



Attn. **Alon Elbaz & Jelena Jorov**
NetPay Ltd.
11 Hasadnaot street, Herzeliha, Israel

Dear Alon Elbaz, Dear Elena Jorov,

I would like to thank you and the NetPay Ltd team for your contribution and hospitality provided during the on-site Global Risk Management Program.

MasterCard would like to thank NetPay Ltd for the thorough preparation ahead of the GRMP Review which was clearly evidenced by the procedures and software presentations made to MasterCard during the Review which were both detailed and comprehensive.

This document contains MasterCard's key findings and recommendations based on the discussions during the course of the onsite review.

An 'action plan' is also attached which is required to be completed by NetPay Ltd and returned to MasterCard within next 1 month and detailing the various NetPay Ltd actions taken against the 'requirements and recommendations'.

Please do not hesitate to contact me at any time should you have any questions.

Yours Sincerely,

A handwritten signature in blue ink, appearing to read "Bochenek".

Bogdan Bochenek
CEE Customer Fraud Management
MasterCard Europe SA Branch in Poland
53 Emilii Plater str. 00-113 Warsaw, Poland

Cc: Andras Hemberger – CEE cluster area manager
Ofer Golan – ICC-CAL

Encl. 1) Action Plan document

GLOBAL RISK MANAGEMENT PROGRAM

NetPay Ltd

ADVANCING COMMERCE

Monday 16th May 2016



TABLE OF CONTENTS

1.0	Executive Summary	3
1.1.	Assumptions and Liabilities	3
1.2.	Introduction	3
1.3.	Compliance with the MasterCard Standards and Recommended Actions.....	4
1.4.	Conclusion	4
2.0	Requirements.....	5
2.1.	Payment Facilitator Program	5
2.2.	PCI Compliance	6
2.3.	Fraud Loss Control Program & Minimum Monitoring Requirements	7
2.4.	Sub-Merchant Monitoring.....	10
2.5.	Sub-merchant Screening Procedures.....	10
2.6.	MATCH Inquiry.....	12
2.7.	Payment Facilitator Obligations.....	17
2.8.	Sub Merchant Compliance with Standards	21
2.9.	Business Risk Assessment and Mitigation (BRAM)	24
2.10.	MasterCard Registration Program	29
2.11.	Excessive Chargeback Program (ECP).....	33
2.12.	Global Merchant Audit Program (GMAP)	35
2.13.	Questionable Merchant Audit Program (QMAP).....	36
2.14.	Account Data Compromise Event Management.....	37
3.0	Recommendations / Supplementary Information.....	40
3.1	MasterCard Compliance.....	40
3.2	MasterCard Anti-Money Laundering (AML Requirements)	41
3.3	MasterCard Connect for Service Providers	42



- 3.4 MasterCard Key Operational Documents 44
- 3.5 MasterCard Best Practice for Service Providers..... 45
- 3.6 MasterCard Training for Service Providers 46
- 3.7 Merchant Education..... 47
- 3.8 Fraud Reporting..... 49
- 3.9 MasterCard Fraud Management Solutions 51
- 3.10 SecureCode Strategy..... 53
- 3.11 Mitigating Fraudulent Authorization Reversals..... 55
- 3.12 Chargeback Management Best Practices..... 57

1.0 Executive Summary

1.1. Assumptions and Liabilities

This report and its enclosed recommendations are based on information provided by NetPay Ltd during the course of the Global Risk Management Program (GRMP) Review. MasterCard accept no responsibility for any errors or omissions in any information provided to us. This report is confidential and must not be provided to any third party without prior written consent from MasterCard.

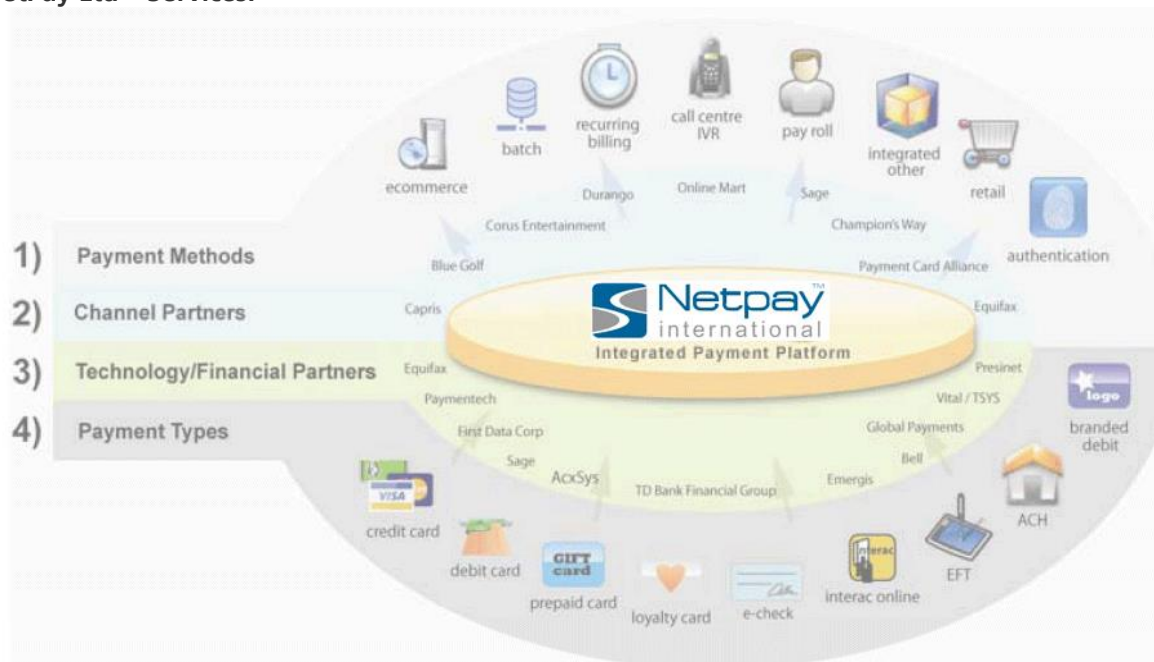
1.2. Introduction

The Global Risk Management Program review is a tool for assessing a Payment Facilitator's current capability to anticipate, manage and protect against inherent internal and external risk in the acquiring portfolio. The review also determines the effectiveness of existing fraud control measures, adherence to MasterCard rules and regulations and (where appropriate) provides industry best practice guidelines.

MasterCard Worldwide is committed to working closely with its customers and third parties to fully understand their business dynamics and rationale, while ensuring that customers and third parties conduct their business in a risk adverse manner without creating an undue disadvantage for other parties. Working with Customer, we aim to identify avenues of opportunity to better enable Customer to manage its fraud and compliance in a cost effective manner.

Under the framework of the Global Risk Management Program (GRMP), MasterCard by partnering with third party customers is ensuring that they uphold their compliance requirements, implement and maintain proper fraud risk control standards to protect the brand and integrity of the MasterCard network.

NetPay Ltd – Services:



1.3. Compliance with the MasterCard Standards and Recommended Actions

During the course of the review, compliance with the Payment Facilitator Requirements were assessed and the findings have been detailed in the following sections of the report.

- Section 2.0 Requirements and Findings
- Section 3.0 Recommendations

These Requirements and Recommendations will help to ensure ongoing compliance with the MasterCard Rules and enhance existing risk management policy and procedures which, will ensure that NetPay Ltd is in a favorable position to expand its business while maintaining fraud risk exposure at an acceptable level to the business.

It is recommended that NetPay Ltd continue to work with MasterCard to review and implement both the Requirements and Recommendations to ensure ongoing compliance with MasterCard Standards.

1.4. Conclusion

During the review, NetPay Ltd clearly demonstrated their ability to comprehensively assess and mitigate acceptance risk.

It was evident during the GRMP Review that NetPay Ltd is fully committed to meeting MasterCard's Rules and Compliance Standards by the proactive and market leading activities they conduct.

To enhance the current acquiring risk and compliance framework recommendations have been made to drive accountability and value chain partner visibility.

Key Requirements & Recommendations:

- Payment Facilitator program
- PCI Compliance
- Fraud Loss Control Program & Minimum Monitoring Requirements
- Sub-Merchant Monitoring
- Sub-merchant Screening Procedures
- MATCH Inquiry
- Payment Facilitator Obligations
- Sub Merchant Compliance with Standards
- Business Risk Assessment and Mitigation (BRAM)
- MasterCard Registration Program
- Excessive Chargeback Program (ECP)
- Global Merchant Audit Program (GMAP)
- Questionable Merchant Audit Program (QMAP)
- Account Data Compromise Event Management



2.0 Requirements

2.1. Payment Facilitator Program

Summary

MasterCard announced revised Standards for the Payment Facilitator and Service Provider programs within the **Global Operations Bulletin No 10, 1st October 2014**.

Background

The payments landscape is changing with the emergence of new technologies and new participants in the global payment space. To help ensure the continued success of MasterCard and its customers, MasterCard rules and policies must evolve to align with market needs and continue to protect the MasterCard franchise.

The Payment Facilitator and Service Provider programs were created to help grow MasterCard merchant acceptance. The Payment Facilitator model is a cost effective way for small merchants in an e-commerce, face-to-face and mobile point-of-sale environment to accept MasterCard.

Summary of Rules Changes

The following rules changes are effective immediately, as outlined in the revised Standards.

- A Payment Facilitator will be classified as a type of Service Provider, rather than as a Merchant (but will continue to be able to perform all of its existing services, such as paying sub merchants for transactions).
- The sub merchant transaction volume threshold will be raised from USD 100,000 to USD 1,000,000 in combined MasterCard® and Maestro® annual transactions. Entities with higher volumes must enter into a direct merchant agreement with the acquirer
- The acquiring of transactions from a Payment Facilitator located outside of the area of use of the customer's license will be permitted, provided the transactions occur at sub merchants located within the customer's area of use.
- The performance of a credit check when screening a prospective merchant or sub merchant will no longer be required if the entity has annual combined MasterCard and Maestro transaction volume (actual or projected) of USD 100,000 or less.

In addition, the following changes are effective 17 April 2015 (with Release 15.Q2):

Acquirers must populate new transaction data fields to uniquely identify the Payment Facilitator and the sub merchant (refer to the article "Global 545—Service Provider and Merchant Identification Enhancements," in the Release 15.Q2 Document—Dual and Single Message Systems.

Acquirers are no longer be required to provide quarterly reporting of Payment Facilitator activity and monthly reporting of high-risk Payment Facilitator activity.

The acquirer must provide to MasterCard a quarterly Non-Processed Transaction Activity report for each Sub merchant of the Payment Facilitator that includes the following:

- Sub merchant name and location as appears in DE 43 (Card Acceptor Name/Location) of clearing records
- Sub merchant "doing business as" name or URL
- Sub merchant MCCs
- Transaction sales count and amount for each MCC
- Transaction chargeback count and amount for each MCC

- The card acceptor name field (DE 43, subfield 1) of authorization and Clearing messages must always display the Payment Facilitator name followed by "*" and the sub merchant name.
- Acquirers must populate a new Independent Sales Organization (ISO) identification number in all transactions for which an ISO provides merchant or ATM owner support.

Customers can find complete details about this enhancement in the article *Global 545—Service Provider and Merchant Identification Enhancements*, in the *Release 15.Q2 Document—Dual and Single Message Systems*.

Additional MasterCard Bulletins:

1. MasterCard announced clarifications for the Revised Standards for the Payment Facilitator and Service Provider programs within the **Global Operations Bulletin No 12, 1st December 2014**.
 - Merchant Screening – Credit Checks
 - ISO / PF Identifier Requirements
2. MasterCard announced clarifications and reminders for the Revised Standards for the Payment Facilitator and Service Provider programs within the **Global Operations Bulletin No 8, 3rd August 2015**.
 - Clarification of the definition of Non-Processed Transaction Activity
3. MasterCard announced the Global Risk Management Program Incentive for Payment Facilitators and their Sponsoring Acquirers within the **Global Security Bulletin No 11, 16th November 2015**.
4. MasterCard announced the Price Reduction for Global Risk Management Program – Third Party Risk Reviews within the Global Pricing Bulletin No 2, 22 February 2016 **Global Security Bulletin No 11, 16th November 2015**.

2.2. PCI Compliance

The MasterCard Compliant Service Provider List

➔ <https://www.mastercard.us/en-us/merchants/safety-security/security-recommendations/site-data-protection-PCI.html#>

A company's name appears on this Compliant Service Provider List if

- (i) MasterCard has received a copy of an Attestation of Compliance (AOC) by a Qualified Security Assessor (QSA) reflecting validation of the company being PCI DSS compliant and
- (ii) MasterCard records reflect the company is registered as a Service Provider by one or more MasterCard Customers.

The date of the AOC and the name of the QSA are also provided. Each AOC is valid for one year. MasterCard receives copies of AOCs from various sources.

This Compliant Service Provider List is provided solely for the convenience of MasterCard Customers and any Customer that relies upon or otherwise uses this Compliant Service Provider list does so at the Customer's sole risk. While MasterCard endeavors to keep the list current as of the date set forth in the footer, MasterCard disclaims any and all warranties of any kind, including any warranty of accuracy or completeness or fitness for any particular purpose. MasterCard disclaims any and all liability of any nature relating to or arising in connection with the use of or reliance on the Compliant Service Provider List or any part thereof. Each MasterCard Customer is obligated to comply with MasterCard Rules and other Standards pertaining to use of a Service Provider.

During the review it was determined, that NetPay Ltd has actual and valid PCI-Compliance certification in the form of Attestation of Compliance [AOC] certificate, issued to NetPay Ltd by Qualified Security Assessor's company of Comsec Consulting Ltd, dated December 19th, 2015. Provided AOC certification is valid until December 18th, 2016 which means that by this date, NetPay Ltd is required to provide new annual AOC certificate.

Requirements

Section 10.3 of the MasterCard's Security Rules and Procedures states in part:

10.3 MasterCard Site Data Protection (SDP) Program

The MasterCard Site Data Protection (SDP) Program is designed to encourage Customers, Merchants, Third Party Processors (TPPs), and Data Storage Entities (DSEs) to protect against account data compromises. SDP facilitates the identification and correction of vulnerabilities in security processes, procedures, and Web site configurations. For the purposes of the SDP Program, TPPs and DSEs are collectively referred to as "Service Providers" in this chapter.

Acquirers must implement the MasterCard SDP Program by ensuring that their Merchants and Service Providers are compliant with the Payment Card Industry Data Security Standard (PCI DSS) and that all applicable third party-provided payment applications used by their Merchants and Service Providers are compliant with the Payment Card Industry Payment Application Data Security Standard (PCI PA-DSS), in accordance with the implementation schedule defined in section 10.3.1 of this manual. Going forward, the Payment Card Industry Data Security Standard and the Payment Card Industry Payment Application Data Security Standard will be components of SDP; these documents set forth security Standards that MasterCard hopes will be adopted as industry standards across the payment brands.

A Customer that complies with the SDP Program Requirements may qualify for a reduction, partial or total, of certain costs or assessments if the Customer, a Merchant, or a Service Provider is the source of an account data compromise.

MasterCard has sole discretion to interpret and enforce the SDP Program Standards

A Payment Facilitator is compliant with the PCI Data Security Standard in accordance with the MasterCard Site Data Protection (SDP) Program implementation schedule applicable to Merchants, as set forth in section 10.3.4, "Implementation Schedule," of the *Security Rules and Procedures* manual.

2.3. Fraud Loss Control Program & Minimum Monitoring Requirements

Finding

During the review, it was determined that NetPay Ltd under their current Acquiring Partnership with ICC CAL is contracted to undertake 'transaction monitoring' on behalf of Acquirer but NetPay Ltd does undertake monitoring activities to mitigate potential financial risk to both NetPay Ltd and their sub-merchants and comply with the MasterCard Standards as they apply to Payment Facilitators.

ICC CAL in accordance with the MasterCard Loss Control Standards as applicable to Acquirers undertakes monitoring of the Sub-merchants transactional activity for suspected activity or processing illegal or brand-damaging Transactions.

During the review, it was determined that NetPay Ltd utilizes MaxMind (3rd Party vendor delivered) Risk & Fraud Detection System which provides 'transactional monitoring' across their Sub-merchant portfolio

and where NetPay Ltd carries the liability for any financial loss resulting from Financial Risk, Fraud, Chargeback and Compliance Risk.

NetPay Ltd within their completed 'GRMP Questionnaire' confirmed that they had implemented almost all of the minimum MasterCard Loss Control Standards applicable to merchant acquiring (recommended 150% Rule is not) and demonstrated during the review that their internal monitoring meets the MasterCard Loss Control Standards.

NetPay Ltd demonstrated during the review a clear understanding as to the need to monitor 'merchant and transactional' activity to identify potential risk both from a credit, fraud, chargeback and compliance perspective in order to protect both NetPay Ltd, MasterCard and their Acquiring partners from both financial and reputational risk.

Requirements

Each Payment Facilitator must monitor on an ongoing basis the Activity and use of the Marks of each of its Sub-merchants for the purpose of deterring fraudulent and other wrongful activity and to ensure ongoing compliance with the Standards. For purposes of this Rule, the minimum Merchant monitoring Standards set forth in the Security Rules and Procedures manual apply with respect to Sub-merchants.

6.2.2 Acquirer Fraud Loss Control Programs

An Acquirer's fraud loss control program must meet the following minimum Requirements, and preferably will include the recommended additional parameters. The program must automatically generate daily fraud monitoring reports or real-time alerts. Acquirer staff trained to identify potential fraud must analyze the data in these reports within 24 hours.

To comply with the fraud loss control Standards, Acquirers also must transmit complete and unaltered data in all Card-read authorization request messages, and also CVC 2 for all CNP and voice-authorized Transactions. Additionally – for Card Present environments, Acquirers with high fraud levels must:

- Install "read and display" terminals in areas determined to be at high risk for fraud or counterfeit activity, or
- Install Hybrid POS Terminals

6.2.2.1 Acquirer Authorization Monitoring Requirements

Daily reports or real-time alerts monitoring Merchant authorization requests must be generated at the latest on the day following the authorization request, and must be based on the following parameters:

- Number of authorization requests above a threshold set by the Acquirer for that Merchant
- Ratio of non-Card-read to Card-read Transactions that is above the threshold set by the Acquirer for that Merchant
- PAN key entry ratio that is above the threshold set by the Acquirer for that Merchant
- Repeated authorization requests for the same amount or the same Cardholder account
- Increased number of authorization requests
- "Out of pattern" fallback Transaction volume

6.2.2.2 Acquirer Merchant Deposit Monitoring Requirements

Daily reports or real-time alerts monitoring Merchant deposits must be generated at the latest on the day following the deposit, and must be based on the following parameters:

- Increases in Merchant deposit volume
- Increase in a Merchant's average ticket size and number of Transactions per deposit
- Change in frequency of deposits
- Frequency of Transactions on the same Cardholder account, including credit Transactions
- Unusual number of credits, or credit dollar volume, exceeding a level of sales dollar volume appropriate to the Merchant category
- Large credit Transaction amounts, significantly greater than the average ticket size for the Merchant's sales
- Credits issued subsequent to the receipt of a chargeback with the same account number and followed by a second presentment
- Credits issued to an account number not used previously at the Merchant location

90-day Rule

The Acquirer must compare daily deposits against the average Transaction count and amount for each Merchant over a period of at least 90 days, to lessen the effect of normal variances in a Merchant's business. For new Merchants, the Acquirer should compare the average Transaction count and amount for other Merchants within the same MCC assigned to the Merchant. In the event that suspicious credit or refund Transaction activity is identified, if appropriate, the Acquirer should consider the suspension of transactions pending further investigation.

150 Percent Recommendation

To optimize the effectiveness of fraud analysis staff, Merchants that appear in the monitoring reports should exceed the average by 150 percent or more. However, the amount over the average is at the Acquirer's discretion.

6.2.2.3 Recommended Additional Acquirer Monitoring

MasterCard recommends that Acquirers additionally monitor the following parameters:

- Fallback methods
- Credit Transactions (such as refunds) and Merchant authorization reversals
- Transactions conducted at high-risk Merchants
- PAN key-entry Transactions exceeding ratio
- Abnormal hours or seasons
- Inactive Merchants
- Transactions with no approval code
- Transactions that were declined

- Inconsistent authorization and clearing data elements for the same Transactions

Web Site Monitoring Recommendation

MasterCard recommends that Acquirers use a Web site monitoring solution to review their electronic commerce (e-commerce) Merchants' activity to avoid processing illegal or brand-damaging Transactions.

2.4. Sub-Merchant Monitoring

Finding

During the review, it was determined that NetPay Ltd monitors all MasterCard transaction activity processed via their Sub-merchants.

Refer to Section 2.2 Fraud Loss Control Program & Minimum Monitoring Requirements

Requirement

Each Payment Facilitator must monitor on an ongoing basis the Activity and use of the Marks of each of its Sub-merchants for the purpose of deterring fraudulent and other wrongful activity and to ensure ongoing compliance with the Standards. For purposes of this Rule, the minimum Merchant monitoring Standards set forth in the Security Rules and Procedures manual apply with respect to Sub-merchants.

These monitoring Requirements can be found in the **MasterCard Security Rules & Procedures (Chapter 6): 6.2.2 Acquirer Fraud Loss Control Program**

- 6.2.2.1 Acquirer Authorization Monitoring Requirements
- 6.2.2.2 Acquirer Merchant Deposit Monitoring Requirements
- 6.2.2.3 Recommended Additional Acquirer Monitoring

2.5. Sub-merchant Screening Procedures

Finding

During the review it was evidenced that NetPay Ltd has a comprehensive set of 'Merchant Boarding & Due Diligence' policies and procedures which were provided to MasterCard within the following NetPay Ltd policy documents.

- Payment Facilitator Operational Guidelines and Procedures

viewed during onsite review.

To ensure compliance with the MasterCard Standards a merchant boarding platform was reviewed for data availability parameterization and setting up requirements.

NetPay Ltd as part of their merchant screening procedures utilize additional services provided by the following sources to supplement reviews:

- Whols

- World-Check One
- Thomson Reuters – Under review for PEP's & Sanctions Checks
- Qualys SSL Labs

NetPay Ltd indicated that currently they do undertake 'Credit Check's as part of the Sub-merchant boarding procedures. Subsequent screening procedures take place only upon irregularities identification and then DBI and/or D&B databases are checked.

The Money Laundering Regulations 2007 (as Amended) require NetPay Ltd to undertake due diligence measures in respect of their Sub-merchants both at the point of recruitment and post recruitment and the procedures adopted by NetPay Ltd to meet these requirements are documented within the Risk Management Policy.

MasterCard would refer NetPay Ltd to the Payment Facilitator requirements.

Requirements.

Each Payment Facilitator, before signing a Sub merchant Agreement, must verify that the prospective Sub merchant is a bona fide business. Such verification must include at least both of the following:

- For each prospective Sub merchant with more than USD 100,000 in projected or actual annual combined MasterCard and Maestro Transaction volume, conduct a credit check (such as by obtaining a credit report from a credit bureau). If the credit check raises questions or does not provide sufficient information, the Payment Facilitator also should conduct a credit check of:
 - The owner, if the prospective Sub merchant is a sole proprietor; or
 - The partners, if the prospective Sub merchant is a partnership; or
 - The principal shareholders, if the prospective Sub merchant is a corporation.

A credit check must also be performed if required by the Acquirer or applicable law or regulation.

- Perform background investigations and reference checks of the prospective Sub merchant.
- Check for the validity of the business address and other information provided.
- Request that the Acquirer for which the Payment Facilitator is an agent submit an inquiry to the MasterCard Member Alert to Control High-risk (Merchants) (MATCH™) system if the prospective Sub merchant proposes to accept MasterCard Cards. (The Acquirer itself must directly perform the MATCH system inquiry.). The MATCH inquiry for a prospective Sub merchant proposing to conduct e-commerce Transactions must include the Universal Resource Locator (URL) address of the prospective Sub merchant's website.

NOTE: A Customer must participate in the MATCH system unless excused by MasterCard or prohibited by law.

As a best practice, the Payment Facilitator also should:

- Inspect the prospective Sub merchant's premises (both physical locations and Internet URLs, as applicable) and records to ensure that it has the proper facilities, equipment, inventory, agreements, and personnel required and if necessary, license or permit and other capabilities to conduct the business.
- Ensure that the prospective Sub merchant is able to support the provision of products or services to be marketed, and has procedures and resources to timely and appropriately respond to Cardholder inquiries and to support refund requests.
- Investigate the prospective Sub merchant's previous and other relationships with Customers or Payment Facilitators, if any.

2.6. MATCH Inquiry

Since 1 September 2000, it is a mandate for all MasterCard Acquirers to subscribe to the Member Alert to Control High-Risk Merchants (MATCH) service. The MATCH database contains the details of thousands of merchants that have been terminated by their acquirer for fraud, risk and non-compliance related reasons.

Finding

During the review, it was determined that NetPay Ltd forwards information to ICC CAL in respect of all Sub-merchants so that a MATCH inquiry can be performed prior boarding. However, the same process was not always followed subsequent to Sub-merchants termination.

With respect to the Sub-merchants within the NetPay Ltd portfolio the responsibility for conducting queries into MATCH and uploading terminated merchant data relating to the respective Sub-merchants sits with ICC CAL as the Acquirer.

Should the NetPay Ltd planning wider its scope of activities to include MATCH inquiries/reporting, the Acquirer(s) NetPay Ltd is working with must extend service provider registration scope accordingly, up to Third Party Processor Type-II level, as defined by MasterCard Rules manual in chapter 7.

Recommendation:

NetPay Ltd should ensure that any terminated merchants under their various contractual agreements are formally communicated to the respective Acquirer for uploading to MATCH.

NetPay Ltd should also seek the following confirmations from the respective Acquirer:

- A terminated merchant has been uploaded to MATCH
- An inquiry has been made of MATCH for all Sub-merchants submitted to the Acquirer by NetPay Ltd

Requirements:

Section 11 of the MasterCard Security and Procedures states in part:

11.1 MATCH Overview

MasterCard designed MATCH™, the Member Alert to Control High-risk (Merchants) system, to provide Acquirers with the opportunity to develop and review enhanced or incremental risk information before entering into a Merchant Agreement. MATCH is a mandatory system for Acquirers. The MATCH database includes information about certain Merchants (and their owners) that an Acquirer has terminated.

When an Acquirer considers signing a Merchant, MATCH can help the Acquirer assess whether the Merchant was terminated by another Acquirer due to circumstances that could affect the decision whether to acquire for this Merchant and, if a decision is made to acquire, whether to implement specific action or conditions with respect to acquiring.

WARNING!

MasterCard does not verify, otherwise confirm, or ask for confirmation of either the basis for or accuracy of any information that is reported to or listed in MATCH. It is possible that information has been wrongfully reported or inaccurately reported. It is also possible that facts and circumstances giving rise to a MATCH report may be subject to interpretation and dispute.

11.2 MATCH Standards

MasterCard mandates that all Acquirers with Merchant activity use MATCH.⁵

To use means both to:

- Add information about a Merchant that is terminated while or because a circumstance exists (See section 11.2.2), and
- Inquire against the MATCH database

Customers must act diligently, reasonably, and in good faith to comply with MATCH Standards.

11.2.1 Certification

Each Acquirer that conducts Merchant acquiring Activity must be certified by MasterCard to use MATCH because it is a mandatory system. An Acquirer that does not comply with these Requirements may be assessed for noncompliance, as described in this chapter.

Certification is the process by which MasterCard connects an Acquirer to the MATCH system, so that the Acquirer may send and receive MATCH records to and from MasterCard. To be certified for MATCH usage, Acquirers must request access for each Member ID/ICA number under which acquiring Activity is conducted.

NOTE: An Acquirer that conducts Merchant acquiring Activity under a Member ID/ICA number that does not have access to the MATCH system is not considered certified.

11.2.2 When to Add a Merchant to MATCH

If either the Acquirer or the Merchant acts to terminate the acquiring relationship (such as by giving notice of termination) and, at the time of that act, the Acquirer has reason to believe that a condition described in Table 11.4 exists, then the Acquirer must add the required information to MATCH within five calendar days of the earlier of either:

A decision by the Acquirer to terminate the acquiring relationship, regardless of the effective date of the termination, or

Receipt by the Acquirer of notice by or on behalf of the Merchant of a decision to terminate the acquiring relationship, regardless of the effective date of the termination.

Acquirers must act diligently, reasonably, and in good faith to comply with MATCH system Requirements.

Acquirers may not use or threaten to use MATCH as a collection tool for minor Merchant discretionary activity. One of the defined reason codes in Table 11.4 must be met or suspected (at decision to terminate) to justify a Merchant addition. Acquirers that use or threaten to use MATCH as a collection tool for minor Merchant discretionary activity are subject to noncompliance assessments as described in Table 11.3.

An Acquirer that fails to enter a Merchant into MATCH is subject to a noncompliance assessment, and may be subject to an unfavourable ruling in a compliance case filed by a subsequent Acquirer of that Merchant.

11.2.3 Inquiring about a Merchant

An Acquirer must check MATCH before signing an agreement with a Merchant in accordance with section 7.1 of this manual.

An Acquirer that enters into a Merchant Agreement without first submitting an inquiry to MATCH about the Merchant may be subject to an unfavourable ruling in a compliance case filed by a subsequent Acquirer of that Merchant.

Acquirers must conduct inquiries under the proper Member ID/ICA Number for reporting compliance reasons. If an Acquirer does not conduct the inquiry under the proper Member ID/ICA Number (that is, the Member ID/ICA Number that is actually processing for the Merchant), MasterCard may find the Acquirer in noncompliance and may impose an assessment.

Failure to comply with either the requirement of adding a terminated Merchant or inquiring about a Merchant may result in noncompliance assessments.

11.2.6 MATCH Record Retention

An Acquirer should retain all MATCH records returned by MasterCard to substantiate that the Acquirer complied with the required procedures. MasterCard recommends that the Acquirer retain these records in a manner that allows for easy retrieval.

Merchant records remain on the MATCH system for five years. Each month, MATCH automatically purges any Merchant information that has been in the database for five years.

NOTE: The MATCH system database stores inquiry records for 360 days.

11.3 Merchants Listed by MasterCard

A Merchant listing may prompt inquiry or additional inquiry by an Acquirer about the Merchant. If MATCH inquiry data matches data in the MATCH file, either by an exact or phonetic match, MasterCard will generate a response record. The Member ID/ICA

Number 1996 in a response record, together with one of the MATCH reason codes listed indicates that the inquiry record matches a MasterCard Listed Merchant.

NOTE: A value of 1996 in the MasterCard Reference Number field of a response record indicates that an inquiry possibly matched a questionable Merchant record.

Acquirers that receive a possible match response with Member ID/ICA Number 1996 in the MasterCard Reference Number field may contact the Merchant Fraud Control staff as described in the Security and Risk Services section of Appendix C.

11.3.1 Questionable Merchants

MATCH also contains data about Merchants and their owners classified as questionable by the Merchant Fraud Control staff. These Merchants and owners are listed as questionable Merchants because MasterCard is auditing the Merchant for compliance with rules.

The questionable Merchant listings may prompt inquiry or additional inquiry by an Acquirer about the Merchant. If MATCH inquiry data matches data in the MATCH file, either by an exact or phonetic match, MasterCard will generate a response record. The Member ID/ICA Number 1996 in a response record, together with a MATCH reason code 00, indicates that the inquiry record matches a questionable Merchant entry.

11.4 Merchant Removal from MATCH

MasterCard may remove a Merchant listing from MATCH for the following reasons:

1. The Acquirer reports to MasterCard that the Acquirer added the Merchant to MATCH in error.
2. The Merchant listing is for reason code 12 (Payment Card Industry Data Security Standard Noncompliance) and the Acquirer has confirmed that the Merchant has become compliant with the Payment Card Industry Data Security Standard. The Acquirer must submit the request to remove a MATCH reason code 12 Merchant listing from MATCH in writing on the Acquirer's letterhead to Merchant Fraud Control.

11.5 MATCH Reason Codes

MATCH reason codes identify whether a Merchant was added to the system by the Acquirer or by MasterCard, and the reason for the listing.

11.5.1 Reason Codes for Merchants Listed by the Acquirer

The following reason codes indicate why an Acquirer reported a terminated Merchant to MATCH

Description

- **01 Account Data Compromise**

An occurrence that results, directly or indirectly, in the unauthorized access to or disclosure of Account data.

- **02 Common Point of Purchase (CPP)**
Account data is stolen at the Merchant and then used for fraudulent purchases at other Merchant locations.
- **03 Laundering**
The Merchant was engaged in laundering activity. Laundering means that a Merchant presented to its Acquirer Transaction records that were not valid Transactions for sales of goods or services between that Merchant and a bona fide Cardholder.
- **04 Excessive Chargebacks**
With respect to a Merchant reported by a MasterCard Acquirer, the number of chargebacks in any single month exceeded 1% of the number of MasterCard sales Transactions in that month, and those chargebacks totaled USD 5,000 or more.

With respect to a merchant reported by an American Express acquirer (ICA numbers 102 through 125), the merchant exceeded the chargeback thresholds of American Express, as determined by American Express.

- **05 Excessive Fraud**
The Merchant effected fraudulent Transactions of any type (counterfeit or otherwise) meeting or exceeding the following minimum reporting Standard: the Merchant's fraud-to-sales dollar volume ratio was 8% or greater in a calendar month, and the Merchant effected 10 or more fraudulent Transactions totaling USD 5,000 or more in that calendar month.
- **06 Reserved for Future Use**
- **07 Fraud Conviction**
There was a criminal fraud conviction of a principal owner or partner of the Merchant.
- **08 MasterCard Questionable Merchant Audit Program**
The Merchant was determined to be a Questionable Merchant as per the criteria set forth in the MasterCard Questionable Merchant Audit Program
- **09 Bankruptcy/Liquidation/Insolvency**
The Merchant was unable or is likely to become unable to discharge its financial obligations.
- **10 Violation of Standards**
With respect to a Merchant reported by a MasterCard Acquirer, the Merchant was in violation of one or more Standards that describe procedures to be employed by the Merchant in Transactions in which Cards are used, including, by way of example and not limitation, the Standards for honoring all Cards, displaying the Marks, charges to Cardholders, minimum/maximum Transaction amount restrictions, and prohibited Transactions set forth in Chapter 5 of the MasterCard Rules manual.

With respect to a merchant reported by an American Express acquirer (ICA numbers 102 through 125), the merchant was in violation of one or more American Express bylaws, rules, operating regulations, and policies that set forth procedures to be employed by the merchant in transactions in which American Express cards are used.

- **11 Merchant Collusion**
The Merchant participated in fraudulent collusive activity.

- **12 PCI Data Security Standard Noncompliance**
The Merchant failed to comply with Payment Card Industry (PCI) Data Security Standard Requirements.
- **13 Illegal Transactions**
The Merchant was engaged in illegal Transactions.
- **14 Identity Theft**
The Acquirer has reason to believe that the identity of the listed Merchant or its principal owner(s) was unlawfully assumed for the purpose of unlawfully entering into a Merchant Agreement.

Benefit:

MATCH records details of merchants identified for Account Data Compromise Events, Common Point of Purchase Events, Laundering, Excessive Chargebacks, Excessive Fraud, Fraud Conviction, Bankrupts, Violation of Standards, Merchant Collusion, PCI Data Security noncompliance, Illegal transactions and Identity Theft.

MATCH also supports retrospective alerts for up 360 days.

By checking MATCH before signing up a new merchant ICC CAL will be able to identify high-risk merchants and take the appropriate actions (i.e. declining the application). All acquirers are required to prove that they checked the MATCH database before signing up a new merchant. Acquirers are also required to add terminated merchants for relevant reason codes to MATCH within 5 days of the decision to terminate to assist other acquirers identify high risk merchants.

2.7. Payment Facilitator Obligations

The Acquirer must ensure that its Payment Facilitator satisfies all of the obligations set forth in the **MasterCard Rule 7.8**.

Finding:

NetPay Ltd within their completed 'GRMP Questionnaire' and during the Review Meeting confirmed that they had both implemented and maintain on an ongoing basis all of the Payment Facilitator Obligations as required by MasterCard.

NETPAY LTD currently have 40 Sub-merchants under their Terms of Service and some of them already have processed in excess of \$1MN with MasterCard/Maestro transactions during last 52 weeks.

All of these Sub-merchants should have been entered into a direct contractual relationship with ICC CAL as a tri-partite agreement between all parties.

In such cases ICC CAL as the Acquirer will be required to register NetPay Ltd as a 'Third Party Processor' (TPP) within the tri-partite agreement.

As a Third Party Processor (TPP) NetPay Ltd may perform any of the following Program Services as part of any such agreement:

- POI Terminal operation with electronic data capture deployment
- Authorization services, including but not limited to authorization routing, payment gateway and switching services, voice authorization, and call referral processing
- Clearing file preparation and submission

- **Settlement processing (excluding possession, ownership, or control of settlement funds, which is not permitted)**
- Cardholder and/or Merchant statement preparation with access to Account data, Transaction data, or both
- Cardholder customer service with access to Account data, Transaction data, or both
- Fraud control and risk monitoring, including but not limited to fraud screening and fraud scoring services
- Chargeback processing
- Any other services determined by the Corporation in its sole discretion to be TPP Program Service

MasterCard would refer NetPay Ltd to the above Program Services which prevent NetPay Ltd undertaking the 'settlement' of funds to Sub-merchants processing in excess of \$1m and as a TPP then ICC CAL is required to undertake such activity.

In respect of those Sub-merchants processing in excess of \$1MN ICC CAL is required to register NETPAY LTD as a TPP acting in a tri-partite merchant agreement.

MasterCard requires ICC CAL to undertake the 'Settlement' of funds to these Merchants until such time as the Rules applicable to Payment Facilitators and TPP's are revised by MasterCard.

ICC CAL may seek a waiver to this Requirement by submitting a 'Variance Request Form' via their MasterCard Representative or via email to variance_requests@mastercard.com

These obligations are as follows:

7.8.1 Sub-merchant Agreement

The Acquirer is responsible for all acts and omissions of a Payment Facilitator and of any Sub merchant.

A Payment Facilitator may not be a Sub merchant of any other Payment Facilitator, nor may a Payment Facilitator be a Payment Facilitator for another Payment Facilitator.

Unless otherwise approved by the Corporation, any Sub merchant that exceeds USD 1,000,000 in MasterCard and Maestro combined annual Transaction volume must enter into a Merchant Agreement directly with a Customer.

7.8.1.1 Required Sub-merchant Agreement Terms

A Sub merchant Agreement must include all provisions required to be included in a Merchant Agreement, in addition to complying with Rule 7.8.1 and this Rule 7.8.1.1. The failure of the Payment Facilitator to include the substance of any one or more of such Standards in the Sub merchant Agreement or the grant of a variance by the Corporation with respect to any one or more such Standards does not relieve an Acquirer from responsibility for chargebacks or compliance related to the Activity of or use of the Marks by the Sub merchant.

The Sub merchant Agreement must, in substance, include all of the following provisions:

1. On an ongoing basis, the Sub merchant is promptly to provide the Payment Facilitator with the current address of each of its offices, all “doing business as” (DBA) names used by the Sub merchant, and a complete description of goods sold and services provided.
2. In the event of any inconsistency between any provisions of the Sub merchant Agreement and the Standards, the Standards will govern.
3. The Payment Facilitator is responsible for the Card acceptance policies and procedures of the Sub merchant, and may require any changes to its website or otherwise that it deems necessary or appropriate to ensure that the Sub merchant remains in compliance with the Standards governing the use of the Marks.
4. The Sub merchant Agreement automatically and immediately terminates if the Corporation de-registers the Payment Facilitator or if the Payment Facilitator’s Acquirer ceases to be a Customer for any reason or if such Acquirer fails to have a valid License with the Corporation to use any Mark accepted by the Sub merchant.
5. The Payment Facilitator may, at its discretion or at the direction of its Acquirer or the Corporation, immediately terminate the Sub merchant Agreement for activity deemed to be fraudulent or otherwise wrongful by the Payment Facilitator, its Acquirer, or the Corporation.
6. The Sub merchant acknowledges and agrees:
 - a. To comply with all applicable Standards, as amended from time to time;
 - b. That the Corporation is the sole and exclusive owner of the Marks;
 - c. Not to contest the ownership of the Marks for any reason;
 - d. The Corporation may at any time, immediately and without advance notice, prohibit the Sub merchant from using any of the Marks for any reason;
 - e. The Corporation has the right to enforce any provision of the Standards and to prohibit the Sub merchant and/or its Payment Facilitator from engaging in any conduct the Corporation deems could injure or could create a risk of injury to the Corporation, including injury to reputation, or that could adversely affect the integrity of the Interchange System, the Corporation’s Confidential Information as defined in the Standards, or both; and
 - f. The Sub merchant will not take any action that could interfere with or prevent the exercise of this right by the Corporation.

The Sub merchant Agreement must not contain any terms that conflict with any Standard.

7.8.2 Obligations as a Sponsor of Sub merchants

A Payment Facilitator must fulfill all of the following obligations with respect to each of its Sub-merchants.

1. Submit Valid Transactions

Finding

NetPay Ltd undertake Sub-Merchant due diligence in compliance with the MasterCard Rules in respect of the Prevention of Money Laundering and Terrorism Financing.

NetPay Ltd undertakes Sub-merchant transaction monitoring in accordance with The MasterCard Rules in respect of the Prevention of Money Laundering and Terrorism Financing.

Requirements

The Payment Facilitator must submit to its Acquirer records of valid Transactions submitted by a Sub merchant and involving a bona fide Cardholder.

The Payment Facilitator must not submit to its Acquirer any Transaction that the Payment Facilitator or the Sub-merchant knows or should have known to be fraudulent or not authorized by the Cardholder, or that either knows or should have known to be authorized by a Cardholder colluding with the Sub-merchant for a fraudulent purpose.

For purposes of this Rule, the Sub-merchant is deemed to be responsible for the conduct of its employees, agents, and representatives.

2. Sub merchant Compliance with the Standards

Finding

NetPay Ltd confirmed they have been provided with the MasterCard Rules as they apply to a Payment Facilitator and fully adhere to compliance with these rules.

NetPay Ltd hold regular meetings and conference calls with their Acquirer to discuss all aspects of the relationship and performance.

Requirements

The Payment Facilitator must ensure that each of its Sub merchants complies with the Standards applicable to Merchants.

3. Maintaining Sub merchant Information

Finding

NetPay Ltd maintains a record of each Sub-merchant during the lifecycle of the relationship which includes the MasterCard requirements and the Sub-merchant is required to notify NetPay Ltd of any changes immediately.

Requirements

The Payment Facilitator must maintain, on an ongoing basis, the names, addresses, and URLs if applicable of each of its Sub merchants. The Acquirer must ensure that the Payment Facilitator promptly supplies the Corporation with any such information upon request

4. Payments to Sub merchants

Finding

During the review, it was determined that NetPay Ltd is responsible for the settlement of funds to the Sub-merchant following receipt of funds from their Acquiring Partners.

The Sub-merchant is paid the net amount of any transaction, less all agreed fees which are then credited to the Sub-merchants account.

Requirements

Each Payment Facilitator must pay each Sub-merchant for all Transactions the Payment Facilitator submits to its Acquirer on the Sub-merchant's behalf. This obligation is not discharged with regard to a Transaction until the Sub-merchant receives payment from the Payment Facilitator with which the Sub-merchant has entered into an agreement, notwithstanding any payment arrangement between the Sub-merchant and the Payment Facilitator or between the Payment Facilitator and its Acquirer. A Sub-merchant agreement may provide for a Payment Facilitator to withhold amounts for chargeback reserves or similar purposes.

5. Supplying Materials to Sub merchants

Finding

NetPay Ltd provide both support and materials to their Sub-merchants via the following channels:

- Site inspections
- Online Portal
- Help Desk

Requirements

Each Payment Facilitator must regularly ensure that each of its Sub merchants is provided with all materials necessary to effect Transactions in accordance with the Standards and to signify Card acceptance.

6. Sub merchant Monitoring

See Section 2.3

Requirements

Each Payment Facilitator must monitor on an ongoing basis the Activity and use of the Marks of each of its Sub merchants for the purpose of deterring fraudulent and other wrongful activity and to ensure ongoing compliance with the Standards. For purposes of this Rule, the minimum Merchant monitoring Standards set forth in the *Security Rules and Procedures* manual apply with respect to Sub merchants.

2.8. Sub Merchant Compliance with Standards

Requirements

The Payment Facilitator is responsible for ensuring that each of its Sub-merchants complies with the Standards, including but not limited to the Rules 5.5, 5.6 and Rule 5.7. The Payment Facilitator must take such actions that may be necessary or appropriate to ensure the Sub-merchant's ongoing compliance with the Standards.

5.5 Sub-merchant Location

Finding:

NetPay Ltd undertake Sub-Merchant due diligence in compliance with the MasterCard Rules and Money Laundering Regulations 2007 (As Amended) in order to identify the location of the Sub-merchant.

As Netpay Ltd. is registered in only in Israel under the company registration No. 513279000, **Netpay Ltd may have no rights to passport its activities and services within the European Union (EU) & European Economic Area (EEA).**

NetPay Ltd are fully aware of the MasterCard requirements that a Sub-merchant may accept Cards only at locations that are within the Acquirer's Area of Use and as part of their due-diligence upon boarding a Sub-merchant review the location of a Sub-merchant to ensure compliance with this requirement.

Requirements:

Except as otherwise provided in the Standards, a **Sub-merchant may accept Cards only at locations that are within the Acquirer's Area of Use.**

In the absence of persuasive contrary information, a Sub merchant's location generally is deemed to be the address set forth in the Sub merchant Agreement. The Acquirer is responsible for verifying that such address is a location from which the Sub merchant is conducting the business described in the Sub merchant application, or the Acquirer may permit the Payment Facilitator to manage this obligation on its behalf. When determining a Sub merchant's location, the Acquirer or Payment Facilitator should consider, among other factors, whether the Sub merchant

- (i) holds a business license or is otherwise authorized to conduct the business;
- (ii) pay taxes; and
- (iii) maintains an office or other physical presence and can receive business-related mail. By way of example and not limitation, a post office box address, the location at which a server is stored, the address of a warehouse having no business-related functions, and the Uniform Resource Locator (URL) of a website do not establish a physical location. The Acquirer must transmit the Sub merchant location, substantially the same as it appears on any Transaction receipt provided, in DE 43.

Any disagreement between Customers regarding a Sub merchant location may be referred to the Corporation for final resolution. The Corporation has the right, at any time, to determine a Sub merchant's location based upon such information as may be available.

5.5.1 Disclosure of Sub merchant Location

Finding:

NetPay Ltd as part of their due diligence procedures in support of their Acquirer, ICC CAL ensures that their Sub-merchants are compliant with the MasterCard requirements in respect of 'Disclosure of Sub-merchant Location'

Requirements:

An Acquirer must ensure that each of its Payment Facilitators' Sub merchants prominently and clearly discloses to the Cardholder at all points of interaction:

1. The name of the Sub merchant, so that the Cardholder can easily distinguish the Sub merchant from any other party, such as a supplier of products or services to the Sub merchant; and
2. The location (physical address) of the Sub merchant to enable the Cardholder to easily determine, among other things, whether the Transaction will be a Domestic Transaction or a Cross-border Transaction. The Sub merchant location must be disclosed before the Cardholder is prompted to provide Card information.

The Sub merchant name and location, as disclosed to the Cardholder, must be the same as what is provided in authorization and clearing Transaction messages.

5.6 Responsibility for Transactions

Finding:

NetPay Ltd as part of their due diligence procedures in support of their Acquirer, ICC CAL ensures that their Sub-merchants are compliant with the MasterCard requirements in respect of 'Responsibility for Transactions'

NetPay Ltd also acting on behalf of their Sub-merchants provides 'Help Desk Service' and 'Dispute Resolution' function.

Requirements:

Each Merchant and Sub merchant must ensure that the Cardholder is easily able to understand that the Merchant or Sub merchant is responsible for the Transaction, including delivery of the goods (whether physical or digital) or provision of the services that are the subject of the Transaction, and for customer service and dispute resolution, all in accordance with the terms applicable to the Transaction.

5.7 Transaction Message Data

Finding:

NetPay Ltd submits transaction messaging in respect of all authorization and clearing messages in accordance with the MasterCard Standards and in accordance with the requirements as provided by their Acquirer, ICC CAL.

Requirements:

An Acquirer must provide valid, accurate, and consistent data in all authorization and clearing Transaction messages. Refer to the *Single Message System Specifications*, *Customer Interface Specification* and *IPM Clearing Formats* manuals for technical Requirements relating to Transaction data.

5.7.1 Card Acceptor Business Code (MCC) Information

Finding:

NetPay Ltd applies the appropriate MCC's for all sub-merchants and communicates these when submitting new merchant's applications to the Acquirer, ICC CAL.

NetPay Ltd currently has no Sub-merchants providing goods or services which require specific MCC identification.

Requirements:

The Acquirer must ensure that each Merchant and Sub merchant is identified in authorization and clearing Transaction messages with the Card acceptor business code (MCC) that reflects the primary business of the Merchant or Sub merchant.

Any Transaction that includes the sale of products or services properly identified with one of the following MCCs must be identified with such MCC:

- Gambling Transactions (MCC 7995)
- Money Transfer (MCC 4829)
- Quasi Cash—Customer Financial Institution (MCC 6050)
- Quasi Cash—Merchant (MCC 6051)

For MCC descriptions, refer to Chapter 3 of the *Quick Reference Booklet*.

MasterCard shall have the ultimate authority to dictate the appropriate MCC if any dispute shall arise.

5.7.2 Sub merchant Name Information

Finding:

During the review, it was determined that NetPay Ltd has the capability to utilize a unique merchant descriptor identifier with each Sub-merchant.

- NetPay Ltd Brand Name*Sub-merchant

Requirements:

If the Cardholder is linked to a Payment Facilitator's website from a Sub merchant's website for payment, the name of the Payment Facilitator must appear in DE 43 (Card Acceptor Name/Location), subfield 1 (Card Acceptor Name) in conjunction with the name of the Sub merchant.

If the Cardholder accesses the Payment Facilitator's website directly, and its name is visible to the Cardholder throughout Transaction from selection of products and/or services to the completion of the checkout process, then the Payment Facilitator's name may appear in DE 43 without the name of the Sub merchant. For Card-present Transactions, both the Payment Facilitator name and the Sub merchant name must appear in DE 43, unless only the name of the Payment Facilitator is known to the Cardholder.

Effective for Transactions occurring on or after 17 April 2015, the Acquirer must ensure that a Transaction conducted by a Sub merchant includes the names of both the Payment Facilitator and the Sub merchant in DE 43 (Card Acceptor Name/Location), subfield 1 (Card Acceptor Name). The Payment Facilitator name, in full or in abbreviated form, must be three, seven, or 12 characters in length, followed by "*" and the Sub merchant name.

2.9. Business Risk Assessment and Mitigation (BRAM)

Finding

NetPay Ltd confirmed that their Acquiring Partner ICC CAL contracts directly with G2 LLC to undertake their 'web content monitoring'.

It was confirmed during the review that NetPay Ltd submits all Sub-merchant URL's to ICC CAL who in turn upload to G2 LLC for the following services:

- Persistent Merchant Monitoring
- Transaction Laundering

NetPay Ltd evidenced it is not performing acquiring activities with Sub-merchants classified as high-risk by MasterCard definitions, however NetPay Ltd expressed its interest to know the duties behind such activities.

MasterCard Standards require customers to comply with all applicable laws and not to engage in illegal behavior, or in behavior that would reflect negatively on MasterCard. MasterCard launched the BRAM Program in 2005 to protect MasterCard, its customers, merchants, and cardholders from activities that may be illegal or could negatively impact the brands of MasterCard, and other stakeholders in the payments network. MasterCard launched the BRAM Monitoring Program (BMP) in 2007. The BMP is a non-mandated program available to any acquirer processing electronic commerce (e-commerce) transactions. As part of the BMP, acquirers chose the services of either G2 or Trustwave or any other web-crawling agent they selected to monitor their merchant portfolios. MasterCard Standards encourage acquirers to effectively screen and actively monitor the activity of each merchant.

MasterCard encourages each acquirer to conduct due diligence on each of its merchants and their services on an ongoing basis to determine the legality and legitimacy of the goods or services being offered for sale and the jurisdictions where they are being sold.

As a reminder, the impermissible activities addressed by the BRAM program include, but are not limited to the:

- Illegal sale of drugs on Schedule I of the Controlled Substances Act (CSA), or that are otherwise prohibited by applicable law from being sold
- Illegal sale of prescription drugs
- Illegal sale of tobacco products
- Brand-damaging sale of images of offensive and/or non-consensual adult pornography
- Illegal sale of images of child exploitation
- Facilitation of Internet gambling in jurisdictions where it is illegal
- Sale of counterfeit merchandise
- Sale of goods or services in violation of intellectual property rights
- Sale of illegal electronic devices (such as modification chips and jammers)
- Sale of certain types of drugs or chemicals (such as synthetic drugs, salvia divinorum, psilocybin mushrooms and spores, and nitrite inhalants)
- Illegal sale of any other product or service

NOTE: The products, services, and merchant models mentioned in this article do not represent an exhaustive list of illegal or brand-damaging activities.

MasterCard appreciates its customers' ongoing cooperation in helping prevent illegal or brand-damaging merchant activity from entering the MasterCard Payments network.

Recent Trends

MasterCard has become aware of new product offerings from other vendors available in the market for monitoring illegal or brand-damaging transactions (“BRAM monitoring”) in addition to the services provided by G2, Trustwave or other Merchant Monitoring Service Providers. New products have also been developed to detect occurrences of “merchant transaction laundering.” Both of these types of products are essential for effective merchant monitoring to help ensure compliance with MasterCard Standards.

What is Merchant Transaction Laundering?

Merchant transaction laundering is the action whereby a merchant processes payment card transactions on behalf of another merchant (also known in the industry as “factoring” or “transaction aggregation”). MasterCard has observed an increase in the number of BRAM compliance investigations concerning merchant transaction laundering. In most cases, it appears that the acquirer was not aware of such activity and did not implement a sufficiently robust monitoring or detection service to address this activity. Without a viable monitoring service in place, the acquirer may have difficulty in detecting merchant transaction laundering and consequently the BRAM activity resulting from the unknown merchant transaction laundering. MasterCard deems merchant transaction laundering to be a violation of MasterCard Rule 5.1.

Merchant transaction laundering may trigger BRAM noncompliance as well as assessments for noncompliance with other MasterCard Standards, such as card acceptor business code (MCC) miscoding violations or failure to register a high-risk merchant through the MasterCard Registration Program (MRP). MasterCard encourages acquirers to monitor for and detect merchant transaction laundering.

Introducing the Merchant Monitoring Program (MMP)

MasterCard is replacing the BMP to adapt to new trends and technologies in the industry and to further MasterCard compliance efforts and those of its customers. The new MMP is designed to:

- Encourage acquirers to proactively monitor for and prevent BRAM violations related to content, products, and services.
- Encourage acquirers to proactively monitor for and prevent merchant transaction laundering.
- Create an optional framework to incent transaction laundering detection.
- Permit acquirers to leverage any service provider as a solution for BRAM monitoring and merchant transaction laundering detection services.
- Require acquirers to register their chosen service provider to participate in the MMP.
- Provide potential assessment mitigation for acquirers that register an MMSP for monitoring and detecting BRAM and merchant transaction laundering activity and comply with MMP Requirements.
- Supersede use of the LOU under the current BMP.

MasterCard reminds acquirers that they are solely responsible for ensuring that their merchants’ activity complies fully with MasterCard Standards.

MMP and MMSP Requirements

If the acquirer chooses to participate in the MMP, the acquirer must:
(Revised Standards)

- Register the MMSP with MasterCard and provide a description of the MMSP’s services, URL, and related marketing materials describing the services being rendered.
- Submit to the MMSP for monitoring all merchant information and any data that the MMSP needs to successfully monitor the particular merchant (including the merchant name, all merchant URLs, the Doing-Business-As [DBA] name and address).

- Ensure that the MMSP persistently monitors on a monthly and ongoing basis for any identifications related to BRAM content, products, and services and/or monitors and detects merchant transaction laundering.
- Ensure that the MMSP is identifying and reporting to the acquirer all identifications of BRAM and/or merchant transaction laundering.
- Investigate and take action in response to the identification report provided by the MMSP by ceasing any violating activity or event within 15 days of the notification from the MMSP.
- Report the resolution of the identification to the MMSP within 15 calendar days of the original MMSP notification and prior to MasterCard identification and notification.
- Provide MasterCard with a monthly report of all merchants and URLs monitored, which must include all identifications and resolutions for any merchant monitored and submitted by either the MMSP with a copy to the acquirer or directly from the acquirer.
- Provide an MMSP Incident Report if an MMSP monitored merchant and URL are identified by MasterCard but not identified by the MMSP, and provide an explanation of how and why the violation was not detected and how the MMSP will resolve to ensure that future identifications will be detected.

As a reminder, an Acquirer must add any merchant terminated for reason of a BRAM violation to the MasterCard Alert to Control High-risk Merchants (MATCH™) system per the MasterCard MATCH Requirements.

Acquirers that register an MMSP may be afforded a level of assessment mitigation if the acquirer performs all program and reporting Requirements. If an acquirer fails to meet all of the Requirements, MasterCard reserves the right to apply the related assessments. If an acquirer has its own internal dedicated system to persistently monitor and detect for BRAM and/or transaction laundering, the acquirer may register itself. Such an acquirer must comply with all of the MMP Requirements.

Acquirer Use of an MMSP

MasterCard has created a new service provider category called an MMSP. Acquirers can voluntarily register MMSPs as a service provider with MasterCard for participation in the MMP.

An acquirer may choose a single service provider to provide both BRAM monitoring and merchant transaction laundering detection services, or the acquirer may elect to choose two or more service providers to provide BRAM monitoring and merchant transaction laundering detection services. If the acquirer chooses to participate in the MMP, the acquirer must register the MMSP or itself along with its internal detection system and comply with all MMP and service provider Requirements.

To register an MMSP, the acquirer must submit all information and materials required by MasterCard in connection with the proposed registration via email message to Email: mmp@mastercard.com

Acquirer or MMSP Monthly Report Submission Requirements

MasterCard will require the acquirer or MMSP to provide monthly reports as part of participation in the MMP. The report format has been developed by MasterCard, and all data fields must be complete and accurate. Data fields required include:

- Acquirer name and ICA number
- MMSP name
- Report submitter contact name and email address
- Merchant name
- URL(s)
- MCC
- Violation type

- Violation category
- URL content details
- Date MMSP reported to acquirer
- Date acquirer resolved and reported to MMSP Investigation findings and final resolution status

This monthly report must be received by MasterCard on the fifth day of the month for the preceding month's monitoring. The acquirer or MMSP must send the report via the file transfer protocol (FTP) system or via email message to Email: **mmp@mastercard.com**

It is the responsibility of the Acquirer to ensure that the report is received by MasterCard per the required date. Failure to provide the monthly report on time may result in the loss of mitigation of an assessment in the event of a BRAM or merchant transaction laundering violation. If the report is not complete, then MasterCard will reject the report. The report then must be resubmitted within two business days.

MMP Assessment and Mitigation Structure

MasterCard has enhanced the assessment and mitigation framework to provide mitigation for participation in the MMP. MasterCard may adjust the assessment mitigation structure at any time at its discretion.

The following table depicts scenarios and the potential mitigation of noncompliance assessments relating to a particular merchant. With regard to any particular merchant, MasterCard retains discretion in determining whether any mitigation is appropriate and the amount of such mitigation.

Scenario	If the acquirer has a registered MMSP or registered an internal dedicated detection system and has complied with all MMP requirements	If the acquirer does not have an MMSP, or has not registered an internal dedicated detection system, or is using an unregistered MMSP
BRAM or merchant transaction laundering activity ("activity") was proactively identified by the acquirer via its registered internal dedicated detection system or by the acquirer's MMSP, and the activity was ceased prior to MasterCard identification	100% mitigation	100% mitigation
No detection of activity by the acquirer via its registered internal dedicated detection system or by the acquirer's MMSP, but MasterCard identified the violating activity, and the activity was ceased within two business days of MasterCard identification	75% mitigation	25% mitigation
No detection of activity by the acquirer via its registered internal dedicated detection system or by the acquirer's MMSP, but MasterCard identified the violating activity, and the activity was not ceased within two business days	0% mitigation	0% mitigation

MasterCard recognizes that there is the risk of poor performance of an MMSP. Therefore, MasterCard encourages acquirers to vet prospective MMSPs thoroughly to minimize the likelihood of poor performance. If an MMSP does not identify and report a possible violation, the acquirer must provide to MasterCard an MMSP Incident Report within five business days of the identification notification sent by

MasterCard. The incident report must provide an explanation for how and why the identification was not detected and how the MMSP will resolve to ensure future violations will be detected.

An acquirer may not receive mitigation for:

- Repeated failures by the MMSP or internal dedicated detection system to identify violations
- Repeated violations
- A merchant or URL that was not monitored by the registered MMSP or internal dedicated detection system
- Non-submission of the monthly MMSP report
- Non-submission of an incident report
- Failure to respond to an investigation

Benefit

Compliance with the MasterCard BRAM & Merchant Monitoring Program (MMP) will enhance the ability of NetPay Ltd to identify Sub-merchants conducting illegal or fraudulent activities and reduce your risk of non-compliance with MasterCard standards due to unregistered merchants or merchants with BRAM violations – in case you will plan to conduct such Sub-merchants acquiring.

2.10. MasterCard Registration Program

Finding

During the review, it was determined that NetPay Ltd does operate as a High Risk Payment Facilitator.

NetPay Ltd are fully aware of the MasterCard registration Requirements for specified High Risk MCC's should they recruit within other sectors in the future.

Recommendation

If any merchants are identified that require registration, ensure that they are registered and general monitoring Requirements satisfied as per **Chapter 9 of the Security Rules and Procedures**.

Requirements

Section 9 of the MasterCard's Security Rules and Procedures 9 states in part:

9.1 *MasterCard Registration Program Overview*

MasterCard require Customers to register the following Merchant types, including Sub merchants, and other entities using the MasterCard Registration Program (MRP) system, available via MasterCard Connect™:

- Non-face-to-face adult content and services Merchants—MCCs 5967 and 7841 (refer to section 9.4.1)
- Non-face-to-face gambling Merchants—MCCs 7995 and 9754 (refer to section 9.4.2)
- Non-face-to-face pharmaceutical Merchants—MCC 5122 and MCC 5912 (refer to section 9.4.3)
- Non-face-to-face tobacco product Merchants—MCC 5993 (refer to section 9.4.3)

- Merchants reported under the Excessive Chargeback Program (refer to section 8.3)

High-Risk Cyberlocker Registration Requirements

Effective 15 September 2015, Acquirers must register a cyberlocker merchant or sub merchant that exhibits one or more of the high-risk criteria stated in this article. Any entity (such as a reseller, affiliate, payment facilitator, or digital wallet operator) that provides access to, or accepts payments on behalf of, such a cyberlocker will be also deemed by MasterCard as a high-risk cyberlocker merchant.

During registration, the Acquirer must provide each website URL from which transactions may arise, whether the website is that of the cyberlocker merchant, sub merchant, or other entity.

Acquirers must register high-risk cyberlockers under card acceptor business code (MCC) 4816 (Computer Network/Information Services) via the MRP system. In addition, acquirers must identify such cyberlockers with MCC 4816 and transaction category code (TCC) T for transactions occurring on or after 15 September 2015.

Refer to MasterCard Global Security Bulletin No. 3, 13 March 2015 - Addition of Cyberlockers to the BRAM Program and Revised Standards for Cyberlocker Merchant Registration

During registration, the Acquirer must provide each website URL from which Transactions as described in this section may arise, whether the website is that of a Merchant, a Payment Facilitator's Sub merchant, or other entity. With respect to Transactions submitted by a Staged Digital Wallet Operator (DWO), each individual website URL at which Transactions as described in this section may be effected must be individually registered.

If a Customer acquires Transactions for any of the Merchant types listed herein without first registering the Merchant or Sub merchant in accordance with the Standards described in this section, MasterCard may assess the Customer as set forth in section 9.2.1 of this manual. In addition, the Acquirer must ensure that the violation is corrected promptly.

9.2 General Registration Requirements

The Customer must provide all of the information requested for each Merchant, Sub merchant, or other entity required to be registered through the MRP system. For each such entity, the requested information includes:

- The name, doing business as (DBA) name, and address
- The central access phone number, customer service phone number, or e-mail address
- The name(s), address(es), and tax identification number(s) (or other relevant national identification number) of the principal owner(s)
- A detailed description of the service(s), product(s), or both that the entity will offer to Cardholders
 - A description of payment processing procedures, Cardholder disclosures, and other practices including, but not limited to:
- Data solicited from the Cardholder
- Authorization process (including floor limits)

- Customer service return policies for card transactions
- Disclosure made by the Merchant before soliciting payment information (including currency conversion at the Point of Interaction [POI])
- Data storage and security practices
- The identity of any previous business relationship(s) involving the principal owner(s) of the entity
- A certification, by the officer of the Customer with direct responsibility to ensure compliance of the registered entity with the Standards, stating that after conducting a diligent and good faith investigation, the Customer believes that the information contained in the registration request is true and accurate

Only MasterCard can modify or delete information about a registered entity. Customers must submit any modification(s) about a registered entity in writing to MasterCard, with an explanation for the request. MasterCard reserves the right to deny a modification request.

Customers should send any additional requested information and modification requests to the vice president of Merchant Fraud Control at the address provided in Appendix C.

For Requirements specific to Merchants that are required to implement the MasterCard SDP Program, refer to section 10.3 of this manual.

9.3 General Monitoring Requirements

The monitoring Requirements described in this section apply to Customers that acquire non-face-to-face adult content and services Transactions, non-face-to-face gambling Transactions, non-face-to-face pharmaceutical and tobacco product Transactions, state lottery Transactions (U.S. Region only), skill games Transactions (U.S. Region only), or Transactions from Merchants reported under the Excessive Chargeback Program:

The Acquirer must ensure that each such Merchant implements real-time and batch procedures to monitor continually all of the following:

- Simultaneous multiple Transactions using the same Account number
- Consecutive or excessive attempts using the same Account number
- When attempted fraud is evident, a Merchant should implement temporary bank identification number (BIN) blocking as a fraud deterrent.
- The Acquirer must ensure that each such Merchant complies with the fraud control Standards in Chapter 6 of this manual and maintains a total chargeback-to-interchange sales volume ratio below the Excessive Chargeback Program thresholds. For information about the Excessive Chargeback Program, refer to section 8.3 of this manual.

9.4 Additional Requirements for Specific Merchant Categories

Customers should review thoroughly these additional Requirements for specific Merchant categories.

9.4.1 Non-face-to-face Adult Content and Services Merchants

A non-face-to-face adult content and services Transaction occurs when a consumer uses an Account in a Card-not-present environment to purchase adult content or services, which may include but is not limited to subscription website access; streaming video; and videotape and DVD rentals and sales.

An Acquirer must identify all non-face-to-face adult content and services Transactions using one of the following MCC and TCC combinations, as appropriate:

- MCC 5967 (Direct Marketing—Inbound Telemarketing Merchants) and TCC T; or
- MCC 7841 (Video Entertainment Rental Stores) and TCC T.

Before an Acquirer may process non-face-to-face adult content and services Transactions from a Merchant or Sub merchant, it must register the Merchant with MasterCard as described in section 9.2 of this manual.

9.4.2 Non-face-to-face Gambling Merchants

A non-face-to-face gambling Transaction occurs in a Card-not-present environment when a consumer uses an Account to place a wager or purchase chips or other value usable for gambling provided by a wagering or betting establishment as defined by MCC 7995 (Gambling Transactions) or MCC 9754 (Gambling—Horse Racing, Dog Racing, Non-Sports Intrastate Internet Gambling).

Before acquiring Transactions reflecting non-face-to-face gambling, an Acquirer first must register the Merchant or Sub merchant with MasterCard as described in section 9.2.

An Acquirer must identify all non-face-to-face gambling Transactions using MCC 7995 and TCC U unless the Acquirer has also registered the Merchant or Sub merchant as described below, in which case the Acquirer may use MCC 9754 instead of MCC 7995.

[...]

Notification of changes. The Acquirer must certify that it will notify MasterCard of any changes to the information that it has provided to MasterCard, including changes in applicable law, Merchant activities, and Merchant systems. Such notification shall include

- Any revisions or additions to the information provided to MasterCard (for example, legal opinion, third-party certification) to make the information current and complete. Such notification is required within ten (10) days of any such change.

Acceptance of responsibilities. The Acquirer must specifically affirm that it will not submit restricted Transactions from the Merchant for authorization. The Acquirer must also specifically reaffirm its indemnification to MasterCard in connection with the Acquirer's or Merchant's activities. Such reaffirmation shall specifically indicate that the Acquirer acknowledges and agrees that the Transactions constitute the Acquirer's Activity and are subject to Rule 2.3 of the *MasterCard Rules* manual, regardless of the Acquirer's compliance with the MasterCard *Internet Gambling Policy* or these Requirements.

9.4.3 Pharmaceutical and Tobacco Product Merchants

A non-face-to-face pharmaceutical Transaction occurs in a Card-not-present environment when a consumer uses an Account to purchase prescription medicines from a Merchant whose primary business is non-face-to-face selling of prescription drugs.

A non-face-to-face tobacco product Transaction occurs in a Card-not-present environment when a consumer uses an Account to purchase tobacco products (including, but not limited to cigarettes, cigars,

or loose tobacco) from a Merchant whose primary business is non-face-to-face selling of tobacco products.

Before acquiring Transactions as described below, an Acquirer first must register the Merchant with MasterCard as described in section 9.2:

- Non-face-to-face sale of pharmaceuticals (MCC 5122 and MCC 5912)
- Non-face-to-face sale of tobacco products (MCC 5993)

An Acquirer must identify all non-face-to-face pharmaceutical Transactions using MCC 5122 (Drugs, Drug Proprietors, and Druggists Sundries) and TCC T for wholesale purchases or MCC 5912 (Drug Stores, Pharmacies) and TCC T for retail purchases. An Acquirer must identify all non-face-to-face tobacco product Transactions using MCC 5993 (Cigar Stores and Stands) and TCC T.

For clarity, the term acquiring, as used in this section, is “acquiring Activity” as such term is used in Rule 2.3 of the *MasterCard Rules* manual.

At the time of registration of a Merchant or Sub merchant in accordance with this section, the Acquirer of such Merchant or Sub merchant must have verified that the Merchant’s or Sub merchant’s activity complies fully with all laws applicable to MasterCard, the Merchant or Sub merchant, the Issuer, the Acquirer, and any prospective customer of the Merchant or Sub merchant. Such verification may include, but is not limited to, a written opinion from independent, reputable, and qualified legal counsel or accreditation by a recognized third party.

By registering a Merchant or Sub merchant as required by this section, the Acquirer represents and warrants that the Acquirer has verified compliance with applicable law as described above. The Acquirer must maintain such verification for so long as it acquires Transactions from the Merchant or Sub merchant that is subject to the afore described registration requirements and must, no less frequently than every 12 months, confirm continued compliance with applicable law concerning the business of the registered Merchant or Sub merchant. The Acquirer must furnish MasterCard with a copy of such documentation promptly upon request.

Benefit

Ensuring high risk merchants are identified and registered in accordance with MasterCard Requirements will enable NetPay Ltd to assess and mitigate the risk for these types of merchants. In addition, non-face to face gambling, prescription drug, tobacco and ecommerce adult content merchants that are properly registered decreases the risk of entering into agreements with merchants that are not in compliance with MasterCard’s Business Risk Assessment and Mitigation (BRAM) Program.

2.11. Excessive Chargeback Program (ECP)

Finding

During the review, it was determined that NetPay Ltd does not have merchants currently in MasterCard Excessive Chargeback Program.

NetPay Ltd indicates it is familiar with this particular program and monitors Sub-merchant chargeback activity against the program thresholds in order to identify activity which may violate the program and enable NetPay Ltd to take appropriate action to mitigate potential risk.

Recommendation

It is recommended NetPay Ltd includes ECP within their Risk Management Policy to help ensure the ongoing compliance and senior management visibility.

Requirements

Section 8.3 of the MasterCard Security Rules and Procedures states in part:

8.3 Excessive Chargeback Program

MasterCard designed the Excessive Chargeback Program (ECP) to encourage each Acquirer to closely monitor, on an ongoing basis, its chargeback performance at the Merchant level and to determine promptly when a Merchant has exceeded or is likely to exceed monthly chargeback thresholds.

8.3.1 Definitions

The following terms used in the ECP have the meanings set forth below.

Merchant

A Merchant is defined as any distinct Merchant location, whether a Merchant's physical location or a Merchant's Internet site or uniform resource locator (URL) that is identified by a distinct billing descriptor by the Acquirer in the Transaction record.

Chargeback-to-Transaction Ratio (CTR)

The CTR is the number of MasterCard chargebacks received by the Acquirer for a Merchant in a calendar month divided by the number of the Merchant's MasterCard sales Transactions in the preceding month acquired by that Acquirer. (A CTR of 1% equals 100 basis points, and a CTR of 1.5% equals 150 basis points.)

Chargeback-Monitored Merchant (CMM)

A CMM is a Merchant that has a CTR in excess of 100 basis points and at least 100 chargebacks in a calendar month.

Excessive Chargeback Merchant (ECM)

A Merchant is an ECM if in each of two consecutive calendar months (the "trigger months"), the Merchant has a minimum CTR of 150 basis points and at Least 100 chargebacks in each month. This designation is maintained until the ECM's CTR is below 150 basis points for two consecutive months.

8.3.2 Reporting Requirements

It is the Acquirer's responsibility on an ongoing basis to monitor each of its Merchants in accordance with the Standards, including but not limited to sections 6.2.2, 7.2, and 7.2.3 of this manual.

The ECP requires an Acquirer to calculate, for each calendar month, the CTR in basis points for each of its Merchants and report to MasterCard any Merchant that is a CMM or ECM as defined in section 8.3.1.

MasterCard will assess an Acquirer of a CMM or ECM the reporting fees set forth in section 8.3.2.2.

2.12. Global Merchant Audit Program (GMAP)

Finding

During the review, it was determined that NetPay Ltd is aware of the GMAP Program Requirements and the need to monitor its merchant portfolio against the GMAP thresholds to identify merchant potentially creating a risk to the business.

Currently NetPay Ltd receives GMAP notifications directly from ICC CAL upon being reported by MasterCard.

MasterCard acknowledged that monitoring the merchant portfolio against reported fraud is dependent upon the receipt of confirmed fraud reports from the respective Acquirer(s) from SAFE and Fraud Reporter.

It was confirmed during the GRMP Review that NetPay Ltd receive SAFE and Fraud Reporter reports from ICC CAL for any of their Sub-merchants subject of a 'confirmed' fraud report by the respective Issuer.

Recommendation

It is recommended NetPay Ltd includes GMAP within their Risk Management Policy to help ensure the ongoing compliance and senior management visibility.

NetPay Ltd should seek agreement from ICC CAL (and any future acquiring partners) the receipt of confirmed fraud data provided by MasterCard to the Acquirer via SAFE and Fraud Reporter.

By reviewing all Sub-merchants against GMAP criteria will alert NetPay Ltd to any Sub-merchants that process higher levels of fraudulent transactions than would normally be expected and ensure the appropriate actions are taken to mitigate any potential fraud and chargeback risk.

Requirements

Section 8.2 of the MasterCard Security Rules and Procedures Section states in part:

8.2 Global Merchant Audit Program

The Global Merchant Audit Program (GMAP) uses a rolling six months of data to identify Merchant locations that, in any calendar month, meet the criteria set forth in Table 8.1.:

Fraud Criteria for Global Merchant Audit Program Tier Classification

Tier 1 – Informational Fraud Alert

- Three fraudulent Transactions
- At least USD 3,000 in fraudulent Transactions
- A fraud-to-sales dollar volume ratio minimum of 3% and not exceeding 4.99%

Tier 2 – Suggested Training Fraud Alert

- Four fraudulent Transactions
- At least USD 4,000 in fraudulent Transactions
- A fraud-to-sales dollar volume ratio minimum of 5% and not exceeding 7.99%

Tier 3 – High Fraud Alert

- Five fraudulent Transactions
- At least USD 5,000 in fraudulent Transactions
- A fraud-to-sales dollar volume ratio minimum of 8%

If a Merchant location is identified in multiple tiers during any rolling six-month period, GMAP will use the highest tier for the Merchant identification.

If a Merchant has more than one location (or outlet), the program criteria apply to each location independently.

8.2.1 Acquirer Responsibilities

MasterCard will notify an Acquirer of the identification of a Tier 1, Tier 2, or Tier 3 Merchant via the Merchant Online Status Tracking (MOST) tool. GMAP Merchant identifications are provided for information only and no Acquirer response is necessary. **Currently Suspended** - If MasterCard notifies an Acquirer via MOST that a Tier 3 special Merchant audit has been initiated, the Acquirer must respond as described in section 8.2.2.

When a Merchant is identified in Tier 1, Tier 2, or Tier 3, the Acquirer should evaluate the fraud control measures and Merchant training procedures in place for the Merchant. MasterCard strongly recommends that the Acquirer act promptly to correct any identified deficiencies. Suggested enhancements are described in the GMAP Best Practices Guide for Acquirers and Merchants to Control Fraud.

MasterCard, in its sole discretion, may conduct an audit to determine whether a Merchant location is in violation of MasterCard Rule 5.9.1 (a “questionable Merchant”), as described in section 8.1.3, and may assign chargeback liability.

2.13. Questionable Merchant Audit Program (QMAP)

Finding

During the review it was determined NetPay Ltd does not monitor their Sub-Merchant portfolios for ‘QMAP’ violation activity. It was not determined if ICC CAL does, as it was not scope of analysis.

Although MasterCard does not anticipate that NetPay Ltd would have any Sub-merchants falling into this particular Program, NetPay Ltd should make themselves aware of the Program and ensure that their Acquiring Partner is also monitoring for such activity.

Recommendation

It is recommended that NetPay Ltd and their Acquiring Partner(s) monitor their respective merchant portfolios against QMAP Requirements which became effective on the 30th June 2013 when MasterCard launched the Program, which replaced and expanded the existing Cardholder Merchant Collusion

Program to include collusive or otherwise fraudulent merchant activity, which may or may not have involved bust-out accounts.

The QMAP uses similar audit and issuer recovery procedures as currently used in the CMC Program; however, the QMAP includes separate criteria for identifying Questionable Merchants that either have or have not processed transactions on bust-out accounts.

It is recommended that NetPay Ltd engage directly with their Acquiring Partners to confirm monitoring has been implemented against the QMAP compliance thresholds and that processes are in place to alert NetPay Ltd of any violations.

QMAP Overview

The Questionable Merchant Audit Program (QMAP) establishes minimum standards of acceptable Merchant behavior and identifies Merchants that may fail to meet such minimum standards by participating in collusive or otherwise fraudulent or inappropriate activity. The QMAP also permits an Issuer to obtain partial recovery of up to one-half of actual fraud losses resulting from fraudulent Transactions at a Questionable Merchant, based on SAFE reporting.

The criteria to identify a Questionable Merchant and the fraud recovery process can be found within **Chapter 8.4 MasterCard Security Rules & Procedures**

Benefit

By establishing monitoring processes for all merchants under the NETPAY LTD portfolio against QMAP criteria will ensure that NETPAY LTD are alerted to the potential of any merchant engaged in collusive or otherwise fraudulent or inappropriate activity and ensure the relevant actions are taken to mitigate any potential risk.

Using an audit checklist for all MasterCard's compliance programs will ensure NETPAY LTD satisfies its compliance obligations and drive staff accountability and senior management visibility

2.14. Account Data Compromise Event Management

Finding

During the review, it was determined that NetPay Ltd are familiar with the MasterCard Account Data Compromise (ADC) Standards and the requirements in the event of an ADC Event. There are formal policy and procedures in respect of such events however NetPay Ltd nor their Sub-merchants were knowingly testing them for the sake of performance and effectiveness for any payment card account data compromise or potential compromise and their respective events management.

MasterCard would still recommend that NetPay Ltd has an ADC Event Management Plan in place which sets out the Requirements should such an event be identified and is contained within their company 'IT Security' Policy.

Any existing ADC Event Management Plan should include MasterCard specific Requirements.

Requirements

Section 10.2 of the MasterCard's Security Rules and Procedures states in part:

When a Customer or its Agent becomes of an ADC Event or Potential ADC Event either in any of its own systems or environments or in the systems or environments of its Agent(s), the Customer must take (or cause the Agent to take) the following actions, unless otherwise directed in writing by MasterCard.

- Immediately commence a thorough investigation into the ADC Event or Potential ADC Event.
- Immediately, and no later than within twenty-four (24) hours, identify, contain, and mitigate the ADC Event or Potential ADC Event, secure MasterCard account data and preserve all information, in all media, concerning the ADC Event or Potential ADC Event, including:
 1. preserve and safeguard all potential evidence pertinent to a forensic examination of an ADC Event or Potential ADC Event;
 2. isolate compromised systems and media from the network;
 3. preserve all Intrusion Detection Systems, Intrusion Prevention System logs, all firewall, Web, database and events logs;
 4. document all incident response actions; and refrain from restarting or rebooting any compromised or potentially compromised system or taking equivalent or other action that would have the effect of eliminating or destroying information that could potentially provide evidence of an ADC Event or Potential ADC Event.
- Within twenty-four (24) hours, and on an ongoing basis thereafter, submit to MasterCard all known or suspected facts concerning the ADC Event or Potential ADC Event, including, by way of example and not limitation, known or suspected facts as to the cause and source of the ADC Event or Potential ADC Event.
- Within twenty-four (24) hours and continuing throughout the investigation and thereafter, provide to MasterCard, in the required format, all PANs and expiration dates associated with Account data that were actually or potentially accessed or disclosed in connection with the ADC Event or Potential ADC Event and any additional information requested by MasterCard. As used herein, the obligation to obtain and provide PANs to MasterCard applies to any MasterCard or Maestro account number in a bank identification number (BIN)/ Issuer Identification number (IIN) range assigned by MasterCard. This obligation applies regardless of how or why such PANs were received, processed or stored, including, by way of example and not limitation, in connection with or relating to a credit, debit (signature - or PIN-based) proprietary, or any other kind of payment Transaction, incentive or reward program.
- Within seventy-two (72) hours, engage the services of a PCI Forensic Investigator (PFI) to conduct an independent forensic investigation to assess the cause, scope, magnitude, duration and effects of the ADC Event or Potential ADC Event. The PFI engaged to conduct the investigation must not have provided the last PCI compliance report concerning the system or environment to be examined. Prior to the commencement of such PFI's investigation, the Customer must notify MasterCard of the proposed scope and nature of the investigation and obtain preliminary approval of such proposal by MasterCard or, if such preliminary approval is not obtained, of a modified proposal acceptable to MasterCard.
- Within two (2) business days from the date on which the PFI was engaged, identify to MasterCard the engaged PFI and confirm that such PFI has commenced its investigation. Within three (3) business days from the commencement of the forensic investigation, ensure that the PFI submits to MasterCard a preliminary forensic report detailing all investigative findings to date.

- Within twenty (20) business days from the commencement of the forensic investigation, provide to MasterCard a final forensic report detailing all findings, conclusions and recommendations of the PFI, continue to address any outstanding exposure, and implement all recommendations until the ADC Event or Potential ADC Event is resolved to the satisfaction of MasterCard. In connection with the independent forensic investigation and preparation of the final forensic report, no Customer may engage in or enter into any (or permit an Agent to engage in or enter into) any conduct, agreement or understanding that would impair the completeness, accuracy or objectivity of any aspect of the forensic investigation or final forensic report. The Customer shall not engage in any conduct (or permit an Agent to engage in any conduct) that could or would influence, or undermine the independence of, the PFI or undermine the reliability or integrity of the forensic investigation or final forensic report. By way of example, and not limitation, a Customer must not itself, or permit any of its Agents to, take any action or fail to take any action that would have the effect of:
 1. precluding, prohibiting or inhibiting the PFI from communicating directly with MasterCard;
 2. permitting a Customer or its Agent to substantively edit or otherwise alter the forensic report; or
 3. Directing the PFI to withhold information from MasterCard. Notwithstanding the foregoing, MasterCard may engage a PFI on behalf of the Customer in order to expedite the investigation. The Customer on whose behalf the PFI is so engaged will be responsible for all costs associated with the investigation

3.0 Recommendations / Supplementary Information

3.1 MasterCard Compliance

Finding

During the review it was determined that NetPay Ltd has within the Company Structure dedicated functions responsible for Legal, Risk & Compliance which includes the responsibility for risk and awareness of the MasterCard Rules and Security Rules & Procedures as they relate to the overall Member and Service Provider obligations.

Recommendation

It is recommended that a dedicated MasterCard Acquiring Risk Compliance Checklist is developed. The checklist should incorporate all acquiring risk compliance requirements and the relevant owner of the function should sign off on a quarterly basis that they or their relevant team has completed the tasks required. Consideration should be given to including the recommended 'Checklist' within the NetPay Ltd Risk Management Policy.

The following Requirements should be considered for inclusion in any checklist:

MasterCard Rules Manual

- The Licence and Participation – Chapter 1
 - Area of Use – Chapter 1.7
- Standards & Conduct of Activity & Digital Activity – Chapter 2
- Customer Obligations – Chapter 3
 - Integrity of the Brand & Network – Chapter 3.7
- Acquiring – Chapter 5
 - Merchant Agreement – Chapter 5.1
 - Merchant & Sub merchant Compliance with the Standards – Chapter 5.2
 - Acquirer Obligations to Merchants – Chapter 5.3
 - Merchant Identification & Responsibility for Transactions – Chapter 5.6
 - Merchant Obligations for Acceptance – Chapter 5.10
 - Prohibited Practices – Chapter 5.11
 - Illegal or Brand damaging Transactions – Chapter 5.11.7
- Service Providers (SP's) – Chapter 7
- Europe Region – Chapter 12

MasterCard Transaction Processing Rules Manual

- Authorization and Clearing Requirements – Chapter 2
- Acceptance Procedures – Chapter 3
- Card-Not-Present Transactions – Chapter 5

MasterCard Security Rules & Procedures Manual

- Customer Obligations – Chapter 1
- Fraud Loss Control Standards – Chapter 6
- Merchant Screening & Monitoring Standards – Chapter 7
- MasterCard Fraud Control Programs
 - Global Merchant Audit Program (GMAP) – Chapter 8.2
 - Excessive Chargeback Program (ECP) – Chapter 8.3
 - Questionable Merchant Audit Program (QMAP) – Chapter 8.4

- MasterCard Registration Program (MRP) – Chapter 9
- Account Data Protection Standards & Programs – Chapter 10
- Member Alert to Control High Risk Merchants (MATCH) – Chapter 11
- Global Risk Management Program (GRMP) – Chapter 13

Benefit

Completing these actions will help ensure visibility of all MasterCard acquiring risk compliance programs and drive accountability for the entity performing the tasks required. As businesses expand, the integration and evolution of these programs into an entity's security practices will also help ensure that vital compliance tasks continue to be conducted and that there are no gaps in processes.

Copies of the MasterCard Rules, MasterCard Transaction Processing Rules & MasterCard Security Rules & Procedures Manuals should be made available via their acquiring partner(s) in order to ensure NetPay Ltd meet their obligations under the MasterCard Standards.

Refer to MasterCard Rules section 7.2.4 – Disclosure of Standards (See Section 2.3)

Alternatively the above manuals can be accessed via the below link:

<http://www.mastercard.us/merchants/support/rules.html>

3.2 MasterCard Anti-Money Laundering (AML Requirements)**Finding**

During the review, it was determined that NetPay Ltd has a clear and defined AML.

Requirements

As a global payments network, MasterCard is committed to its role in thwarting the money laundering efforts of terrorists and other criminals. In accordance with Section 352(a) of the USA Patriot Act, MasterCard is required to have an Anti-Money Laundering (AML) compliance program ("Program") in place that is reasonably designed to prevent MasterCard systems from being used to facilitate money laundering or support the financing of terrorist activities. As a global organization, MasterCard has designed its Program to mitigate such risks regardless of geographic location.

The MasterCard Standards require that each applicant or customer provide affirmative evidence of compliance with the Program and each customer must, at all times, maintain compliance with the Program Requirements. Each applicant and customer must cooperate with any effort to evaluate compliance with the Program and MasterCard has exclusive authority to determine whether an applicant or customer is in compliance.

MasterCard will conduct an AML review ("Review") of each applicant when participation in the network is requested and further evaluate each customer as part of ongoing monitoring to confirm that the AML program Requirements are met.

The applicant/customer's program must be designed to protect the MasterCard network and at a minimum, must include the following:

- Thorough client identification
- Thorough client due diligence
- Record-keeping of such identification and due diligence
- Appropriate limitations on anonymous activities
- Client activity monitoring to detect suspicious activity

- Steps to be taken when suspicious activity is detected
- An audit process to test controls
- All cardholders, merchants and/or affiliates are checked against the Specially Designated Nationals and Blocked Persons List (the “SDN List”), issued by the U.S. Treasury’s Office of Foreign Assets Control (OFAC),
- At the time the relationship is established and on an ongoing basis and any activity with an individual or entity found to be on the SDN List is immediately terminated; additionally, no activity is conducted in an OFAC sanctioned country.
- OFAC regulations restrict financial transactions in certain countries and with persons and entities included on the OFAC SDN List. All customers, regardless of jurisdiction or places of business, must be in compliance with OFAC regulations at all times.

Furthermore, applicants and customers are required to be in compliance with applicable local laws and regulations at all times.

During a Review or at any other time, MasterCard may determine that further information is necessary to confirm that a customer does not pose a risk to MasterCard when failing to comply with the Standards. This evaluation may include a request for detailed information about one or more of the following: the customer, its activities, its AML procedures and controls, or the identity of its owners, directors, and senior executives. The MasterCard Standards require that each customer fully comply with such request for information and that failure to do so could result in noncompliance assessments or termination of the MasterCard license, or both. If MasterCard identifies a concern during a Review, MasterCard will conduct further due diligence to investigate its findings and provide a recommendation for the Anti-Money Laundering and Trade Sanctions Officer on the action plan to pursue.

Noncompliance

Customers failing to comply with any requirements under the Program or to respond to any request for information may be subject to a noncompliance assessment of up to USD 25,000 (BRL 50,895) at the discretion of MasterCard. MasterCard may implement a full or partial suspension of a customer’s MasterCard activities in instances where MasterCard deems the customer’s noncompliance with the Program to pose significant risk to MasterCard or cause damage to the MasterCard system, its customers or any other stakeholder. In the event of a suspension, no authorization processing may take place after the measure is implemented; clearing and settlement may remain in effect for a limited time to complete processing of transactions authorized before the suspension. MasterCard reserves the right to terminate a Customer for violation of Standards or failure to address concerns identified by MasterCard.

Benefit

Card programs must be operated at all times in full compliance with all applicable laws and local regulations. Ensuring compliance with AML standards protects the NETPAY LTD value chain partners from reputational risk, and limits potential disputes and legal action.

3.3 MasterCard Connect for Service Providers

Finding

During the review, it was determined that the NetPay Ltd does not currently have access to MasterCard Connect via its Acquiring relationship with Acquirer Name and therefore is not fully benefiting from all of the available functions and guidance for Acquirers and Service Provider’s.

MasterCard announced revised Standards for the Payment Facilitator and Service Provider programs within the **Global Operations Bulletin No 10, 1st October 2014**

The following rules changes are effective immediately, as outlined in the revised Standards:

- A Payment Facilitator will be classified as a type of Service Provider, rather than as a Merchant (but will continue to be able to perform all of its existing services, such as paying Sub-merchants for transactions).

Recommendation

A new business function, **Request Access from Company**, is now available to assist Service Providers with requesting or modifying access to MasterCard Connect applications and services.

This function allows a service provider to initiate a request for access to their Principal Customer for approval.

Service providers can access this function through the **Manage My Company** application in MasterCard Connect.

Benefits of New Function

The benefits of using the new function include the following:

- Helps streamline the process for service provider provisioning. The Service Provider can use the automated access request instead of sending the request through email.
- The request goes automatically to the correct Business Administrator for the Principal Customer.
- Helps to eliminate confusion between the service provider and the Principal Customer.
- Provides an audit trail for both the service provider and the Principal Customer.

Using the New Request Access from Company Function

The high-level process for the new function is as follows:

1. The service provider uses the Request Access from Company function to submit the provisioning request. The Business Administrator for the Principal Customer is notified through email that a request is awaiting action.
2. The Business Administrator approves (or declines) the request. The Business Administrator can modify the items in the request, if needed. The requestor at the service provider is notified through email about the status of the request.
3. If the request is approved, the service provider's users can see the provisioned applications and services in the MasterCard Connect Store approximately 15 minutes after the approval.

When the applications and services are available in the MasterCard Connect Store for the service provider's users to order, the order and approval process continues as it is today.

Service Provider Access

To access the new Request Access from Company function:

1. Go to www.mastercardconnect.com.
2. Enter your User ID and Password.
3. Under Applications, select Manage My Company.
4. Under Manage My Company, click Request Access from Company.

Business Administrator Request Management

To manage a request for access:

1. Go to www.mastercardconnect.com.

2. Enter your **User ID** and **Password**.
3. Under **Applications**, select **Manage My Company**.
4. Click the **Organizational Work** tab.
5. Manage the requests that begin with "SPI."

NetPay Ltd should approach its Principle Acquiring Partner to gain appropriate access to MasterCard Connect and the benefits it can provide the whole NetPay Ltd organisation.

There are no restrictions to using MasterCard Connect; however there are protections and security that were implemented with Connect to protect the data and organizations.

Training courses for MasterCard Connect can also be found via: www.mastercard.com/arm

Benefit

Access to MasterCard Connect provides both Acquirers and Service Providers alike access to **MasterCard Key Operational Documents (See 3.4)** and **MasterCard Best Practices (See 3.5)** which will further enhance NetPay Ltd' risk mitigation strategies.

3.4 MasterCard Key Operational Documents

Finding

During the review, it was determined that NetPay Ltd does not currently have access to MasterCard Connect and therefore is fully benefiting from all of the available functions and guidance for Acquirers and Service Provider's

Refer To Section 3.3 MasterCard Connect for Service Providers

Recommendation

It is recommended that NetPay Ltd having access to MasterCard Connect regularly review all of the below mentioned MasterCard Bulletins and Manuals utilizing the relevant information to educate and train your staff and value chain partners.

- Access the MasterCard Connect Library and review and distribute on a monthly basis the relevant MasterCard Bulletins that apply to their business unit.
- Access MasterCard Connect Library and regularly review and distribute the relevant MasterCard Manuals that apply to their business unit. At a minimum this should include the Security Rules and Procedures, Account Data Compromise User Guide, Quick Reference Booklet, MasterCard Registration Program and MasterCard Rules.

It is recommended that NetPay Ltd at a minimum, review the MasterCard Rules and Security Rules and Procedures manuals, available within the MasterCard public website at <http://www.mastercard.us/merchants/support/rules.html> to understand their obligations as a Service Provider on the MasterCard system.

As a Service Provider, NetPay Ltd should in accordance with MasterCard Rules 7.2.4 to be provided with the MasterCard Standards applicable to the Program Service(s) they are expected to perform.

NetPay Ltd should consult with their Acquiring Partner(s) to obtain copies of the MasterCard Standards that pertain to the program services that NetPay Ltd provides.

MasterCard Rules section 7.2.4 states

Disclosure of Standards

Before a Customer proposes an entity to be registered as a Service Provider by the Corporation, the Customer must provide, or ensure the proposed Service Provider has access to the Standards then in effect applicable to Service Providers and the Program Service the proposed Service Provider is expected to perform. After registration, the Customer must provide, or ensure a Service Provider is notified of, any change to the Standards applicable to such Program Service.

Benefit

By reviewing and distributing the above referenced bulletins and manuals will drive constant improvement of NetPay Ltd knowledge and compliance with MasterCard's standards.

3.5 MasterCard Best Practice for Service Providers

Finding

During the review, it was determined that NetPay Ltd does not have access to MasterCard Connect as a Service Provider and therefore is not fully benefiting from all of the available functions and guidance for Acquirers and Service Provider's

Refer To Section 3.3 MasterCard Connect for Service Providers

Recommendation

It is recommended that NetPay Ltd having access to MasterCard Connect inform its customers, staff, and value chain partners about MasterCard's best practices guides, PCI 360 Education Program, SecureCode 360 Webinar series, and Academy of Risk Management (ARM) training courses and conferences:

- The MasterCard ARM website (www.mastercard.com/arm) includes information about ARM conferences and training courses. It also includes PCI 360 and SecureCode 360, which are complimentary programs to raise awareness and promote the adoption of Payment Card Industry Data Security Standard (PCI DSS) Requirements and MasterCard SecureCode through holistic webinars, best practices, and white papers.
- The MasterCard Alerts™ Reading Room contains all of the MasterCard Global Security & Risk Services Best Practices Guides.

Next year's MasterCard Global Risk leadership Conference (Europe) is to be held in between the 26th & 29th September 2016 in Split, Croatia. Further information can be found at:

<https://www.etches.com/ehome/44527>

How to Access the "Best Practices" Guides:

Follow these instructions to access the entire "Best Practices" series of guides:

1. Go to www.mastercardconnect.com.
2. Log on by entering your User ID and Password.
3. From the Applications menu, select MasterCard Alerts.
4. Advance to the References page.
5. From the References menu on the left, click Security & Risk Reading Rooms.
6. Click the appropriate link for your region.
7. Click MasterCard Global Security & Risk Services Best Practices Guides.
8. Click the link of the guide that you want to view in portable document format (PDF).

Benefit

MasterCard's best practices guides, PCI 360 program, SecureCode 360 series, and ARM training courses and conferences provide fraud solutions, training, and knowledge from a variety of industry experts that NetPay Ltd can utilize to educate and train its staff and value chain partners.

It is recommended that NetPay Ltd also regularly reviews all publicly available online resources such as www.mastercardmerchant.com to obtain information about MasterCard Rules, Requirements and trainings.

3.6 MasterCard Training for Service Providers

Finding

During the review it was established that NetPay Ltd provides a training program for all members of staff with regards to AML and associated risk.

During the review MasterCard introduced the new MasterCard Compliance Training Program which is available to all NetPay Ltd employees to assist in enhancing their individual knowledge of MasterCard's Rules and Compliance Programs.

Recommendation

MasterCard recommends that all resources engaged in Risk Management related functions should attend MasterCard Training sessions related to authorization, chargeback, fraud, chip workshop and e-commerce.

The MasterCard Academy of Risk Management has created specific courses to assist with such training: <https://www.etches.com/ehome/57089/103369/>

A selection of the courses available is listed below:

- Fraud Management for Acquirers
- MasterCard Connect Advanced
- Dynamics of Merchant Acquiring
- Advanced Acquiring Workshop
- Introduction to Chargebacks
- MasterCard Chargebacks Seminar
- MasterCard Advanced Chargebacks Seminar
- Merchant Acceptance Seminar
- Fraud Management for Acquirers
- Acquiring with MasterCard
- e-Commerce and Your business

MasterCard highly recommends that the NetPay Ltd implements a training plan to include external trainings as per the above courses to help ensure that NetPay Ltd staff will maintain their knowledge of known and potential fraud risks.

Please contact the MasterCard Academy on academy@mastercard.com for more information.

MasterCard Academy on the Web

MasterCard Academy's mission is to provide appropriate training solutions for our customers that are both scalable and cost effective.

Our three main knowledge-sharing services give you access to a wealth of learning materials:

- Live Events
- E-Learning Suite
- Resource Center

To register for our Live Events, access our E-Learning Suite, Resources Center, or both to complete the registration and ensure your company has an Academy on the Web (AOW) license. Contact the training contact in your company to access AOW. Please note that some topics (such as MasterCard In Control™, Operations Bulletin Review, or Licensing) are available only via our Live Events on AOW. In addition, thanks to your AOW license, you will benefit from a 50 percent discount on the following open seminars: Introduction to MasterCard, Interchange Economics with MasterCard, Prepaid New Customer Onboarding, and e-Commerce & Your Business.

To register for these seminars and to receive your discount code, send an email message to: academy@mastercard.com.

For additional information about Academy on the Web, visit www.mastercardacademy.com

Compliance Program Training

In December 2013 MasterCard announced the launch of its [our e-Learning Website](#)

Many customers often have questions with regards to MasterCard's rules, compliance programs and processes and in response to this MasterCard have created this site as a self-serve educational platform which consists of several user-friendly e-learning modules.

Through this site our customers can learn how our Franchise programs will help them improve their operational effectiveness and grow their business while protecting the integrity of MasterCard's brand and network. MasterCard will also look to expand this site in the future, providing additional best practices and educational materials designed to address the dynamic risks our stakeholders face.

For those customers interacting with merchants, sharing our [Tips for Merchants Page](#) may prove useful for managing chargebacks and selecting a Merchant Service.

3.7 Merchant Education

Finding

NetPay Ltd provides both support and educational materials to their Sub-merchants via the following channels:

- Sub-merchant Help Desk
- Education page on the Website

Recommendations

MasterCard acknowledges that NetPay Ltd has implemented educational information to mitigate risk via their Sub-merchant Helpdesk which provides general guidance in relation to card acceptance 'best practices' to help mitigate financial loss from fraud and chargeback's.

In addition MasterCard would recommend that NetPay Ltd considers the implementation of a 'Merchant Education' page within the general NetPay Ltd website which would further enhance the existing education provided both to Merchants, Partners and Sub-merchants.

MasterCard provides access to Risk Management Training via the following links:

<http://www.mastercard.com/us/merchant/support/demos.html>.

<https://www.mastercard.us/en-us/merchants/safety-security.html>

It is recommended that NetPay Ltd utilises this MasterCard training resources to provide online training for its Sub-merchants which would be a cost effective method to ensure merchants are properly trained with regards to 'risk management'.

Acquirer Responsibilities – Merchant Screening and Monitoring Standards. Chapter 7 MasterCard Security Rules & Procedures (Refers to Payment Facilitator Obligations)

7.2 Ongoing Monitoring

An Acquirer must monitor and confirm regularly that the Transaction activity of each of its Merchants (sales, credits, and chargebacks) is conducted in a legal and ethical manner and in full compliance with the Standards, and ensure that a Payment Facilitator conducts such monitoring with respect to each of its Sub merchants, in an effort to deter fraud. Monitoring must focus on changes in activity over time, activity inconsistent with the Merchant's or Sub merchant's business, or exceptional activity relating to the number of Transactions and Transaction amounts outside the normal fluctuation related to seasonal sales. Specifically for MasterCard POS Transaction processing, ongoing monitoring includes, but is not limited to, the Acquirer fraud loss controls relating to deposit (including credits) and authorization activity described in section 6.2.2.

With respect to an e-commerce Merchant, the Acquirer regularly, as reasonably appropriate in light of all circumstances, must review and monitor the Merchant's website(s) and business activities to confirm and to reconfirm regularly that any activity related to or using a Mark is conducted in a legal and ethical manner and in full compliance with the Standards. The Acquirer must ensure that a Payment Facilitator conducts such monitoring with respect to each of its Sub merchant's website(s).

As a best practice, MasterCard recommends that Acquirers use a website monitoring solution to review their e-commerce Merchants' and Sub merchants' activity to avoid processing illegal or brand-damaging Transactions.

7.3 Merchant Education

Once an acquiring relationship is established, an Acquirer must institute a fraud prevention program, including an education process consisting of periodic visits to Merchants, distribution of related educational literature, and participation in Merchant seminars. Instructions to Merchants must include Card acceptance procedures, use of the Electronic Warning Bulletin file or Warning Notice, authorization procedures including Code 10 procedures, proper completion of Transaction information documents (TIDs) (including primary account number [PAN] truncation), timely presentment of the Transaction to the Acquirer, and proper handling pursuant to Card capture requests. Customers must thoroughly review with Merchants the Standards against the presentment of fraudulent Transactions. In addition, Customers must review the data security procedures to ensure that only appropriate Card data is stored, magnetic stripe data never is stored, and any storage of data is done in accordance with the Standards for encryption, Transaction processing, and other prescribed practices.

An Acquirer must also ensure that a Payment Facilitator conducts appropriate education activities for each of its Sub merchants.

Benefit

NetPay Ltd by implementing a comprehensive merchant education program will raise the awareness of fraud and chargeback risk across the merchant portfolio which will allow merchants to proactively manage their risk to reduce their overall financial expose and minimize loss. By providing an education program to merchants NetPay Ltd will also further enhance its relationship with its merchant portfolio.

Also by following the MasterCard requirements in relation to 'Merchant Screening & Monitoring' NetPay Ltd will remain compliant with MasterCard's Standards.

3.8 Fraud Reporting

Finding

MasterCard ascertained that NetPay Ltd Senior Management were in receipt of a monthly reports provided by their Risk Team which includes, transaction volumes and chargeback's per Sub-merchant.

Weekly and daily calls with the Senior Management also provide the opportunity for the Risk Team to highlight current issues in respect of non-performing merchants, increases in transactional volumes and chargeback's.

The current risk related reporting within NetPay Ltd is focused on 'Chargeback's' and it is not evident that NetPay Ltd has data in respect of confirmed fraud processed through their Sub-merchant portfolio.

During the review NetPay Ltd were unable to confirm whether their Acquirer, ICC CAL provided reporting in respect of confirmed Fraud via SAFE and / or Fraud Reporter.

MasterCard accepts that in the case of NetPay Ltd that the levels of reported fraud via SAFE in respect of Sub-merchants within the portfolio are minimal and the levels of reporting as recommended may appear both excessive and inappropriate at this point in time. But as the Sub-merchant portfolio grows and the incidents of reported fraud increase then NetPay Ltd may wish to develop additional reporting based on the MasterCard reporting criteria.

Recommendation

MasterCard recommends that Acquirers and Service Providers develop their suite of Fraud Management Reports to provide clear oversight to the business of the fraud performance across the portfolio.

The key to improving the fraud reporting is communicating and understanding what each stakeholder requires and then targeting those specific needs.

Industry best practice fraud reporting teams create separate reports for each specific audience depending on their Requirements. Consider the following fraud reporting framework and metrics for each level of management.

Fraud Management Reports should include the reporting of Fraud Basis Points (BP's) for the NetPay Ltd Acquiring Merchant Portfolio which will provide a clear oversight of their fraud performance when benchmarking against published MasterCard Fraud Basis Points for specific Countries and Regions.

It is recommended that NetPay Ltd mirror the reports provided by MasterCard which provide a customer with a breakdown of their fraud performance by the following criteria:

- Acquirer Basis Points (All)
- Acquirer Domestic Basis Points
- Acquirer Cross-Border Basis Points

- Acquirer Cross-Border Intra-Regional Basis Points
- Acquirer Cross-Border Inter-Regional Basis Points

MasterCard calculates Fraud BP using the following calculation

- **$\text{Fraud BPS} = \text{Fraud USD} \div \text{Gross Acquirer Volume (GAV) USD} \times 10,000$**

MasterCard used fraud data reported by Issuers into 'System to avoid Fraud Effectively (SAFE) and is defined as follows:

MasterCard requires issuers to report to SAFE at the customer ID level all MasterCard transactions that the issuer considers to be fraudulent, even if the corresponding accounts are not closed or not in status of fraud. This includes transactions with fraud-related chargebacks, fraudulent On-Us transactions, and transactions where dollar losses were recovered by restitution or by any other means.

MasterCard also recommends that NetPay Ltd develop similar reporting criteria for individual Merchants and Merchant Sectors (MCC's) within their merchant portfolio to further enhance their monitoring capabilities and to identify merchants and sectors with a growing fraud trends in order to take mitigating action at the earliest opportunity.

Industry best practice for fraud reporting includes the creation of separate reports for specific audiences depending on their Requirements. Consider the following fraud reporting framework and metrics for each level of management.

Reporting Levels

- Executive Dashboard
- Senior Management Dashboard
- Fraud Management Departmental Reporting

Executive Dashboard (Suggested)

Consider presenting this data by payment channel:

- Gross Fraud Amount and Basis Points
- Net Fraud Amount and Basis Points
- Net Fraud Write Off

Senior Management Dashboard (Suggested)

Consider presenting this data by payment channel and fraud type:

- Fraud Type Gross Fraud Amount and Basis Points
- Fraud Type Net Fraud Amount and Basis Points
- Gross and Net Fraud Plan and Forecast

- Variance of Actuals to Plan and Forecast
- Fraud Type Net Fraud Write Off
- Fraud Type Chargeback and Recovery Performance
- Fraud Detection Resource Management (false/positives)
- Fraud Detection Loss Management (point of detection)
- Fraud Detection System Management (Detection Rate)
- Marginal Rate of Benefit Analysis

Fraud Management Departmental Reporting (Suggested)

Consider presenting this data by payment channel, fraud type and detection rule:

- Fraud Type Gross Fraud Amount and Basis Points
- Fraud Type Net Fraud Amount and Basis Points
- Gross and Net Fraud Plan and Forecast
- Variance of Actuals to Plan and Forecast
- Fraud Type Net Fraud Write Off
- Fraud Type Chargeback and Recovery Performance
- Fraud False/Positives for each fraud rule
- Fraud Point of Detection for each rule
- Fraud Detection Rate
- Fraud Risk Prioritization for each rule
- Fraud Detection Analyst Performance (False/Negatives)
- Marginal Rate of Benefit Analysis

Benefit

Analytics and reporting provide definitive answers to many questions with regards to the fraud mitigation challenge allowing organizations to make data-driven business decisions. By effectively reporting gross and net fraud losses by fraud type will ensure timely detection of fraud trends and understanding of emerging financial risks that cause net fraud losses. If the fraud reports don't directly target the specific audience Requirements this may reduce the effectiveness and visibility of fraud and loss of productive time for the relevant parties.

3.9 MasterCard Fraud Management Solutions

Finding

During the review it was identified that NetPay Ltd had a clear road map to provide their merchant portfolio with industry leading tools to mitigate both fraud and compliance risk.

At the same time NetPay Ltd expressed its interest to extend their staff knowledge about MasterCard Merchant Security Solutions.

MasterCard acknowledges the importance of security for our customers, merchants and cardholders and is constantly monitoring the evolution of fraud trends, both at a global and market level. A key observation is that fraud has become a global and sophisticated business and it continuously shifts and mutates, so it requires an intelligent and multi-faceted response.

The MasterCard response is to further secure the digital channel with enhanced authentication, enhance the network by providing customers with a toolset for transaction monitoring and establishing programs connecting issuers to merchants and vice versa.

For e-commerce transactions SecureCode is the key infrastructure component to enable strong authentication of transactions. MasterCard is taking further action to ensure accelerated deployment and increase the utility of MasterCard products with SecureCode merchants.

Currently MasterCard provides the following solutions to Acquirers, Service Providers and Merchants.

Information with regards to the BIN Table Resource was provided to NetPay Ltd post the Review meeting.

- **MasterCard Gateway Services** – Our fraud & risk management solution, GateKeeper: 2.0, is split into a range of structured fraud & risk management solutions that can be employed in-house or can be fully outsourced. These are:
 - Tailored to industry specific needs
 - Fit precisely within any business model
 - Requires a single integration
 - Enable all transactions to be fully screened and analyzed for links regardless of payment type, currency, channel or geographic market they originate from

GateKeeper: 2.0 provides end-to-end fraud monitoring, detection and prevention. Using a multi-dimensional approach it tackles fraud & risk from every angle by layering security strategies and technologies that balance protection and profitability at every stage of the payment lifecycle during:

- Account Registration to screen and evaluate consumer account registration risk
 - Payment Authentication to analyze and define security strategies to verify genuine customers
 - Transaction Processing to identify, detect and review high-risk transactions based on unique risk profiles
 - Dispute and Recovery to manage and resolve chargeback disputes to recover losses
 - Evaluation and Refinement to analyze and refine fraud performance against trends
- **SecureCode** – MasterCard are actively working with industry leaders to drive the migration of online authentication standards away from weak, single factor provisioning towards stronger multi-factor provisioning
Refer to Section 3.10 – SecureCode Strategy
 - **Lost Stolen Account Listing** - The API integrates easily into existing operations, enabling access to MasterCard accounts that have been reported as lost or stolen by Issuers globally. Checking the list provides an additional data point for fraud risk scoring and allows the periodic validation of payment accounts already stored on websites such as stored cardholder payment information and to reference after authorization but prior to shipping goods

- **Expert Monitoring Fraud Scoring for Merchants** – MasterCard provide highly predictive real time behaviour based fraud scoring that merchants can receive during authorization or access easily and cost effectively through our Developer Zone API

Fraud Scoring for Merchants provides ecommerce merchants with a predictive behaviour based score in real time during authorization for CNP transactions derived from a comprehensive view of cardholder account transaction history and a regional CNP fraud detection model

The Fraud Scoring for Merchants API enables merchants or Fraud Solution Providers to obtain the merchant fraud score through an alternative channel that doesn't require code changes to the authorization message.

Originally the EMS scoring model was for US Issued accounts only but it has been recently announced that MasterCard has expand this product to other Markets including the United Kingdom and Germany commencing in Q1 2015.

- **Assurance IQ** - Capture and link additional data fields to create a mechanism for merchant and issuer to share and use intelligence in real-time
- **Automated Billing Updater (ABU)** - Enables issuers to communicate account number changes and/or expiration date updates to acquirers to provide to their participating merchants to reduce CNP transaction declines.
- **BIN Table Resource** - The MasterCard sanctioned bin table will be made available to large merchants and Service Providers. Using the Bin table in the transaction verification process should result in:
 - Improved on-line card acceptance through more insight in the product type and origin leading to superior customer experience when shopping at the merchants webshop
 - Improved KYC leading to a reduction of overall cost related to fraud such as fraud & chargeback losses, handling costs, management program costs.

A more comprehensive insight to MasterCard's Merchant Security Solutions can be provided upon request and a separate meeting can be arranged to introduce NetPay Ltd to members of MasterCard's Enterprise Security Solution (ESS) Team.

3.10 SecureCode Strategy

SecureCode is an e-commerce gateway that enables merchants to process and authenticate credit & debit card transactions shifting the liability for a majority of the transactions from the acquirer to the issuer.

Finding

During the review, it was determined that NetPay Ltd had a clear understanding of the SecureCode product and the benefits it affords to merchants.

Currently NetPay Ltd has adopted a 'risk based' approach for Sub-merchant adoption of SecureCode.

Recommendation

MasterCard strongly recommends that NetPay Ltd seeks to establish an Ecommerce Strategy to drive all merchants towards a unique transaction environment and this can be supported by implementing MasterCard SecureCode

In terms of training the MasterCard 360 is a complimentary series of training provided by webinar which is intended to provide Issuers, Acquirers and Merchants interactive and informative guidance on SecureCode adoption, the benefits of deployment, best practice, Issuer authentication options, fraud reduction opportunities and industry trends

For access to the MasterCard SecureCode 360 Training, please use the below links

<http://www.eisewhere.com/ehome/8231/18271/?&>

As consumers around the globe adopt online shopping and other card not present (CNP) channels, fraud has infiltrated the CNP space resulting in increased chargeback's, expenses and other losses impacting Acquirers and Merchants. The card industry globally is under greater financial and regulatory pressure to introduce increased transaction security and reduce fraud

Since the 1st November 2006, MasterCard has implemented a global merchant-only MasterCard SecureCode liability shift and this liability shift covers all qualifying interregional electronic commerce transactions with the exception of MasterCard commercial card transactions, which have been excluded since 1 February 2007.

In the Global Operations Bulletin No 7, 15 July 2013 MasterCard set out revised standards to include Commercial Card Programs in the global merchant only MasterCard SecureCode liability shift.

All interregional commercial card e-commerce transactions, regardless of the country or region in which the commercial card was issued, will be included. The commercial card exclusions for U.S. region domestic and Canada region domestic e-commerce transactions from the merchant-only MasterCard SecureCode liability shifts in place within those regions will be retained.

With respect to authorizations that occur on or after the 11th April 2014, qualifying commercial card transactions will now be included in the global interregional merchant-only liability shift. In the case of an interregional e-commerce transaction between customers located in different regions, liability shifts from the acquirer to the issuer for a message reason code 4837 (No Cardholder Authorization) or 4863 (Cardholder Does Not Recognize—Potential Fraud) chargeback when:

- The merchant is Universal Cardholder Authentication Field (UCAFT™)-enabled.
- All other e-commerce Authorization Request/0100 message Requirements were satisfied.
- The Authorization Request Response/0110 message reflected the issuer's approval of the transaction.

Benefit

By promoting the use of SecureCode, NetPay Ltd will have the ability to profitably service both the credit and debit card acceptance needs of your current and future merchants and open new opportunities globally across all MasterCard products.

The key benefits from a merchant perspective:

- Reduce chargeback's and associated losses
 - **Reason Code 37** (No Cardholder Authorization)

- **Reason Code 63** (Cardholder Doesn't Recognize)
 - **Reason Code 49** (Questionable Merchant Activity)
- Reduce processing expenses
- Maintain the merchants highly effective checkout experience
- Increase sales volume by improving consumer confidence
- Increase sales volume due to improved issuer approval rates through international sales

3.11 Mitigating Fraudulent Authorization Reversals

Finding

During the review it was identified that NetPay Ltd has established rules within their existing monitoring systems to monitor for and alert unusual numbers of 'credit / refund transactions.

Refer to Section 2.2 Fraud Loss Control Program & Minimum Monitoring Requirements

NetPay Ltd are advised based on current 'risk trends' to further review their monitoring capabilities to ensure to both detect and alert 'Fraudulent Authorization Reversal' type attacks at the earliest opportunity in order to mitigate associated risks.

The following recommendations were issued by MasterCard to members within the **Global Security Notice No 3, 27th August 2014**.

Recommendation

MasterCard has recently become aware of an account takeover scheme targeting merchants in which criminals present fraudulent authorization reversals to cross-border issued payment accounts which potentially increases the account's Open-to-Buy balance.

Using these accounts, the criminals subsequently attempt fraudulent ATM transactions. Based on MasterCard observations, it appears that the primary account numbers (PANs) receiving the fraudulent reversals do not have an "offsetting" purchase transaction at the same merchant.

To help mitigate these attacks, MasterCard encourages acquirers and their processors to integrate preventative measures into their fraud and risk monitoring controls, as well as to educate their merchants on the various forms of phishing scams and malware that criminals use.

Overview of Fraudulent Authorization Reversal Attack Vector

This fraud scheme typically begins with the criminal taking control of a valid merchant account through phishing of the merchant credentials. Once the fraudster has successfully gained access to the merchant's account, the criminal targets the merchant's terminal to facilitate the attack. The fraudster then processes fraudulent reversals to PANs for payment cards in the fraudster's possession that have had not been previously used in purchase transactions at that merchant. Within the Reversal Request/0400 message, the criminal uses the merchant's valid merchant identification (MID) number, but alters the merchant's name in an attempt to hide this fraudulent activity. If the issuer accepts the reversal, the funds become available on the fraudster's card accounts, thereby increasing the Open-to-Buy balance for these accounts. MasterCard has observed fraudulent ATM activity on some of these accounts shortly after the processing of the reversals.

Defending Against Fraudulent Authorization Reversal Attempts

Acquirers and processors should establish risk mitigation controls for this fraud scheme. These controls should include measures similar to those employed against fraudulent credits, including the suspension and review of:

- Reversals for which there is no preceding linked authorization request at the targeted merchant location within a specified period of time
- Reversals that are larger than the initial authorization amount at the merchant location
- Multiple reversals for the same cardholder account
- Multiple reversals for multiple cardholder accounts
- Reversals for which the merchant name in the authorization record differs from the valid merchant name
- Reversals for which the card acceptor business code (MCC) differs from that of the valid merchant's MCC
- Reversals for which the Internet Protocol (IP) address differs from that of the valid merchant

If an acquirer or processor suspects that it has processed a fraudulent reversal, they should contact the issuer immediately to attempt to avoid potential loss.

Defending Against Phishing Attempts

To deter a criminal from obtaining the necessary access privileges to initiate an attack against a merchant's network, the acquirer and its merchants should follow anti-phishing best practices:

- Use caution when providing sensitive information, such as user IDs and passwords.
- Do not provide sensitive information to anyone, unless certain of the credentials of the potential recipient of the information.

Guard terminal information.

Do not disclose the MID number, terminal ID number, or acquirer's bank identification number (BIN). Payment brands (such as MasterCard), acquirers, and processors already have this information and would not request it. Therefore, if the merchant receives a call requesting this information, it is likely a phishing attempt by a criminal to gain terminal access. Instead, the merchant should call its acquirer or processor, ask to be transferred to the appropriate person or department that handles the merchant's account, and report the call.

- Avoid clicking on hyperlinks within email communications. Type the URL into the web browser instead.
- Do not download suspicious attachments.
- Instruct employees not to use business computers and workstations for non-business activities, such as web browsing or checking personal email messages.
- When reviewing or responding to emails, verify that the sender's information is correct. Be vigilant for slight misspellings, which may indicate a phishing attempt.
- If the merchant receives a phone call, email, or repair technician visit that is suspicious, the merchant should not respond or provide any information. The merchant should immediately contact its acquirer or processor to verify the legitimacy of the request.

Beware of any unscheduled terminal repair technician arriving at a merchant location requesting access to the point-of-sale (POS) terminal. The technician may be a criminal attempting to gain access. If a repair technician arrives unannounced, the merchant should contact its acquirer or processor to verify the technician's identity using the merchant's own contact information on file, not the contact information provided by the technician.

- Educate staff regarding anti-phishing strategies, such as only opening email messages from a known or trusted source.
- Limit employee access to the MID number, terminal ID, or the acquirer's BIN to help prevent unintentional leaking of this information to a criminal.

Benefit

The early detection of Fraudulent Authorization Reversals will enable NetPay Ltd to be extremely well placed to prevent fraud from entering the MasterCard payment system and protect against fraud loss.

3.12 Chargeback Management Best Practices

Finding

During the review, it was determined that NetPay Ltd has dedicated resource to manage chargeback's for their respective Sub-merchants.

MasterCard would also recommend to NetPay Ltd to consider as appropriate to their business needs further specialist consultative services that are provided by MasterCard under the remit of the Global Risk Management Program (GRMP), details are as follows.

GRMP Fraud Recovery/Chargeback Review Process

MasterCard conducts a comprehensive analysis of the customer's fraud recovery and chargeback performance benchmarked against country and regional peers. A two-day onsite review is conducted by MasterCard staff in collaboration with the customer and involves employee meetings and a walkthrough of the customer's procedures and daily activities. Upon completion of the onsite review, key findings are shared prior to the formal submission of the report within the month. The report contains key findings, recommendations, and a project plan to track the implementation of recommendations.

Fraud Recovery/Chargeback Review Topics

- Fraud dispute customer claim initiation by channel and process
- Cardholder recognition methodologies, including the "talk off" process and merchant identifier options
- Management of cardholder expectations in the fraud dispute experience
- Customer follow-up strategies and communication flows
- Maximization of fraud recoveries, including non-cardholder initiated chargebacks
- Fraud recovery operational efficiencies
- Fraud chargeback, recovery financial reimbursement, and reconciliation processes before and after chargeback, second presentment, and arbitration, including pending funds
- Fraud chargeback case management processes and workflows
- Fraud chargeback reason code decisioning
- System to Avoid Fraud Effectively (SAFE) reporting activities and validation for fraud chargebacks
- Fraud chargeback documentation/declaration management and process flows, including MasterCom
- Fraud chargeback recovery processing technology and workflow strategies
- Fraud chargeback recovery third party processor activities

- Capture and leveraging of fraud chargeback management information data and reporting
- Fraud chargeback change management processes
- Fraud chargeback education

Further information with regards to this additional GRMP Review can be provided upon request.

Recommendation

It is recommended that NetPay Ltd monitors its merchant portfolio against the MasterCard ECP, which has been designed to encourage each acquirer to closely monitor, on an on-going basis, its chargeback performance at the merchant level and to determine promptly when a merchant has exceeded, or is likely to exceed, monthly chargeback thresholds.

NetPay Ltd should also determine a clear policy that would define conditions based typically around a combination of the following parameters, to decide on specific actions to be taken for each individual case:

- Such as CB level for pre-alert
- Merchant revenue
- Merchant collateral
- Merchant category code
- Merchant education needs

Actions to take in each case would be among the following possibilities (or a combination of):

- Terminate the merchant
- Keep the merchant opened but require the merchant to implement specific fraud controls and tools.
- Keep the merchant agreement open but require the merchant to become SecureCode enabled
- Keep the merchant agreement open but implement additional fraud detection rules with real time decline capability of suspected fraudulent transactions.
- Keep the merchant open, address all the needs above and execute a merchant chargeback avoidance education program.

End of report.