parties may be involved.

Mobile processing: the use of mobile devices for credit and debit card transactions by merchants.

Payment card: a card that can be used by a cardholder and accepted by a merchant to make a payment for a purchase or in payment of some obligation.

Payment facilitator (PF): a payment facilitator is a merchant that is registered by an acquirer to facilitate transactions on behalf of sub-merchants. The acquirer is responsible for the actions of the payment facilitator and the sub-merchants. A payment facilitator is operationally similar to a payment service provider.

Payment service provider (PSP): the payment service provider is an organization that contracts with an acquirer to provide payment services to sponsored merchants. The acquirer is responsible for the actions of the PSP and the PSP's sponsored merchants. A payment service provider is operationally similar to a payment facilitator.

Prepaid debit card: a type of debit card where the value of the card is preloaded on the card from the funds paid in advance by the consumer. The consumer does not incur debt from the use of the prepaid debit card when the consumer makes a purchase for goods or services.

Retrieval request: a form used to request a copy of the original sales draft from the merchant. A merchant that fails to send a copy of the sales draft may receive a charge-back. Such charge-backs are not appealable. An issuer may request a copy of the sales draft to verify the signature, to investigate the lack of an imprint, to carry out a cardholder's inquiry, or to look into the possibility of fraud.

Settlement: settlement is the process of transmitting sales information to the card-issuing bank for collection and reimbursement of funds to the merchant. Settlement also refers to the process of calculating, determining, and reporting the net financial position of issuers and acquirers for all transactions that are cleared. Various third-party organizations may be involved in all aspects of settlement.

Third-party organization: any outside company with which the acquirer contracts to provide merchant processing services. These services may include network and data transmissions, merchant accounting, backroom operations, sales, or customer services.

9. Appendixes

Appendix Number	Appendix Name
1.	Top MCC Volumes Report
2.	Transaction Flow
3.	Chart Organization
4.	AML Policy & Procedures
5.	MasterCard 2015 merchant total transaction volume USD
6.	Merchant Application Form & Merchant Application Form Approval
7.	Agreements With Acquirers
8.	Email Confirmations From Acquirers
9.	Business Case- Boursotrade Ltd.
10.	Merchant Service Agreement
11.	Termination Letter
12.	Educational Material-Operational Highlights Chargeback Thresholds-VISA/MC Breach Notification Fraud Thresholds-VISA/MC Breach Notification
13.	PCI Password Procedure PCI Incident Response Procedure
14.	PCI Certificate

15.	Facilitator Agreement

10. References

- The Office of the Comptroller of the Currency's (OCC) **Comptroller's Handbook.**
- **PCI web site**, https://www.pcisecuritystandards.org/.
- **Master Card Rules**, May 2015.
- Master Card Rules, **Security Rules and Procedures**, July 2015.
- Netpay Ltd. Operational Guidelines, September 2009.