emerchantpay

Manual

Basics

Contents

II. Abbreviations

ACH	Automated Clearing House
AML/CTF	Anti-Money Laundering and Counter-Terrorist Financing
APM	Alternative Payment Method
CVM	Card Verification Method
CVV	Card Verification Value
ECP	eComprocessing
emp	emerchantpay
EZC	eZeeCard
EZW	eZeeWallet
EMV	Europay, Mastercard and Visa
EU	European Union
FIU	Financial Intelligence Unit
FX	Foreign Exchange
GPT	Gambling Payment Transaction
HR	Human Resources
IPSP	Intermediary Payment Services Provider
ISO	Independent Sales Organisation
KYC	Know Your Customer
LC	Legal and Compliance
MCSC	Mastercard SecureCode
MID	Merchant Identifier
MLRO	Money Laundering Reporting Officer
MOTO	Mail Order Telephone Order
mPOS	mobile Point of Sale
MSP	Merchant Services Provider
NFC	Near-Field Communication
OCT	Original Credit Transaction
PCI-DSS	Payment Card Industry Data Security Standard
PD	Product Development
PF	Payment Facilitator
PIN	Personal Identification Number
POS	Point of Sale
PSD	Payment Services Directive

III. General

Who we are

emerchantpay ltd., based in the United Kingdom (part of emerchantpay group ltd.), is an authorised electronic money institution regulated by the Financial Conduct Authority of the United Kingdom. Our primary focus is on payment transaction processing with payment cards and other alternative payment methods. That is why our company is a member of the Visa and Mastercard card schemes. The company is divided into two business units:

- Acquiring Bank – responsible for the accepting (acquiring) of payment transactions on behalf of our customers (Merchants) and the direct connectivity with the Visa and Mastercard interchange systems (emerchantpay ltd. is using the trading name E-Comprocessing for the performance of these operations);
- Independent Sales Organisation (ISO) – we are an intermediary between the Merchant and the relevant Acquiring Bank.

emerchantpay group ltd. also comprises of other companies involved with other services, such as payment facilitating, electronic money issuing and digital wallet services. On the other hand, the group involves companies relevant for the facilitating of business operations such as outsourcing companies. Some of these companies are:

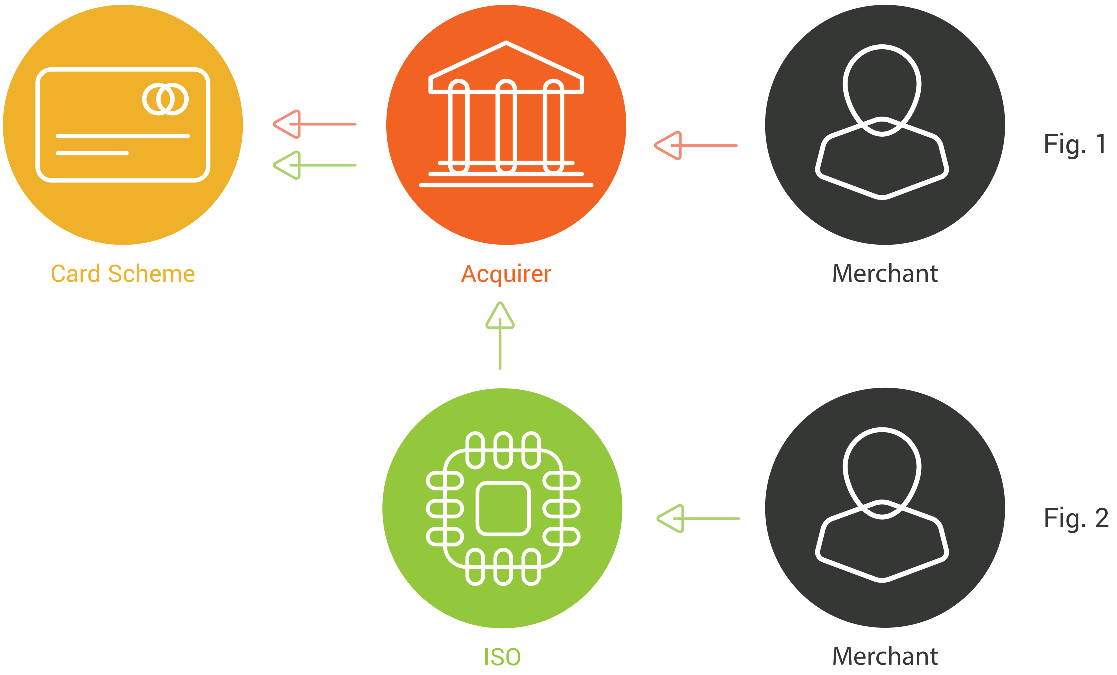
- EMPPay Limited, a UK based payment facilitator registered with the card schemes and responsible for due diligence and settlement of its sponsored merchants;
- eZeeWallet Limited, a Cyprus-based staged-digital wallet operator, under development;
- emerchantpay OOD, a company based in Bulgaria responsible for the facilitating of operations of the authorised electronic money institution – emerchantpay Ltd (UK);
- emerchantpay Corporation, a USA-based *longa manu* of our underwriting department;
- JLF Enterprises, a UK-based company responsible for the pre-paid cards project “eZeeCard”

Acquiring

As mentioned above emerchantpay Ltd. is using the trading name E-Comprocessing (“ECP”) for its activity as an acquiring bank. In order to acquire transactions, we are providing our customers with a fully compliant payment gateway services (see Gateway) and, where relevant, a secure web payment page (if necessary). The relevant rules and regulations that we abide by are the Payment Card Industry Data Security Standard (PCI-DSS) and the card schemes rules for payment card transactions (Fig. 1).

Independent Sales Organisation (ISO)

As an ISO, we have established legal relationships with numerous Acquirers for which we act as an intermediary. As part of this, we are performing the customer due diligence, customer on-boarding and monitoring on behalf of the Acquirer (Fig. 2).



Corporate governance

In the present section, we shall be observing the corporate structure on a group level and the mechanisms for control and governance within the group. In this preliminary paragraph, it should be noted that the operations within our group of companies are diversified in such manner as to mitigate eventual risks and operate in the most effective and efficient manner in an environment of clearly defined roles and responsibilities.

1. Principles

Our group has established the following principles in its structural organisation:

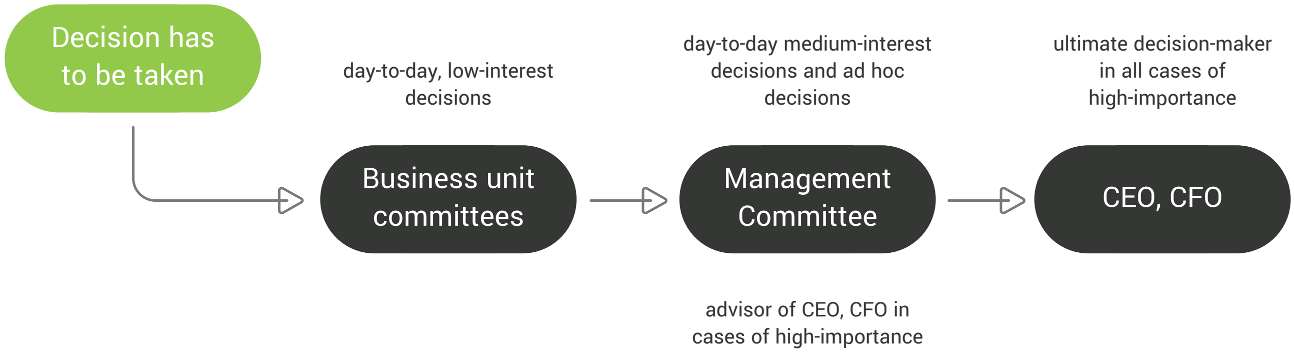
- centralisation – the decision-making authority is vested to the management committee of the respective company, however in some circumstances the ultimate decision is taken by the CEO and the CFO of the group;
- formalisation – the various internal policies that companies within our group implement;
- hierarchical levels – our organisational hierarchy is with the purpose of achieving higher degree of effective supervision over the day-to-day operations;
- departmentalisation – our group implements the dualistic approach, namely we combine both functional and product-based structure.

2. Key functions

Our group has implemented the following key functions:

- executive function – performed by the executive directors of the companies;
- operational function – performed by the various departments respectively for each business unit;
- internal control function – performed by the risk function, compliance function, MLRO and internal audit function for the respective company or on group level;
- supervisory function – performed by the non-executive directors of the respective company or of the group;
- consultative function – performed by the committees on business unit level.

3. Decision-making


Decision has to be taken
day-to-day, low-interest decisions
day-to-day medium-interest decisions and ad hoc decisions
ultimate decision-maker in all cases of high-importance
Business unit committees
Management Committee
CEO, CFO
advisor of CEO, CFO in cases of high-importance

*management committee – decision-making and in some circumstances advisory function on a group level.
*business units – each product-based unit has a functional structure on its own.

Partners

1. Acquiring banks

As an ISO, emerchantpay - in the role of an intermediary between merchants and acquirers - is working with third-party acquiring banks other than its acquiring business unit ECP. Currently we are working with the following acquiring banks:

- B+S – www.bs-payment-europe.com, based in Germany;
- Borgun – www.borgun.com, based in Iceland;
- Elavon – www.elavon.com, based in the United States;
- Korta – www.kortapay.com, based in Iceland.
- Transact Europe – www.transact.eu, based in Bulgaria;
- Worldline – www.worldline.com, part of the Atos group, based in Belgium;

2. Independent Sales Organisations

As an acquiring bank, under the trading name E-Comprocessing (ECP), our company has established legal relationships with other third-party ISOs which help expanding our acquiring unit.

3. Payment Facilitators

As an acquiring bank, we have

contracted with several payment facilitators (PFs) and registered them within the relevant card scheme. These act on behalf of merchants and are responsible for the performance and provision of customer due diligence, merchant accounts and settlement. This is with the purpose of the easier on-boarding of vast number of merchants with low amounts of processing.

For more information, see Payment facilitators.

4. Resellers

In order to expand our market reach, our company has also contracted with numerous reseller agents who promote our payment solutions and introduce to us potential merchants.

Business focus

emerchantpay provides services to all types of merchants having a legal and, if applicable, authorised business. We primarily focus on high-risk businesses, such as:

- financial services;
- cryptocurrencies business;
- games of chance, skill games and casual games;
- adult;
- travel;
- food supplements.

Onboarding

Businesses desiring to accept electronic payments, via credit or debit cards, must choose an acquiring bank to perform the transactions and connectivity with the relevant card schemes on their behalf. Our company comes in this stage either as an intermediary (ISO) between the Merchant and the chosen Acquirer, or as the Acquirer *per se*.

In both of its forms, emerchantpay's Underwriting Department performs the on-boarding process.

The onboarding process consists of:

- application submission;
- application review;
- presentation to credit committee;
- presentation to the acquiring bank;
- merchant agreement and compliance assessment;
- merchant setup;
- integration;
- account activation;
- collection of original KYC documents;
- customer care and customer satisfaction.

emerchantpay is committed to combatting financial crimes and in order to do that effectively, our account managers (aka account executives), responsible for the on-boarding process, are performing customer due diligence of the applying merchants. This includes collecting know your customer (KYC) information about the merchant and the verification of such information.

More information on the procedure performed by the account managers of the underwriting department you can find below (see Underwriting Department).

IV. Payment ecosystem

In the present chapter, the most relevant topics for our business in the world of payments will be observed.

Gateway

A payment gateway authenticates and routes payment details in an extremely secure environment between various parties and related banks. The payment gateway functions in essence as an “encrypted” channel, which securely passes transaction details from the buyer’s device (PC or mobile) to banks for authorisation and approval. On gaining the approval, the payment gateway sends back the information to the merchant thereby completing the “order” and providing verification. A payment gateway is immensely justifiable on account of the multiple benefits it offers including:

- available 24/7/365;
- real-time authorisation;
- customisable reports;
- secure flow of transaction details among customers, merchants and financial institutions;
- multi-currency settlements;
- small fees;
- multiple payment methods.

With respect to our business activity we use the following payment gateways:

- IPGPAY – third-party gateway for Card-not-present transactions;
- Genesis – a product of our company, constantly developing to fit our growing business;
- Pay.ON – third-party gateway for Card-not-present transactions;
- PayPlaza – third-party gateway for Card-present transactions;
- AEVI - third-party gateway for Card-present transactions.

More information on what a payment gateway is and how does it work you can find here.

Payment systems

A payment system is a combination of operations, with the purpose of performing a single transaction. Payment systems transfer funds with formal, standardised arrangements and common rules for the processing, clearing and settlement of payment transactions. Payment systems working with payment cards are referred to as the “schemes”.

Depending on the transaction, whether it is a payment card transaction or an alternative to a payment card transaction, the payment system is either operating under a four-party model or a three-party model.

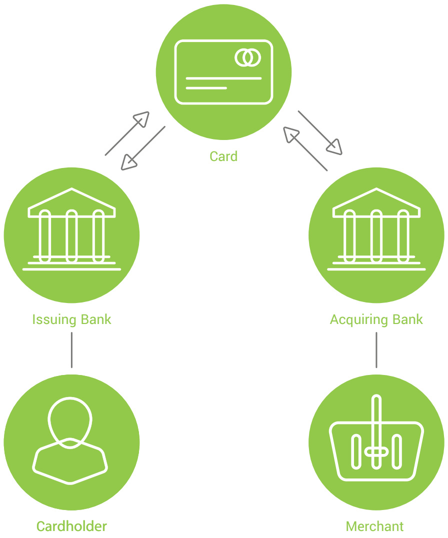


Fig. 3 “4 Party Model (alternative payment method)”

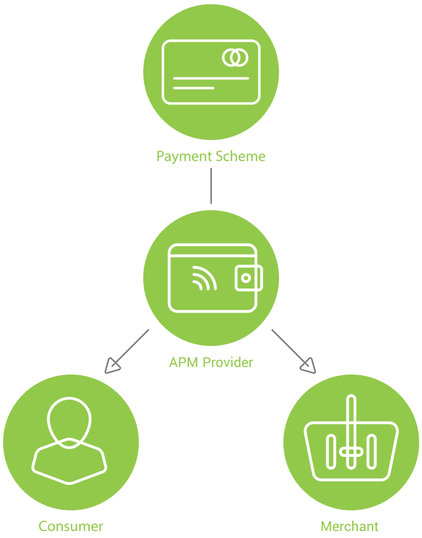


Fig. 4 “3 Party Model (alternative payment method)”

Retail commerce

Retail commerce is the cornerstone of card-based payments. In retail commerce, it is all about the vis-à-vis interaction between the cardholder and the merchant. Transactions in this sphere of payments are called card-present transactions. Card-present transactions can be either affected through a Point of Sale (POS) or mobile Point of Sale (mPOS) device.

1. POS

In retail, the point of sale a terminal device is used by the merchant. The terminal device is provided by the acquiring bank of the company, which is responsible for the latter. In most parts of the world, terminal devices use the chip and PIN method. This is where the card’s EMV chip is read by the terminal device and the cardholder “signs” for the payment transaction with its PIN code.

2. mPOS

Mobile POS devices (mPOS) are again used in a vis-à-vis interaction with the cardholder. The only difference is that the mPOS device is a card reader connected with the smartphone of the Merchant. It uses the mobile data to communicate with the acquiring bank and the smartphone is also used for the entry of the price and PIN code. The plus is that mPOS terminals can be used wherever a mobile data connection is available for the smartphone.

3. Transaction flow

The transaction flow in retail commerce is the same as in the e-commerce (see Fig. 5), with the difference that in retail commerce instead of a web payment page form the cardholder initiates the transaction on the cashier desk via the POS or at another physical place via mPOS device.

eCommerce

1. À propos

With the vast development of internet, a new phenomenon was born – electronic commerce. Businesses realised that with the help of internet they can greatly expand their marketing campaigns and extend sales worldwide. In order to do that, there was still one big issue that had to be solved: the payment. Customers are usually reluctant to pay on delivery, or to go to their bank and send wire transfers. In the light of this, the electronic payments flourished. Payments with credit and debit cards, through the secure web payment pages of merchants, were the accurate solution. After that, many other alternative payment methods (APMs) were developed in order to ease even more the transition of funds (e.g. online wire transfers, electronic wallets, etc.).

2. Transaction flow

In the following diagram, you can track the lifecycle of an electronic commerce card transaction (i.e. card-not-present transaction). Explanations for every stage of the transaction are provided.

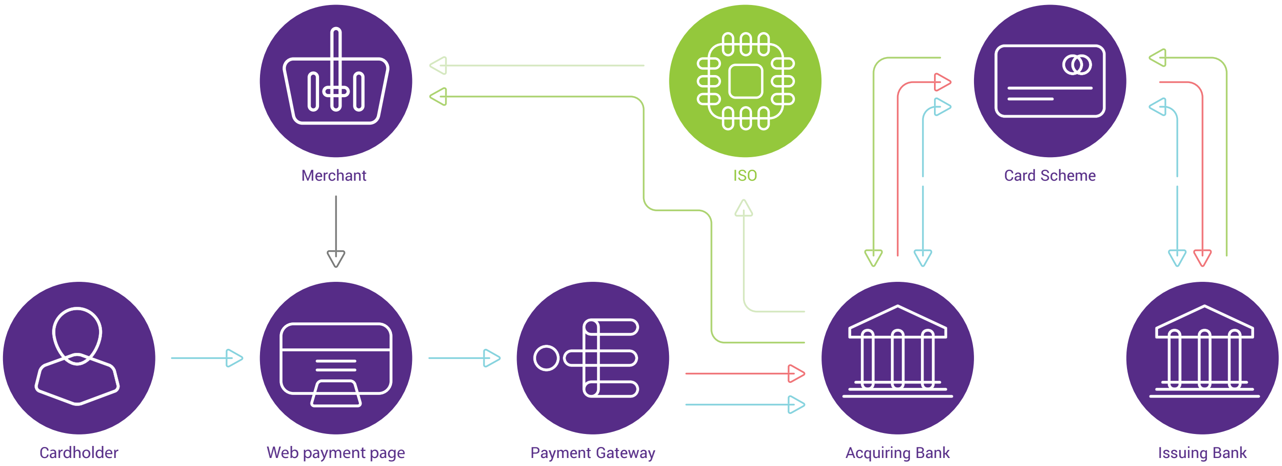


Fig. 5 “Payment Card Transaction: Lifecycle”

Authorisation

1. Cardholder submits its card credentials to the Merchant on the Web Payment Page.
2. Card credentials are sent through the Payment Gateway to the Merchant’s Acquiring Bank which asks the relevant Card Scheme to determine Cardholder’s bank.
3. Card scheme’s authorisation system validates card security features and approves sending to Cardholder’s bank for purchase approval.
4. Cardholder’s bank approves purchase.
5. Card Scheme sends approval to the Acquiring Bank.
6. Acquiring Bank sends approval to Merchant.
7. Cardholder completes purchase and receives receipt.

Capture

1. Gateway sends an 80-byte capture file to the Acquirer.
2. Acquirer sends the file to the Issuing Bank through the Card Scheme system.

Settlement

1. After receiving the capture file (invoice) the Issuing Bank sends the monetary amount to the Acquiring Bank through the Card Scheme.
2. Acquiring bank then sends the amount to the Merchant either directly or through an ISO.

Mobile commerce

Mobile commerce is the payment industry's response to the smartphone craze. Nowadays, mobile phones can perform almost every function of a personal computer or laptop faster and easier. In the light of this, the payment industry has developed mobile applications and mobile-friendly websites making payments via smartphones a reality. Mobile commerce is the way by which a buyer can shop on the run, only with its smartphone.

1. The mobile payments landscape

The line has to be drawn between mobile payments and mobile commerce. Mobile payments are all payments for which a mobile device (smartphone) is used, either by the buyer or the seller. Mobile commerce is only a part of mobile payments. The latter also comprises of payments facilitated by mPOS, near-field communication (NFC) technology implemented in a mobile device, or money transfers effected through mobile banking app.

2. NFC technology

Near-field communication technology is a set of communication protocols that enables two electronic devices, one of which is usually a portable device such as smartphone, to establish communication by bringing them within 4 cm of each other.

For example, cardholder X wants to buy groceries from the supermarket. On the counter X decides to pay using its mobile phone. X has already added its card credentials to its AndroidPay wallet on the phone and using the NFC technology on the device, via AndroidPay, he can send the information to the POS Terminal and effectively authorise the transaction.

Note that NFC on a mobile device would not be part of mobile commerce. Although it is part of mobile payments, it rather qualifies as retail commerce since it is a face-to-face transaction.

The NFC technology is also used outside the mobile payments landscape. In payment cards, it is implemented in the plastic and is used for the communication between the terminal and the card. The latter transactions are usually referred to as "contactless" card transactions (e.g. Mastercard PayPass, Visa PayWave). That is because there is no physical interaction between the card and the POS Terminal there is rather a radio-signal based interaction.

3. Mobile banking

Mobile banking is also not part of mobile commerce, due to the fact that with mobile banking there is no direct interaction with the merchant. In order to qualify as mobile commerce, one must be directly related to the buying of goods or services. Mobile banking is a mobile payment method because one can initiate credit transfers, using an app or a mobile-friendly website on his phone.

4. Mobile commerce

Mobile commerce (or mCommerce) is the tool by which the customer uses a cloud-based instrument such as a mobile app (or mobile-friendly payment page) on its own smartphone for the buying of goods or services online. The methods by which you can perform the transaction are again identical with the methods in e-commerce with one exception – carrier billing. Examples depend on who holds the payment account: for card payments - e.g. Visa/ Mastercard, for carrier billing - e.g. Telenor/ M-Tel, for bank transfers - e.g. ACH, for other APMs (e.g. PayPal).

In order to identify if the payment method is mobile commerce you can ask yourself the following questions:

Are you using your phone?

Where is the information securely held?

Are you buying goods or services?

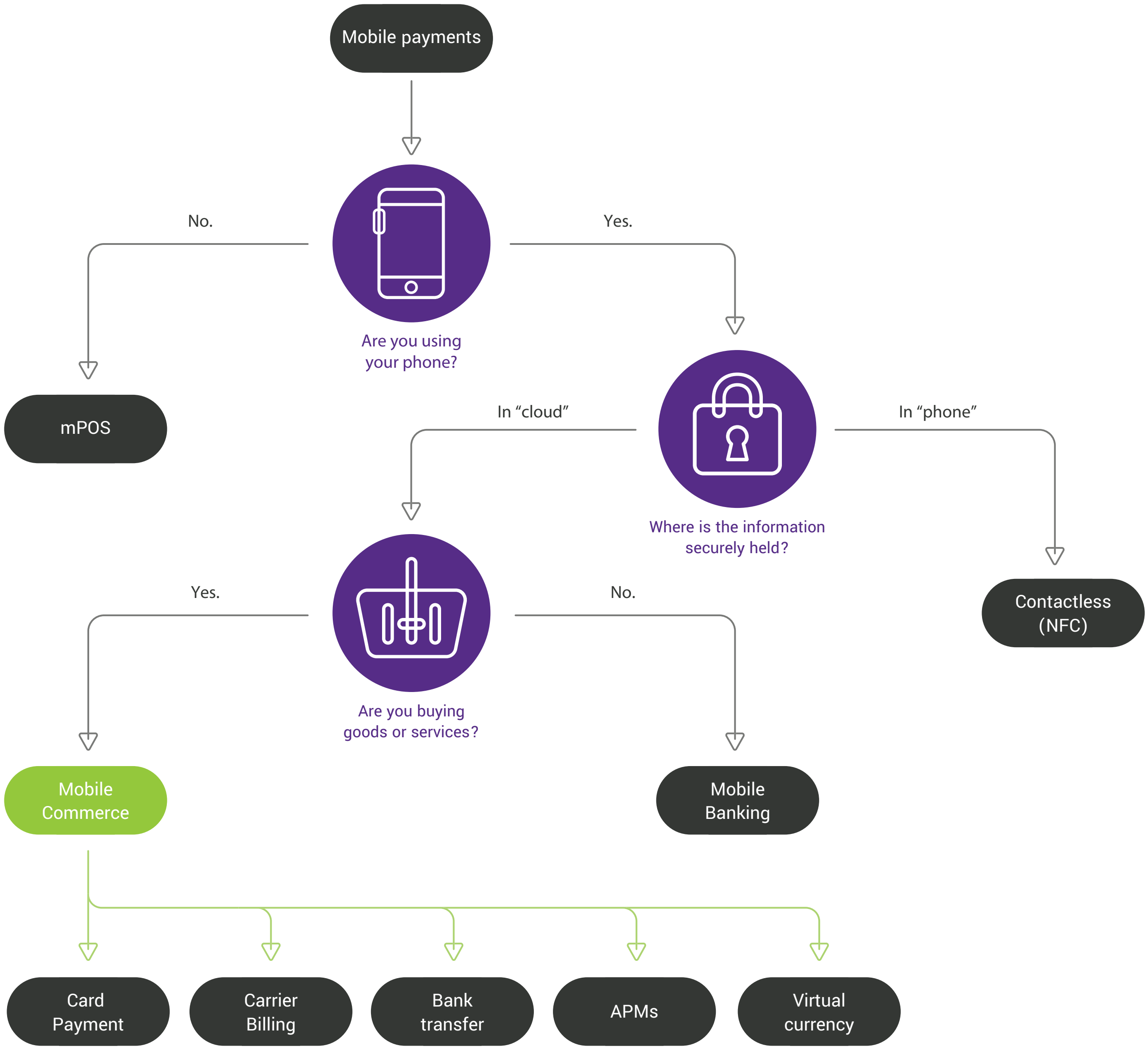


Fig. 6 “Mobile Payments Landscape”

5. In brief

Mobile payments include every payment that is initiated with a mobile device, regardless of the method and whether the buyer or the seller is using the device. Mobile commerce, on the other hand, extends only to the payments that are initiated by the buyer using its own mobile device which is connected to the Internet and the transaction is effected through an app or a mobile-friendly website of the Merchant.

Transactions

In the world of payments, many types of transactions exist. In the present section, we will divide them by their specific characteristics. Note that this section is not exhaustive, it is drafted only with the purpose to present a general framework of the most typical and fundamental types of transactions.

1. Recurring and one-off

Transactions can be **one-off** in the sense that you pay only one time for services or goods. For example, you want to buy a newspaper from the merchant – you enter the website, choose the item and then check-out through the web payment page form. In that case, you will be paying the full amount in exchange for the delivery of the newspaper.

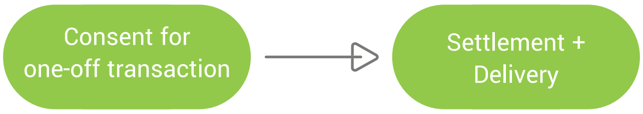


Fig. 7

In case you are buying the current newspaper and subscribing for every newspaper published by the merchant, the transaction would be **periodical (recurring)**.

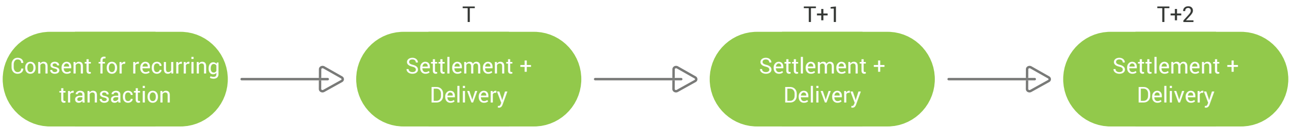


Fig. 8

The difference between a recurring and one-off payment is in the **number of settlements**. In the first case, you give your consent for a transaction once and you are being debited on a certain period of time again and again in exchange of the upcoming items of the same species. With one-off payments, you give your consent once and you receive your item once. There are no further settlements or deliveries.

2. Pay-ins and pay-outs

The receiver of the transaction amount is the main difference between pay-ins and pay-outs.

With a **pay-in (funding)** transaction, the cardholder transfer funds to the merchant in exchange for goods or services.

With a **pay-out (refunding)** transaction, the merchant transfer funds to the cardholder due to cancelled services, returned goods, etc.

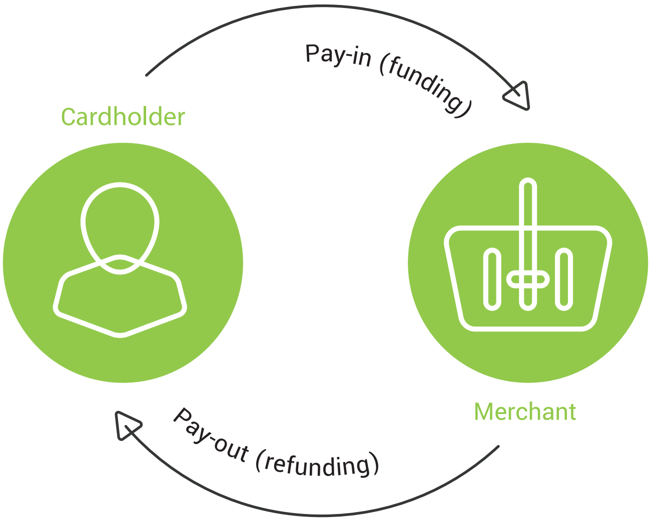


Fig. 9

One special form of a pay-out transaction is the **Original Credit Transaction ("OCT") or the Gaming Payment Transaction ("GPT")**. The latter is specifically designed for the disbursement of gambling winnings from merchants to cardholders.

3. Reversal transactions

Situations where funds from a transaction are returned to the cardholder's bank account. Reversals can be either authorisation reversals, refunds or payment reversals. The main difference between these three is the moment of their initiation.

Reversal, in most cases a transaction is pre-authorised when a cardholder makes a purchase. The funds are then cleared and transferred from the cardholder to the merchant. However, it is possible that the transaction could have incorrect information when submitted. Then, the merchant can contact its acquiring bank to initiate an **authorisation reversal** before the transfer of funds is complete.

Refund is situated between an authorisation reversal and a payment reversal. That is because it occurs after a transaction is cleared, but before the customer files a dispute. While an authorisation reversal cancels the sale outright before any funds are transferred, a refund simply traces the transaction path in reverse. It does not nullify the transaction, it rather creates a new transaction to transfer an amount equal to the total of the original transaction.

Payment reversal (chargeback) is when an issue cannot be resolved neither by an authorisation reversal, or a refund. In this case the issuing bank, on behalf of the cardholder, initiates a dispute for the amount of the transaction.

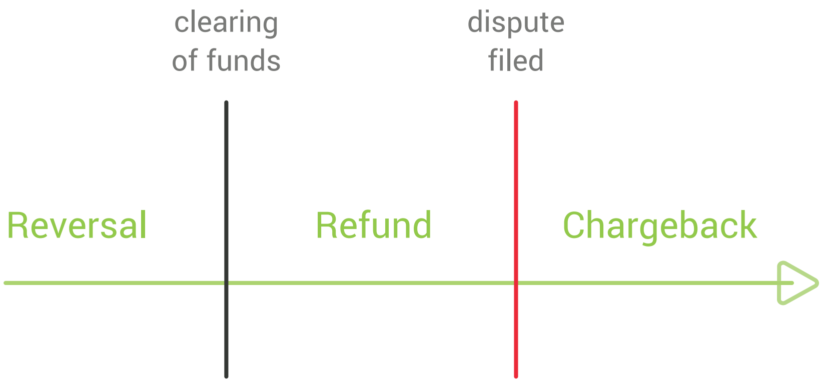


Fig. 10 "Reversal transactions timeline"

4. Credit and direct debit

These types of transactions are non-card payments, usually wire transfers, available only through alternative payment methods ("APMs"). Such an example is the Single Europe Payments Area ("SEPA"). The main difference between credit and direct debit transactions is the initiator.

In a **credit** transaction, the payer (person who pays) instructs its bank to transfer funds to the payee (person who receives) in exchange of goods or services.

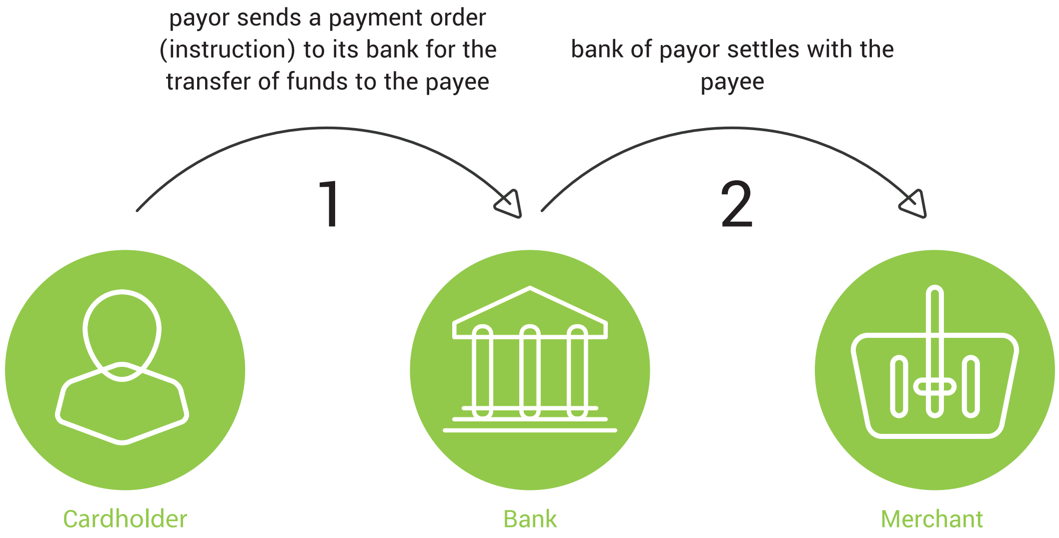

payor sends a payment order (instruction) to its bank for the transfer of funds to the payee
bank of payor settles with the payee
1
2
Cardholder
Bank
Merchant

Fig. 11 "Credit transaction"

In a **direct debit** transaction, the bank of the payee initiates the transfer of funds from the payor's bank account on the basis of a previously given consent from the payor to its bank for that particular payee. In practice this, is mainly used for the payment of electricity bills or other communal bills where it is easier for the payee to give consent for the upcoming bills instead of going to the bank every month to settle with the provider.

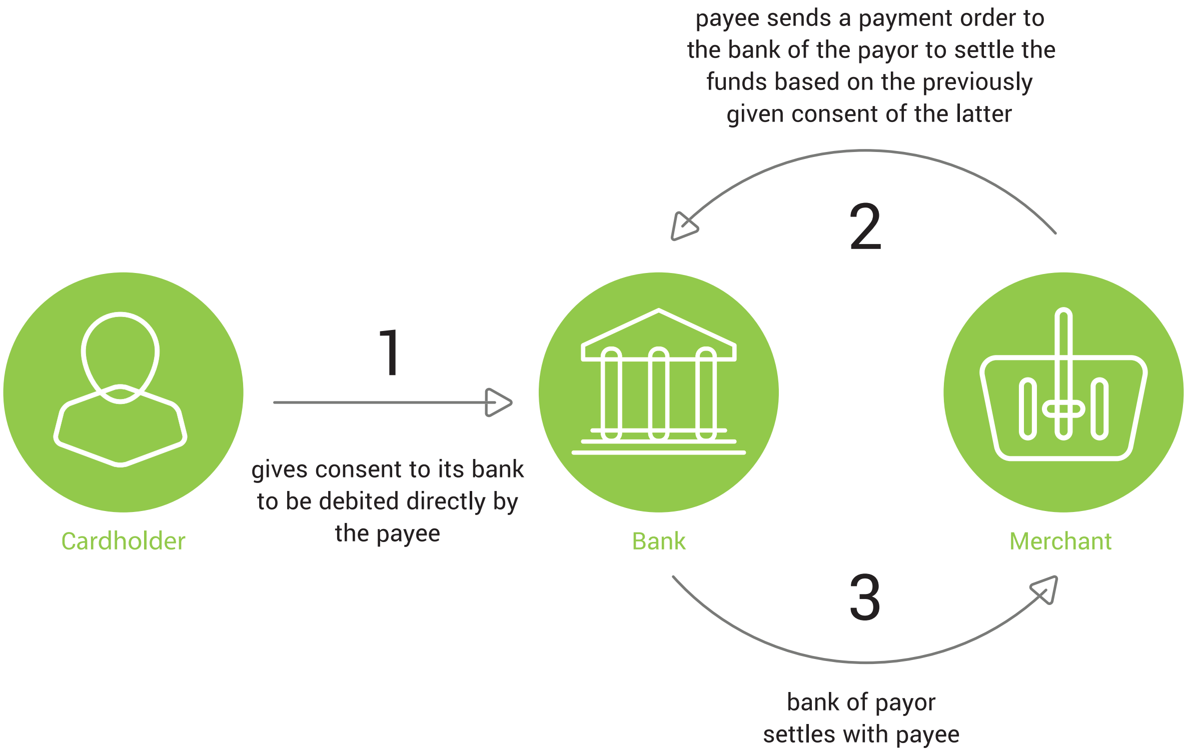

payee sends a payment order to the bank of the payor to settle the funds based on the previously given consent of the latter
2
1
gives consent to its bank to be debited directly by the payee
Cardholder
Bank
Merchant
3
bank of payor settles with payee

Fig. 12 "Direct debit transaction"

Digital currency

"Digital currencies" is the general term encompassing all types of currencies, that are only available in digital form. The main advantage of digital currency is that it allows for instantaneous transactions and borderless transfer-of-ownership.

Digital currencies comprise virtual currencies and electronic money. You may find that both terms are used interchangeably. However, a distinction has to be drawn in accordance with the understanding of the EU legislator.

1. Electronic money

Electronic money is the digital form of fiat currency emitted by a central bank. In practice, it is most common for staged digital wallets where the cardholder funds its wallet with fiat currency using one of the available payment methods. Then, the wallet operator issues electronic money with the fiat currency as an underlying asset. The wallet operator must also issue electronic money at par value (i.e. at the same amount as the amount of fiat currency received). An option for the client to repurchase its e-money is also available, in this process the client returns its available e-money and receives the fiat currency that is behind them.

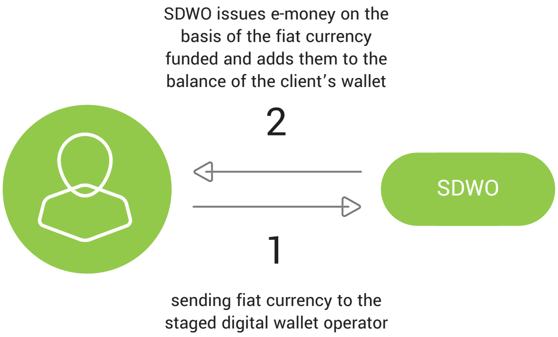

SDWO issues e-money on the basis of the fiat currency funded and adds them to the balance of the client's wallet
2
SDWO
1
sending fiat currency to the staged digital wallet operator

Fig. 13 “Wallet funding”

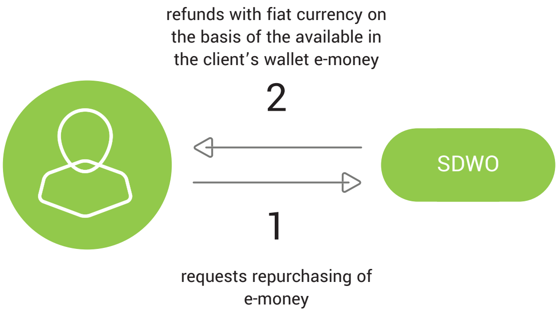

refunds with fiat currency on the basis of the available in the client's wallet e-money
2
SDWO
1
requests repurchasing of e-money

Fig. 14 “E-money repurchasing”

2. Virtual currency

Virtual currency is a digital representation of value which is neither issued by a central bank nor a public authority, nor necessarily attached to a fiat currency. However, it is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically.

There are different types of virtual currencies that differ on whether they are centralised or decentralised, convertible or non-convertible.

Centralised and convertible are such that the virtual currency is issued by a single administrative authority, which controls the systems and that can exchange them for fiat currency. Such examples are the “linden money” used in the online virtual world “Second Life”.

Centralised and non-convertible are such that the virtual currency is issued and controlled by a single administrative authority, but cannot be exchanged for real money (according to the rules of the issuer). Such an example is the “gold” used in the massively multiplayer online role-playing game “World of Warcraft”.

Decentralised and convertible, commonly known as “cryptocurrencies” are such that the virtual currency has no issuer and it is scrutinised by the participants in the blockchain. Cryptocurrencies can be exchanged for real money on again numerous exchange platforms. Such examples are Bitcoin, Ethereum and Ripple.

3. Summary

In order to sum up, digital currencies (genus) are divided in two *species*, one of which with three sub-species. Their differences are depicted below.

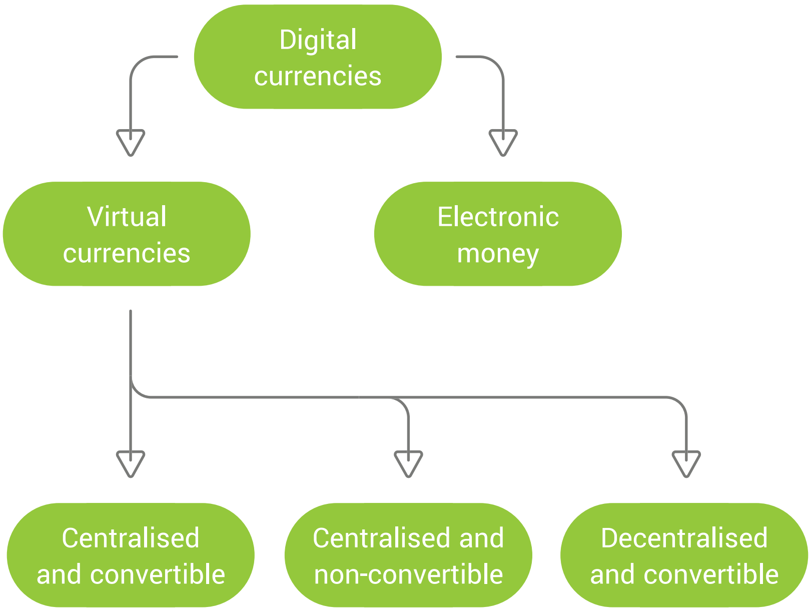

Digital currencies
Virtual currencies
Electronic money
Centralised and convertible
Centralised and non-convertible
Decentralised and convertible

Fig. 15 “Digital currencies family tree”

V. Service providers

Introduction

As an acquiring bank, emerchantpay, with the purpose to extend our reach and enhance our transactional capabilities, uses the services of third-party service providers such as payment facilitators, digital wallet operators, marketplaces, ISOs etc. The term “service provider” derives from the card schemes’ view on the matter and applies to every partner (agent) of our company that receives or otherwise benefits from the card scheme rights of our company, whether directly or indirectly performed by such partners.

Digital wallet

1. À propos

With the development of e-commerce and the need to facilitate payment transactions, digital wallets were invented as a solution. Consumers are not required to fill in order forms on each site when they purchase an item because the information has already been stored and is automatically updated and entered into the order fields across merchant sites when using a digital wallet. Consumers also benefit when using digital wallets because their information is encrypted or protected by a private software code; merchants benefit by receiving protection against fraud.

Two types of digital wallets are available – pass-through digital and staged digital. They differ on whether they provide for the safeguarding of funds.

2. Staged digital wallet

A staged digital wallet is a digital wallet that uses multiple 'stages' to complete the transaction - a 'funding' stage and a 'payment' stage - and does not necessarily pass along card information to the card brand or issuer.

- funding stage, where the wallet acquires money from the purchaser (cardholder)
- payment stage, where the wallet operator provides money to the business (Merchant)

In essence, the staged digital wallet essentially acts as a middleman. With a staged wallet, the card issuer or card network does not necessarily know what type of card was used or other useful information.

3. Our role

In our activity as an Acquirer, we comply with the relevant card Scheme rules applicable to digital wallet operators either **staged digital wallet** or **pass-through digital wallet**.

Given the increased prominence of digital wallets in the payment industry, card schemes have drafted requirements for two basic digital wallet models – the pass-through digital wallet and staged digital wallet models. These requirements include transaction identification and registration requirements for the staged digital wallet model, in order to maintain a proper oversight in how these wallets interact with the respective card scheme network.[1]

Payment facilitators

1. À propos

Survival of the fittest is a well-known concept: the strong survive and the weak disappear. In the world of payments and technology, strong is often associated with longevity given the complexities of launching and igniting new payments technologies.

A payments facilitator (or "PF") allows anyone who wants to offer merchant

[1] More information on digital wallet operators you can find in our policy on the matter at confluence (link).

services on a sub-merchant (sponsored merchant) platform. Those sub-merchants then no longer have to get their own MID. Instead, they can be boarded under the master MID of the PF who is sponsored by an acquiring bank. This allows merchant services to be offered in a very elegant and very efficient manner.

2. Function

Payment facilitators are merchant service providers that simplify the merchant account enrollment process. PFs operate a sub-merchant platform where merchants no longer require their own MID but are boarded directly under the PF's master MID account.

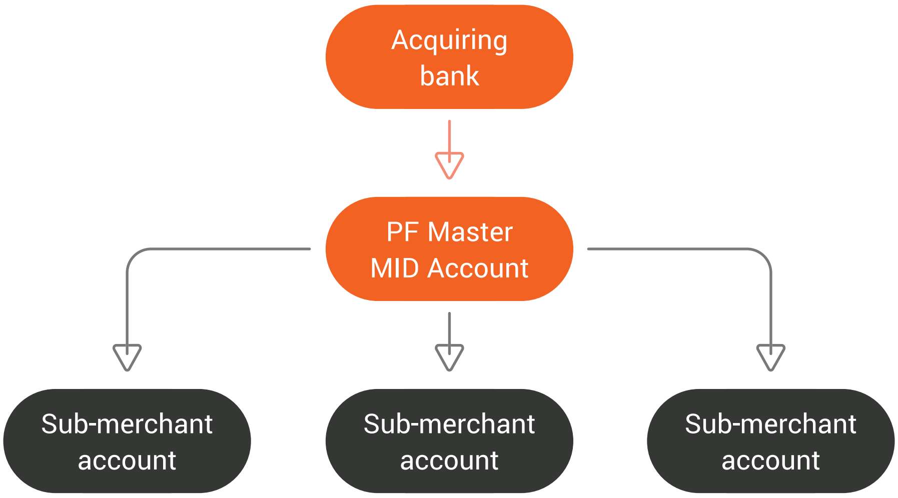


Fig. 16 "PF Platform"

Marketplace

In simple terms, a marketplace is the intermediary between the buyer and the seller. It is simultaneously an agent of the buyer and of the seller. Nowadays, the legal framework in the EU (i.e. PSD1) exempts commercial agents from the application of the directive. This means that marketplaces (e.g. Alibaba, eBay, etc.) may act without being regulated as a payment services provider.

With the introduction of the new directive on payment services (i.e. PSD2), this exemption is no longer available. Marketplaces therefore need to choose between becoming a payment services provider themselves, or using the services of an existing one. In the light of this, our company has acknowledged the business perspective and prepared itself for the onboarding of marketplaces.

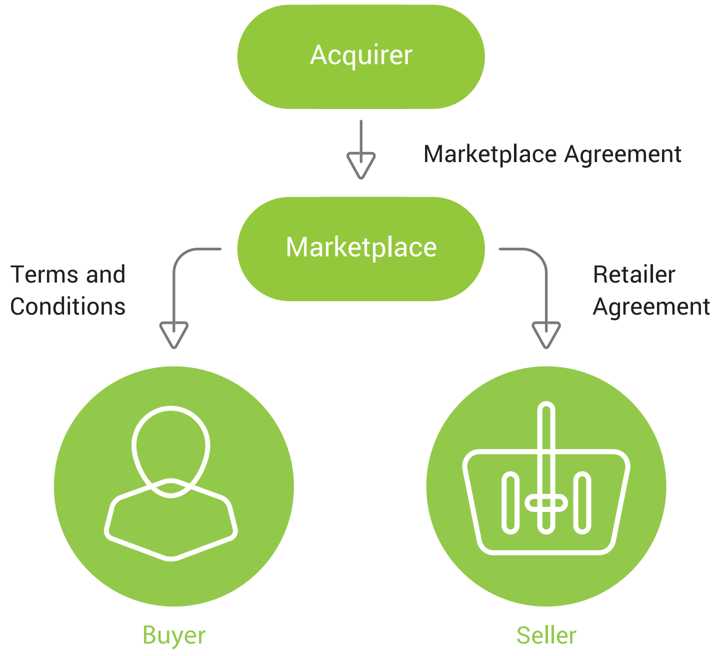


Fig. 17 “Marketplace”

When onboarding marketplaces in the future, they will be registered as third-party agents in compliance with the card scheme requirements.

VI. Underwriting department

Introduction

1. À propos

The underwriting department is responsible for the onboarding of merchants. As of now, business units of emerchantpay group that have independent underwriting departments are the acquiring unit and the ISO unit.

With the development of the digital wallet and the pre-paid cards projects, respective underwriting departments will be created.

The hierarchy of the now-active underwriting departments is the following:

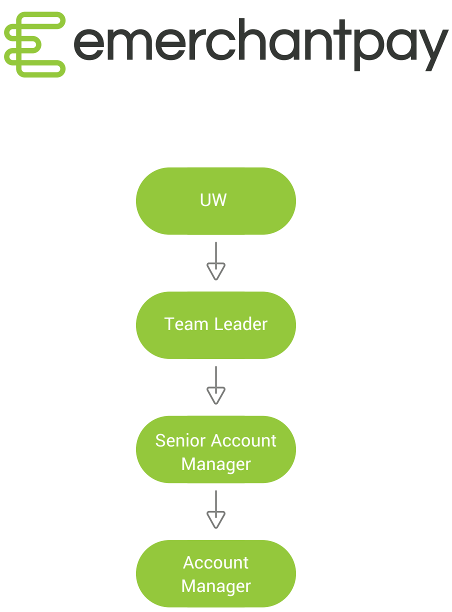


Fig. 18 “ISO Unit hierarchy tree”

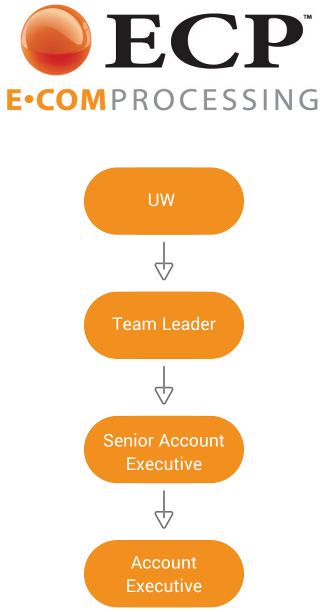


Fig. 19 “Acquiring Unit hierarchy tree”

2. Objectives

Within emerchantpay, the underwriting departments have the main purpose to analyse the business model that the merchant operates, check the merchant background history, collect and assess the relevant documents of the applying merchants and gather enough information to answer the questions:

- “Who are we dealing with?”;
- “What is the merchant business about?”;
- “Are the services or goods marketed legal in the markets the merchant will operate in?”;
- “What is the billing model used by the merchant for charging its customers?”;
- “Does the merchant have any previous experience in the business and what is its performance?”;
- “What is the merchant reputation?”;
- “Does the merchant website contain the relevant information as per the industry standards and the applicable legislation?”;
- The objectives of our underwriting departments are also to keep abreast with any changes in relation with the merchant’s status and to keep the merchant informed on any changes from our side. With other words the underwriting executives are the persons most closely involved with merchants.

Activities

Account executives (or account managers, both terms are used interchangeably) guide applying merchants through the whole process of onboarding which will be observed in the following points.[2]

[2] The following presentation of the underwriting procedure is not exhaustive. For detailed procedure please do not hesitate to contact the relevant business unit department.

1. Application submission

Merchants are presented before the underwriting department, either by a member of our sales team or by a third-party agent. After the initial presentation of the merchant, along with the submission of the application package, a dedicated account executive is assigned to assist the merchant in the process of onboarding.

The application package consists of completed merchant application form, processing statements, know your customer (KYC) documents and any other documents related to the business activity as licenses, authorizations, etc. The KYC comprise documents evidencing the status of the merchant company, its business activities and its representatives.

The merchant application form, along with KYC documents, are required to be submitted in order for the submission to qualify as an application submission.

2. Application review

After the receipt of the required documents, the account executive ensures that the information provided in the merchant application form is consistent with the provided KYC documents.

In order to better evaluate the risk that the merchant represents, account executives make sure that they exhaust every available source of information in order to check the status of the merchant.

In case any questions related to merchant business arise during the application revision, the account executive could contact the merchant directly or the referral agent in order to receive additional information and to be able to build up the merchant case for the further steps of the on-boarding process. For e-commerce merchants, a website check is performed and any website deficiencies are communicated either with the merchant directly or through the agent. No merchant is allowed to start processing before full website compliance is reached.[3]

For retail merchants, an on-site inspection of the premises is conducted before establishing the legal relationship with the purpose of ensuring that the prospective merchant has the proper facilities, equipment, inventory, agreements, and personnel required and if necessary, license or permit and other capabilities to conduct the business.

3. Presentation to credit committee

The credit committee is the authority which makes the ultimate decision for the onboarding of a merchant. There are different authority levels, based on the projected monthly volume of the merchant or the risk associated with the merchant – as indicated by the level of exposure that each merchant represents.

Account executives present the potential merchant to credit committee with all the relevant information and documents as required by the Underwriting Guidelines.

[3] More information on how we perform customer due diligence you can find at confluence (link)

Additionally, the account manager should seek for approval by Credit Committee if any of the initially set conditions need to be revisited or whenever a request which should be granted a consent by Credit Committee is raised during the active relationship with the merchant.

4. Presentation to acquiring bank (ISO only)

If the merchant is endorsed by the credit committee, it is then presented to the acquiring bank by its account executive as explained in the Underwriting Guidelines.

The account executive should follow the respective acquirer requirements when presenting a new merchant. The detailed requirements per bank can be found at **Z:\ISO 9001 and ISO 27001 Procedures_eMP ISO 9001 and ISO 27001 Procedures\DP 3-1 - DETAILED PROCEDURES** - processes related to merchant services at emerchantpay.

The acquirer could approve the merchant application under specific conditions which should be clearly explained to the merchant or the referral agent.

5. Agreement execution

After the approval from the acquiring bank as well as the merchant acceptance of the set conditions, the account executive prepares the merchant agreement and sends it for approval and signature.

The account manager should provide the merchant with all other documents for signature, along with a list of the documents required in paper original when this is applicable.

6. Merchant setup

Upon receipt of evidence for the validly consented merchant agreement (e.g. scanned copy), account executives notify the acquirer (unless the bank directly arranges the agreement execution) and forward any acquirer specific documents and information required for the merchant setup.

When the Merchant Identification Number ("MID") is issued by the bank, the account executive shall prepare the relevant gateway configuration table which to be send to the IT department. Meanwhile, the tech support team sets up the technical details and sends them to the merchant so that integration between the merchant website and emerchantpay gateway can begin.

More information on merchant accounts and integration you can find in the IT department chapter.

During the stage of integration, the account manager ensures that the PCI compliance will be met by the merchant prior to account activation.

7. Account activation

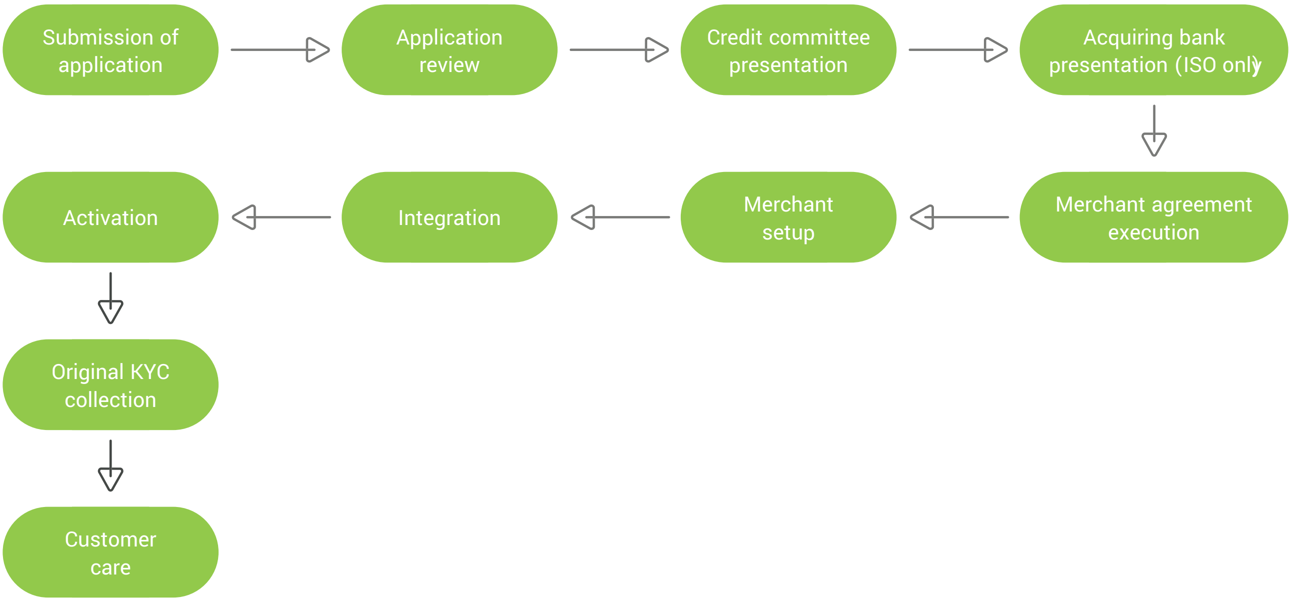
If the integration of the merchant is successfully completed, the account executives performs a second website check to verify compliance. If there are no obstructions, the merchant is sent for activation to a member of the risk department.

8. Collection of original KYC

Before the first settlement to the merchant, account executives collect the original KYC documents in compliance with applicable law and the requirements of the respective acquiring bank. The collected originals are then compared with the already received documents. If there are no discrepancies, the account executive mail the documents to the bank and upon their confirmation, the merchant is allowed to receive settlement.

9. The ongoing relationship

Account executives are required to keep in contact with all merchants and agents comment and remain available for addressing any issues that might occur for the merchant.



Submission of application
Application review
Credit committee presentation
Acquiring bank presentation (ISO only
Merchant agreement execution
Merchant setup
Integration
Activation
Original KYC collection
Customer care

Fig. 20 “Underwriting procedure”

VII. IT department

Introduction

1. À propos

Our IT department is responsible for the development of and support/ web integration with emerchantpay. Web Integration is the connection of a merchant or of a third-party gateway with the emerchantpay gateway. IT department is responsible for the development of the Genesis gateway as well as for the eZeeCard and eZeeWallet products.

2. Objectives

The department is responsible for:

- System Administration and office support activities

- Development and support of the Genesis gateway, eZeeWallet, eZeeCard, emerchantpay web site, etc.
- Direct tech support of Merchants or Integrators via email and/ or ticket system. The tech support team helps solving technical issues related to the Merchant integration and current issues that may arise during processing, and to internal projects managed by the IT department;
- Technical support of merchants and creating account in the gateways (e.g. merchants, manager accounts, client accounts, terminals, MIDs);
- Direct phone and Skype support;
- Review and reply on the incoming tickets from merchants, regarding technical issues or questions;
- Ticketing system operations and support;
- Verifying and approving merchants'/ integrators' integrations with our gateway.

Merchant accounts

During the web integration, merchant accounts are created in our gateway. These accounts are created by opening Terminal IDs ("TIDs"), which are assigned to the respective merchant. All TIDs in the gateway are administrated by our IT department.

Terminal ID indicates the unique identification number of a terminal, which can be searched and indexed by their IDs. The TIDs of our ISO unit are different than and should not be confused with our acquiring unit TIDs.

Merchants can have more than one account, each associated with another TID. For example TID with CVV ON and TID with CVV OFF. Note that terminals are associated only with one currency.

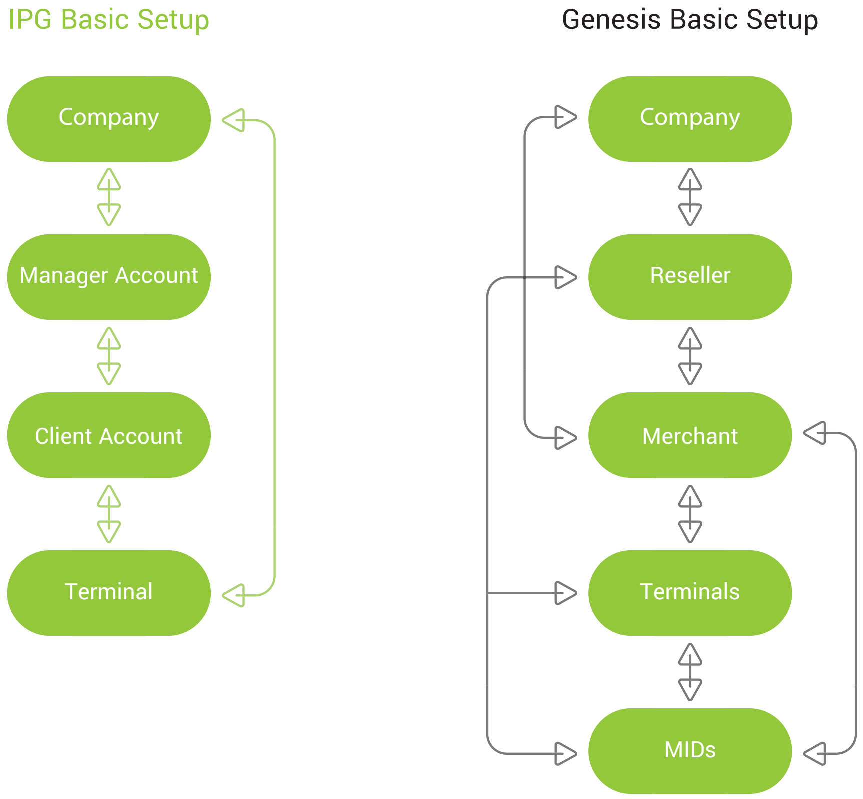


Fig. 21 "Merchant accounts and TIDs"

VIII. System administration

3. Introduction

The system administration department is responsible for providing uninterrupted working conditions, of the entire IT infrastructure of the company, starting from user's workstation trough the local area network to the servers and in-house running applications.

4. Objectives

- Corporate Network and Domain

The corporate network provides wired, wireless and Virtual Private Network (VPN) connection for the company needs. All network connections are restricted and controlled by network firewalls and authenticated by domain controllers, managed by System administration department.

Every device has it's dedicated labeled cable, connected to specific wall socket and then to a specific network port. All of these are documented and managed by the System administration team. Every change have to be done by a Sys Admins team member upon request by email.

Corporate users have their own credentials (username and password). Domain credentials are used for authenticating users when accessing their workstation, the wireless network, corporate email and many integrated applications, like JIRA, Confluence, GitHub and more.

The following policies are applied to Domain passwords:

- Password life: 1 to 42 days
- Password requirements: At least 10 symbols, upper and lower case letter, a digit and/or special symbol (*&^%$#@!~)

Password change is forced by domain controllers every 42 days, but can be manually done via the corporate password management portal: https://emppwd.emerchantpay.com/pm/

Account lockouts may occur in the following scenarios:

- Wrong password is typed 5 times in a row;
- Wrong password is saved in a device.

In these cases the corporate password management portal can be used to unlock the account: https://emppwd.emerchantpay.com/pm/

- Shared resources

Corporate shared resources are accessible for emerchantpay users according to their team and position. Accessible to all are:

'Z:/Manuals' – Where HOW TO guides can be found;

'Z:/General information' – Where any other important info is kept, and

'Z:/Events' – Where Pics and Videos from company events are stored.

- Software and the WEB

Software used in the company is legit and licensed. System administrator rights are required to install additional software, but only after a manager's approval. Even if software installation does not require Administrator rights, approval is required for installation.

Social media sites and torrents access is forbidden in the corporate network.

- Physical Access

  emerchantpay's office infrastructure is protected by a physical access control system, which is also used for time tracking and user activity. Access cards are managed and provided by Sys Admins. In case of a LOST or FORGOTTEN card, user should inform Office administrators team by e-mail to office@emerchantpay.com to block the card.

- Workstation and Peripheral devices

  Every employee has his personal workstation – a PC or laptop, a keyboard, a mouse and a headset. Every change of these have to be done by a member of Sys Admins team upon manager's approval.

  Storing of personal files on the workstation is not acceptable and such are removed on every scheduled maintenance.

  Printers and scanners are present in every department.

- Conference rooms and calls

  There are nine conference rooms in Sofia office, named on the cities with an office of emerchantpay:

  - **London – 1st floor main building**
  - **Tonbridge - 1st floor main building**
  - **Sofia – 2nd floor main building**
  - **Amsterdam - 2nd floor main building**
  - **Jersey - 2nd floor main building**
  - **Boca Raton – 3rd floor main building**
  - **Dubai – 4th floor main building**
  - **Berlin – 2nd floor IT building**
  - **Frankfurt - 2nd floor IT building**

  Conference calls can be initiated and joined via the corporate VoIP system. HOW TO manuals can be found in Z:/Manuals.

- Communications

  System administration department is using a ticketing system to track and handle the support requests. A support ticket is opened by sending an email to itsupport@emerchantpay.com. Every other type of communication is not a valid support request and may be missed and even ignored.

IX. Risk management

Introduction

1. À propos

Our group risk management departments are established for the two main business units, namely ISO and acquiring bank.

The hierarchy is the following:

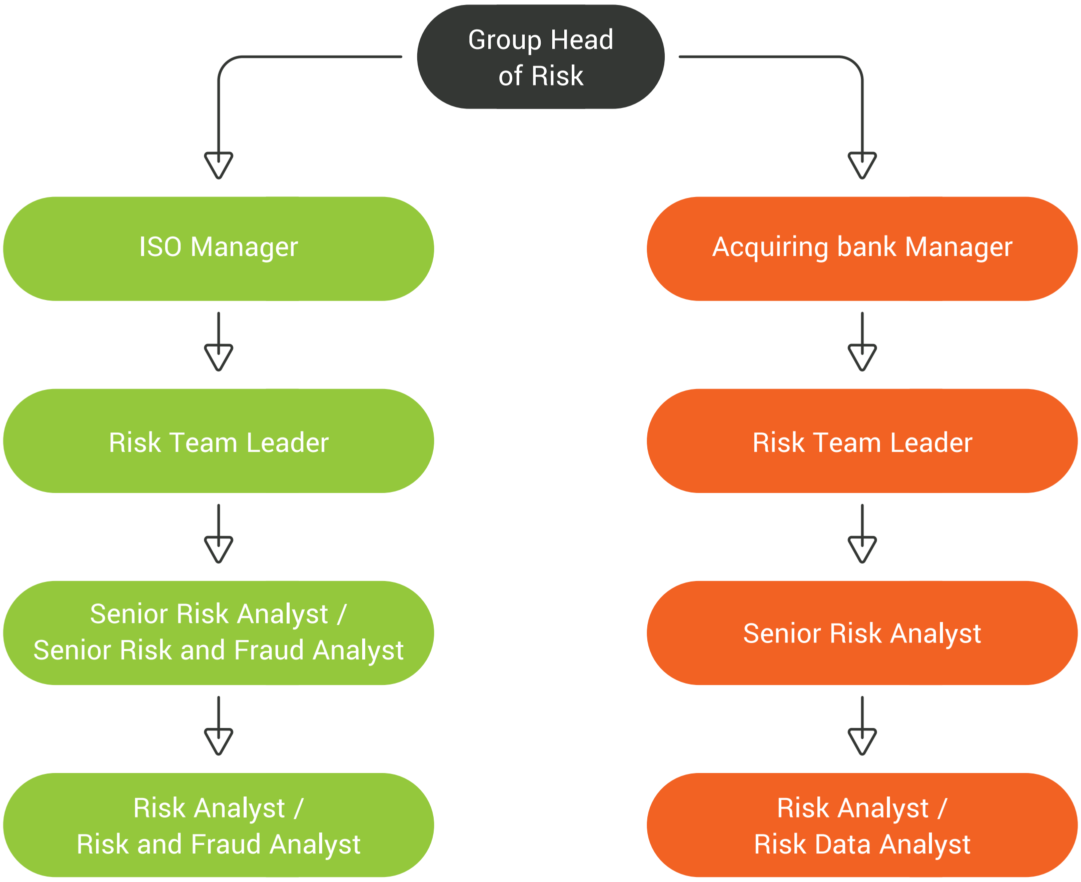

Group Head of Risk
ISO Manager
Risk Team Leader
Senior Risk Analyst / Senior Risk and Fraud Analyst
Risk Analyst / Risk and Fraud Analyst
Acquiring bank Manager
Risk Team Leader
Senior Risk Analyst
Risk Analyst / Risk Data Analyst

Fig. 22 “Merchant accounts and TIDs”

2. Objectives

Risk department mitigates risk based on a two-fold approach:

- protecting cardholders and merchants from fraudulent or criminal activity;
- prevent financial losses for the company and its partners

Risk management involves:

- merchant monitoring and control;
- payment card fraud prevention;

- chargeback management;
- merchant training;
- merchant PCI compliance monitoring;
- website compliance monitoring;
- risk assessment of merchants and websites;
- risk assessment of transaction activity for suspicious transaction or behaviour.

Risks mitigation

Our risk department is involved in combatting financial crime and has implemented various systems. It also controls financial crime risk mitigation.

1. Risks tools

emerchantpay has assembled a comprehensive set of fraud-scrubbing tools that protect the merchant as well as their customers.

Our risk-rule fraud management system uses the latest technologies that enables transaction-scoring behind the scenes. This seamless solution ensures reduced fraud levels and lowers chargeback losses. Maximising the merchant's revenue, while minimising their financial risk, is our main priority.

- **3-D Secure payer authentication** – Verified by Visa ("VbV") and Mastercard SecureCode®;
- **Address Verification Service ("AVS")** – verifies the cardholder's billing address by comparing it to the one on record at the credit card company;
- **BIN country check** – cross-checks whether the card issuer's country matches the one provided by the cardholder;
- **Device fingerprinting** – a combination of third party tools that help to identify users coming from the same (mobile) device, as well as identifying the true IP address, geolocation and if hidden proxy addresses have been used;
- **Telephone authentication and verification** – a tool supported by a third-party provider, fully integrated with our system that maintains a detailed database of shoppers. It also creates automated voice calls or SMS texts with a one-time PIN code that consumers use for authentication at the checkout page;
- **Negative lists and blacklists** – a proprietary database including blacklisted card numbers, and IP and email addresses;
- **Payment Card Industry Data Security Standard ("PCI DSS") Compliance** – PCI Level 1 gateway providers, including our own proprietary gateway solution;
- **PCI Scanning Services** – an integrated solution that helps our merchants reach PCI DSS compliance;
- **Positive lists and whitelists** – accept transactions based on matching cardholder information from your own and emerchantpay's databases;
- **Unique fraud management system** – real-time transaction technology with extended customisation options for merchants;
- **Transaction thresholds and limits** – predefined limits for a transaction, including minimum and maximum amount, and limits per approved transactions per day, week and/or month;

- **Velocity checking** – stops repetitive attempts with the same credit card within a specific period.

2. Risk management activities

Risk management at boarding stage

Participation in Merchant Approval Process – the Risk Executive is involved in Credit Committee Levels.

Determine Approval Processing Terms - upon approval risk, the executive may request specific approval terms. These includemonthly volume caps, velocity and transaction count/amount limits, rolling reserve % and settlement delay (weekly), fraud scrubbing tools to be enabled, 3D processing (full/ partial), internal industry policies to be followed, specific card schemes or local requirements to be met.

Risk Management after activation

Merchant activation – the risk department activates the accounts if all requirements are met (documents are collected, integration is ready). Upon activation, the risk executive sets the risk parameters in the gateway and enable the fraud scrubbing tools.

Initial merchant monitoring – upon first real transaction is processed, the risk executive shall closely monitor merchant processing on a daily basis during first 7-10 days. In addition to this, they shall answer a pre-defied question related to the merchant activity.

Ongoing compliance merchant monitoring – the Risk Executives are performing a series of activities, on a daily and monthly basis, to ensure… that the merchant account is in good standing. These include handling disputes, fraud performance, perform Website/Content checks on monthly base, monitoring transaction activity or lack of activity, checking the PCI compliance status of merchant.

Weekly Settlement Committee reviews - the risk executive is involved in the approval process for the merchant's weekly settlement.

Reporting and analysis – the risk department prepares a chargeback report for each acquiring bank, either each week or once-per-month, under an initially agreed schedule.

Termination – the risk executives are performing a series of activities upon the termination of merchant's account.

X. Finance and Treasury department

Introduction

1. À propos

Our company has two separate treasury departments for each of the main business units, namely ISO and acquiring. In general treasury departments within our group are responsible for the movement of funds in the scope of their business unit.

Movement of funds includes every operation that is initiated with the purpose of disbursing or collecting monetary amounts, including but not limited to, reconciliation, billing, payments to merchants, profit collecting, commissioning agents.

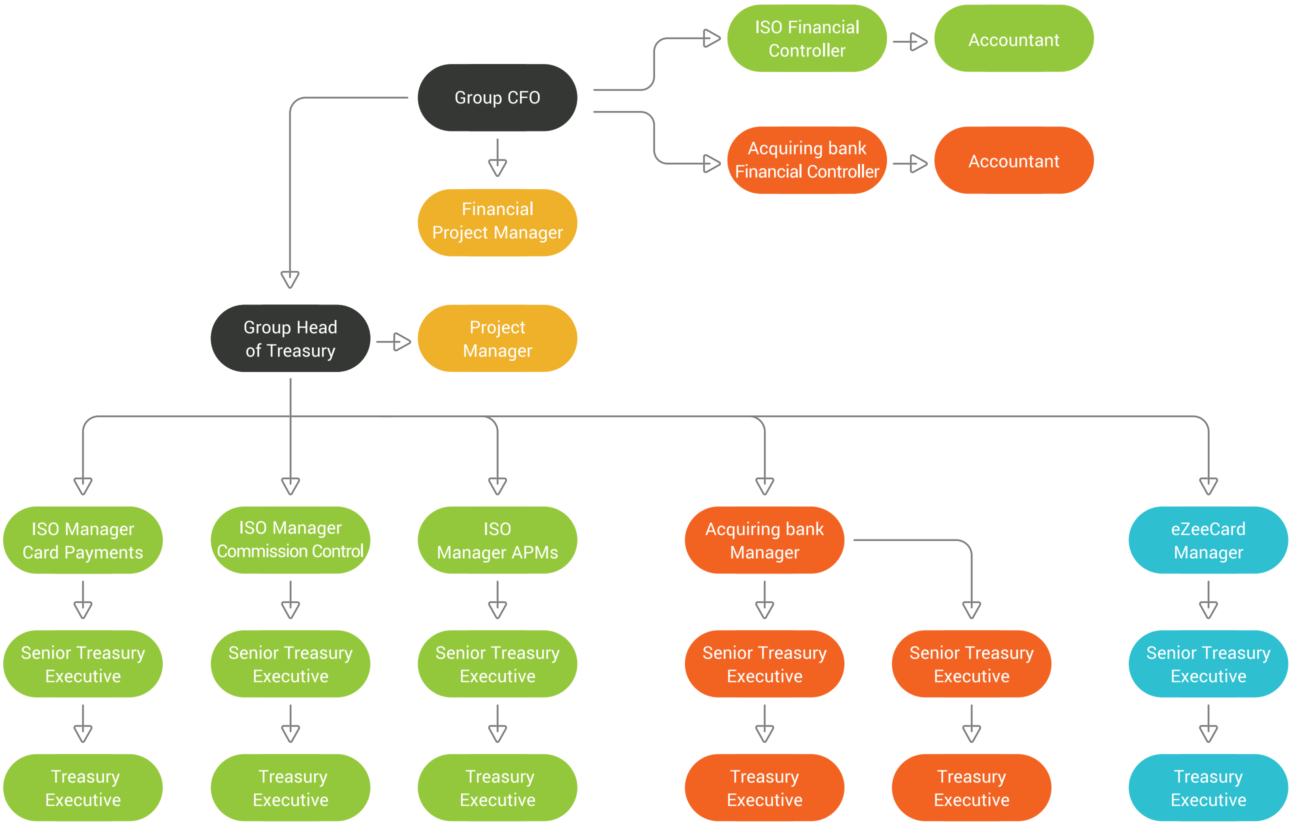

Group CFO
ISO Financial Controller
Accountant
Acquiring bank Financial Controller
Accountant
Financial Project Manager
Group Head of Treasury
Project Manager
ISO Manager Card Payments
ISO Manager Commission Control
ISO Manager APMs
Acquiring bank Manager
eZeeCard Manager
Senior Treasury Executive
Senior Treasury Executive
Senior Treasury Executive
Senior Treasury Executive
Senior Treasury Executive
Senior Treasury Executive
Treasury Executive
Treasury Executive
Treasury Executive
Treasury Executive
Treasury Executive
Treasury Executive

Fig. 23 “Merchant accounts and TIDs”

2. Objectives

The main objectives of the treasury departments are:

- to execute reconciliation and billing activities related to merchants' processing via Acquiring Banks and Alternative Payment Providers;
- to execute payments to the benefit of Merchants from own bank accounts, or by giving payment instructions/ cancellations to other parties;
- to calculate and collect company's profit from various parties involved in the processing chain- merchants, Acquirers, APMs or Card Schemes;
- to work out the Agents' /ISO's Commissions and to execute the payout to their benefit. Calculate or check other processing costs;
- to prepare specific reports used by other Departments and the management team.

Activities

Treasury executives perform various activities related to the movement of funds in and out of the company. In the present chapter, the main activities of a treasury executive will be presented.

1. Reconciliation

Reconciliation comes from the Latin word reconcilare, which means to "to bring together again". Basically, reconciliation a process that confirms whether the money leaving an account is the same amount that is spent.

In our business reconciliation is performed with the purpose to prove that all transactions are registered on both sides – emerchantpay Gateway and the Acquiring bank/APM system. The transactions are matched by type, status and amount. Usually, the transaction ID is the unique matching criteria.

Due to the different types of reports our partners provide, there are two main types of reconciliation – automated and manual.

- **Automated reconciliation** – automatic matching of processed transactions can be performed on a Gateway level by retrieving data from the acquiring bank/ APM and appliying predefined rules. Another option of automatic reconciliation is using an Internal software "ReconArt" that handles data import, mapping, enrichment of data and flagging exceptions each of, which need manual follow-up by a team member;
- **Manual reconciliation** – in this scenario, a member of the Treasury team performs all the checks manually by following a routine periodic matching of transaction data from multiple sources. After a manual download of transaction data, totals are compared and transaction types. Business logic used to allocate codes and status for dispositions – cut-off time, billing cycle, technical error, etc. Treasury contacts the IT team, acquiring bank/ APM in order to trigger exception investigation and resolution.

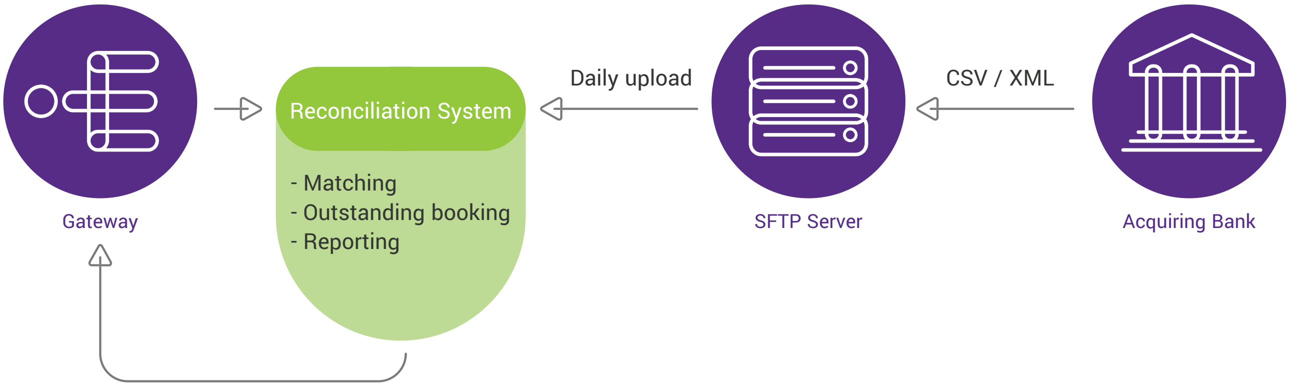


Fig. 24

2. Billing statement

A billing statement is a periodic report that our company issues to merchants showing their periodic net settlement balance, rolling reserve balance, fees, deductions and other key financial information.

Merchants need to understand how exactly their settlement is calculated and what it is based on. The basis is the gross volume of processed transactions in the last billing period. A rolling reserves balance report is an important part of the billing statement reports. Reserves are usually deducted as a percentage of sales and kept for a period of 6 months, then released back to the merchant account. On each statement, the amount deducted or released should be indicated, as well as the total reserve balance.

All fee types are deducted, as governed by the payment services agreement, and all items should correspond to the pricing schedules signed between all parties. Most often, the following billing items are commonly used in the industry, where the terminology or billing frequency may differ, however the methodology of calculation is approximately the same:

- **Merchant Discount Rate** – fixed or variable percentage applied to total sales volume, or to each captured transaction separately;
- **Transaction fee** – a flat fee charged per each approved or declined authorisation;
- **Refund Transaction, fee or OCT/GBT** – fixed value charged per each refund of original sales transaction or per pay-out or (payment of winnings);
- **Chargeback fee** – a flat fee charged for each processed chargeback (or retrieval request, chargeback reversal, re-presentment);
- **Foreign Exchange Conversion fee** – FX conversion from processing to settlement currency may be needed for some accounts, whereby a certain fee or an FX margin will be applied;
- **Wire transfer fee** – fixed charge per remittance to cover bank transfer costs;
- **One-time set-up fee and annual fees, fixed values charge** – one-off or once

monthly, annually;

- **PCI scan, VbV/MCSC fees** – fees charged for these services usually charged on monthly or annual basis.

Billing statements generation process differs depending on acquiring bank/ APM. Therefore formats of the reports, periodicity and distribution will also vary.

3. Payments to merchants

emerchantpay is responsible for ensuring that the elements of risks and financial exposure, involved in merchant card and alternative payment activities, are fully understood, properly managed and controlled. According to acquiring banks' policies and as per the contractual obligations, that we have consented to, our company bears financial liability for direct and sponsored merchants.

Therefore, all payments to merchants, in all cases, either when instructed directly by acquiring banks/ I/PSPs to merchants or either instructed by the emerchantpay Treasury department directly to merchants need to be strictly reviewed and verified by an internal Payments Committee.

Treasury department executives prepare, on a weekly basis, reports on the accumulated net settlement amounts and gross sales volumes of merchants processing via acquiring banks or APM providers. Separate reports are created for each acquiring bank and amounts are presented by billing cycle periods for each merchant account or APM. Additional information such as chargeback activity, outstanding balances or any important notes could be included upon request in any report, thus aiming to provide an adequate indication for the position of each merchant.

Each week, two or more Payments Committee meetings are being held in order to review all merchants' financial status and approve each week's net settlements, including rolling reserve releases. Decisions are taken based upon several controls or performance indicators, such as merchants' processing and fraud performance, credit risk exposure and compliance with procedures.

Only after a majority-backed decision is made, payments to merchants can be executed by the authorised members in the treasury department or can be instructed to the respective acquiring banks/institutions. The relevant records are kept on the server folders. A summary file, containing notes about any held/ released payments, is distributed to all participants. A separate procedure is followed for approval of partial and final payments to merchants.

Once merchant payment amounts are approved, manual work is performed related to the actual remittance of settlements to clients – usually using different banking partners for different transactional entities, or geographical regions. Our correspondent banks usually use SWIFT as the global provider of financial messages.

The treasury team follows different procedures for each set of merchants and several users participate in initialising and authorising the payments, keeping up-to-date beneficiaries' database and reconciling of bank account balances in different online banking platforms. The emerchantpay treasury team maintains relationships with various banking partners and seeks solutions to meet the particulars banking needs.

4. Profit collection

Our company collects its revenue from partnering acquiring banks on a monthly basis. There are two separate approaches, depending on the way the process has been agreed with the particular partner:

- acquiring banks send the revenue calculation together with supporting files, containing the processing breakdown to emerchantpay for their approval. Upon receiving a response from emerchantpay, the bank wires the revenue;
- emerchantpay (ISO) does the revenue calculation, based on data received throughout the month from the acquiring bank and/or data obtained from emerchantpay's gateways. Then, the file is sent to the acquiring bank for their approval and the money is wired.

In some cases, if the acquiring bank does not support the collection of some of the fees which are present in the agreement signed between emerchantpay and the merchant, emerchantpay has to resort to manual collection of these fees with the sending of invoices to merchants. The invoices are usually prepared on a monthly basis and are based on data obtained from the gateways.

5. Agents commission

An agent or a reseller is a merchant service provider (MSP) or an independent sales organisation (ISO), which acquires merchant customers for payment processing services.

All agents have personal buy rates (percentage based) negotiated with emerchantpay. Each agent has their commission worked out depending on:

- negotiated rates; and
- merchant performance like:
  - gross sales;
  - number of transactions.

The agent commissions are calculated on either a weekly or on a monthly basis, depending on the acquiring bank the agents' merchants process through. The agents receive commission on emerchantpay's profit earned on the discount rate, transactions (approved/declined) and refunds. Other items, such as one-time setup fees, might also fall under the agent agreement if additionally negotiated. No commission is earned on chargebacks. The minimum payment amount is 500 units of each currency.

6. Preparing reports

Regular reports prepared by the treasury department are listed below.

Payment overview is prepared in MS Excel and its aim is to show the processing result for one billing cycle. It comprises a spreadsheet with all:

- Settlement due to get paid;
- Gross volume;
- Additionally requested information.

Depending on who provides the billing details, the net settlement figures are provided by either the billing module of IPG, or the acquirer/ APM. The processing data is downloaded from the IPG Gateway.

The result of the processing could be either positive net settlement or negative net settlement. The net settlement itself represents the difference between the gross sales and any deductions such as chargebacks, chargeback fees, transaction fees, refunds and commissions. The net settlement is the amount that is expected to be wired to the merchant, which is obtained from the billing statement or from the acquirer settlement report.

Agents commission report, prepared weekly, and is based on the referred merchant's performance. It displays the agent's final settlement funds, held on the basis of the credit committee's decision.

A processing report is prepared on a monthly basis following the end of the previous month. It is presented in two formats – an Excel spreadsheet with summary of volumes delivered by acquiring banks and APMs, and a word version with feedback on the excel data. Further details on processing volumes are provided on request.

In addition, various planned or ad hoc reports are being prepared by the team – mostly in Excel spreadsheets by gathering and summarising data information from different sources. Most common business information and reporting is provided in the following areas: profitability analysis, costs, portfolio or pricing analysis, banking, beneficiaries, merchant industries and other.

Acquiring bank

ECP, as an acquiring bank, receives funds for merchants' card-based transactions processed through VISA and Mastercard to the respective issuing bank. The funds are received at ECP client accounts and are designated for payments to merchants. For its acquiring and payment services ECP charges different fees which are deducted from the funds received on behalf of the merchants.

ECP's Treasury team provides the following two main functions:

- Payments;
- Cost control.

1. Payments

The ECP payments team provides either daily or weekly settlements to merchants. Daily settlement means that the merchant's billing is done on daily basis (fees and deductions are netted against fund proceeds on daily basis). Weekly settlement means that all fees and deductions are netted against fund proceeds every Tuesday, including all transactions processed over the previous seven days (Wednesday – Tuesday).

Payments are processed with certain days of delay, which is usually seven days, e.g. net settlement worked out on Tuesday this week, will be paid on the next Tuesday.

Payment frequency depends on a few criteria – in particular, the risk level and merchants' needs of working capital.

As e-commerce payments is high-risk activity, to mitigate the credit risk ECP collects rolling reserves as a form of security. The rolling reserve, is a type of cash reserve which withholds a small percentage of all of a merchant's net fund proceeds in a rolling reserve account for a predetermined amount of time (usually 6 months). The funds are then released to the merchant. Alternatively, merchant can place security deposit for a certain amount of time.

Payments are made directly to merchants or PFs. ECP uses different banks and alternative payment providers to effect payments to merchants. Settlement could be in any of the main currencies. Where merchants' settlement currency differs from the merchant's bank account currency, ECP may render brokerage services in order to provide for the desired payment currency.

ECP provides detailed and exhaustive reporting to merchants and partners for processed transactions, fund proceeds, fees charged, deductions and any other adjustments over the settlement period. This is so that merchants and partners can reconcile against their records.

The team monitors debit balances and chase merchants to cover negative positions. The ultimate goal is timely and accurate settlement to all merchants.

2. Cost control

ECP may either approach prospective customer directly or use agents/ resellers for acquiring merchants. If agents/ resellers are in the middle, they are entitled to agent commission. The latter is calculated and paid once per month, based on the commercials as set forth in an agreement between ECP and the reseller.

The ECP treasury team make sure that all rates quoted to partners or merchants are above cost and provide for the margin envisaged by the management. As a member of Visa and Mastercard, ECP incurs different member fees. Therefore, ECP periodically reconciles scheme invoices against the revenue collected from merchants and partners.

In relation to cost control, ECP Treasury department also:

- Manages FX risk on daily basis and make sure that any FX losses are passed on to merchants accordingly;
- Produces number of profitability and performance reports and provides them to management on monthly basis;
- Advises management and partners on changes in scheme fees and member-to-member fees (interchange);
- Produces solutions for calculating transactions cost to support sales team and management in price negotiations with customers.

The ultimate goal is for all merchants to be charged accurately (not under or overcharged), and all costs to be controlled which should ensure stable and predictable operating income.

XI. Product development

PD team acts as a bridge between emerchantpay's Sales and Marketing teams (**Commercial stakeholders**), and Management, Underwriting, Treasury, Risk teams and all other stakeholders (**Operational stakeholders**),on the one hand and **IT Development** team on the other.

1. Management of software products

The Product Development team acts as Technical Product Owner and emerchantpay's Product Expert.

2. Workflow

If it is decided that a new feature, product amendment or an addition to a product is needed in respect of our group's business interest, the Product Development team is responsible for its execution.

Requests are invoked by the sales department, which ensures that every request is properly justified. Product development clarifies the requirements that have to be met in order to implement the solution. For this purpose, the department closely works with the IT to organise the development plan, user acceptance testing and pilot merchant integration.

3. Product Development Flow

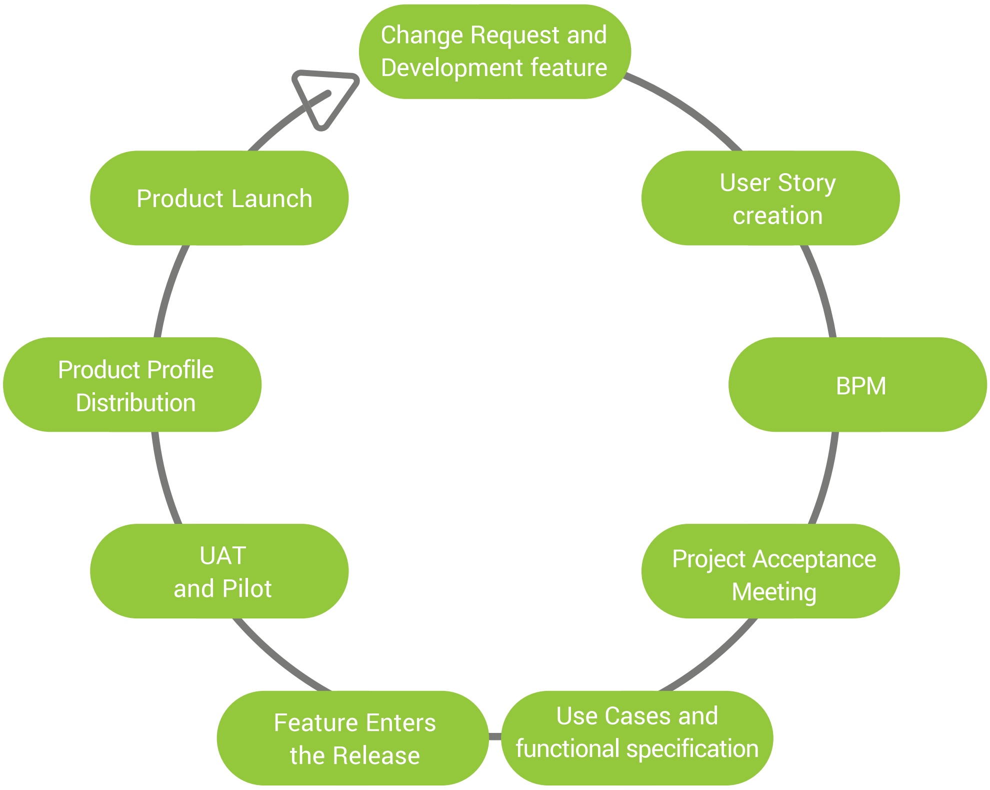

Change Request and Development feature
User Story creation
BPM
Project Acceptance Meeting
Use Cases and functional specification
Feature Enters the Release
UAT and Pilot
Product Profile Distribution
Product Launch

Fig. 25 "PD Workflow"

4. Product Team Information Hub

- All product profiles can be found in Confluence (link).
- Any questions related to existing and/or in progress products (including, but not limited, to APM and acquirers) can be sent to PD@eMerchantPay.com.

5. The Team structure

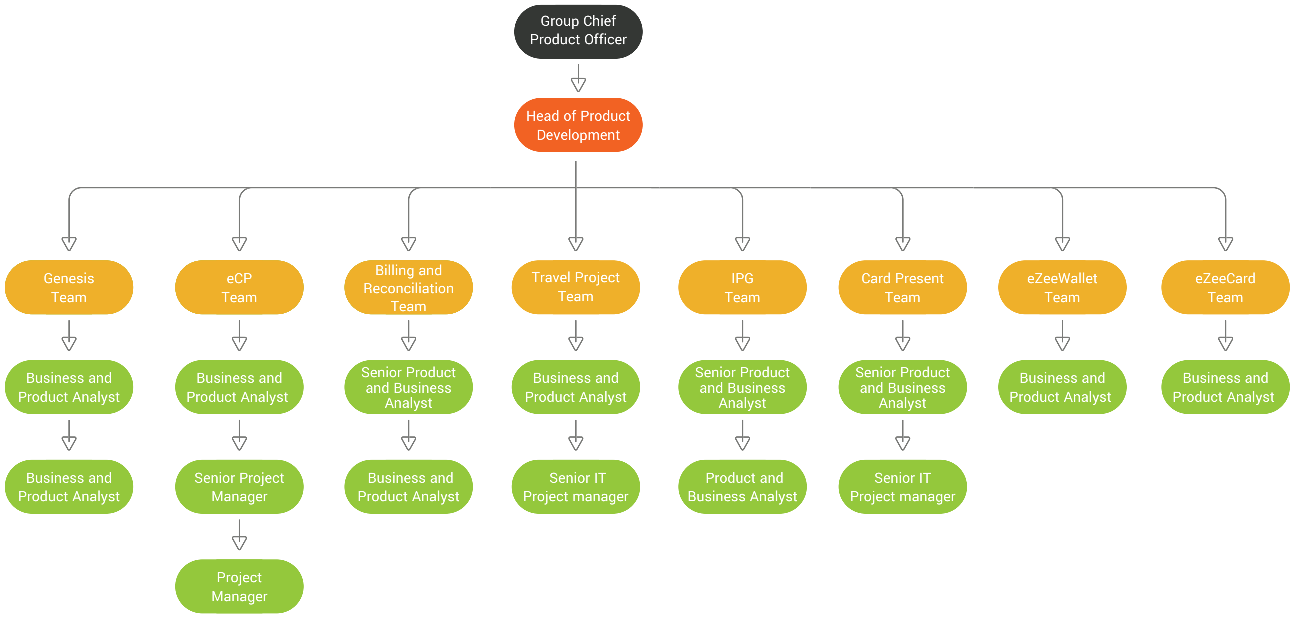

Group Chief Product Officer
Head of Product Development
Genesis Team
Business and Product Analyst
Business and Product Analyst
eCP Team
Business and Product Analyst
Senior Project Manager
Project Manager
Billing and Reconciliation Team
Senior Product and Business Analyst
Business and Product Analyst
Travel Project Team
Business and Product Analyst
Senior IT Project manager
IPG Team
Senior Product and Business Analyst
Product and Business Analyst
Card Present Team
Senior Product and Business Analyst
Senior IT Project manager
eZeeWallet Team
Business and Product Analyst
eZeeCard Team
Business and Product Analyst

Fig. 26 “The team structure of PD”

XII. Legal & Compliance department

Introduction

1. À propos

Our legal and compliance (“LC”) department is separated into two interconnected department units – legal unit and compliance unit.

The department within emerchantpay is on a group level, meaning it serves all business units.

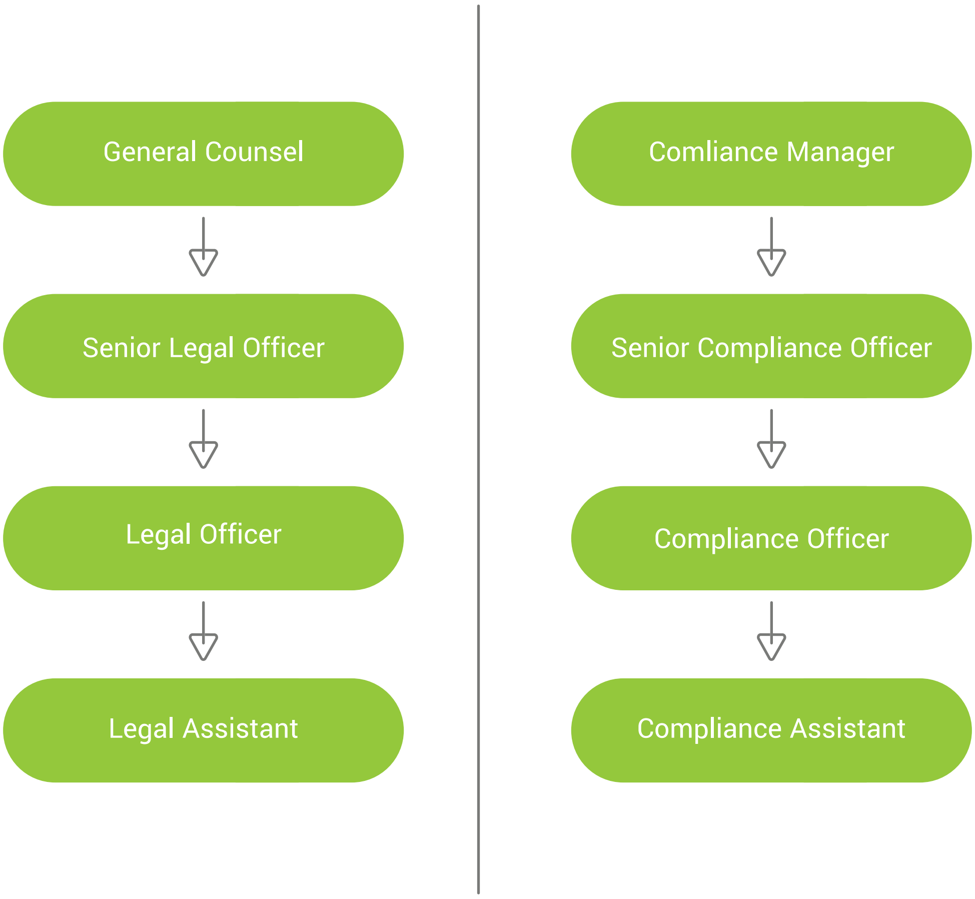


Fig. 27 “LC Department hierarchy”

2. Objectives

The main objectives of our LC department are as follows:

- **identification** –identify the risks that an organisation faces and advise on them;
- **prevention** – design and implement controls to protect an organisation from those risks;
- **monitoring and detection** – monitor and report on the effectiveness of those controls in the management of an organisations exposure to risks;
- **resolution** – resolve compliance difficulties as they occur;
- **advisory** – advise the business on rules and controls.

The LC department is using a two-staged method in order to meet its objectives. We develop and implement such internal policies and procedures as to comply with all external legislation and rules imposed on our group as to remain fully compliant and mitigate the risks of exposure.

In essence, we operate on these two levels:

- **Level 1** – external compliance – development and implementation of policies and procedures satisfying the requirements deriving from legislation, regulations, rules and standards applicable for our business activity;
- **Level 2** – internal compliance – being

abreast with environmental change and updating policies mutatis mutandis,

making sure that our employees abide by the internal policies and procedures.

Activities

emerchantpay’s overall risk-taking activities are managed, with respect to its business risk appetite, by using three lines of defence:

- business line (this is the first line comprising operational management);
- risk line (second line of defence, comprising risk management, compliance and money laundering reporting officer);
- third line (internal audit line).

Due to the two-pillar structure of our LC department, the responsibilities are also divided as follows:

Legal unit works in partnership with the business line and is responsible for:

- policy making – establishing written guidance to staff members through policies, codes of conduct, manuals, etc; advising senior management engagement efforts on key procedures developments related to the workflows and business processes in their respective departments/units;
- advising on legislation – in respect of proposed and existing regulations and insights into emerging best practices and legislative initiatives, on whether and how strategic and business model considerations are likely to satisfy the supervisors’ judgements about the fair treatment of customers, market integrity, financial soundness, etc.;
- relationship management – liaison with relevant external bodies, including regulators, standard setters and external experts.

Compliance unit acts purely as a second line and will cooperate with third line of defence, being responsible for:

- contact point – within the firm for compliance issues;
- tutor – to educate staff, to keep employees abreast of industry regulatory and legislative developments and provide them with respective trainings, to ensure they are versed with the technicalities and complexities of the functions they perform;
- monitoring – compliance with policies and procedures and conducting investigations on alleged breaches;

MLRO

1. À propos

Along with the fast-growing payments industry, the legislation in respect to anti-money laundering is accordingly expanding its arsenal with new mechanisms to battle money laundering.

One of these mechanisms is the newly-implemented obligation for financial institutions to appoint a money-laundering reporting officer.

The MLRO position within our company is not involved with any department. It is independent and communicates only with senior management.

2. Objectives

The MLRO's main objectives are as follows:

- vigilance over business activity;
- duly reporting suspicious transactions to the competent authority;
- key liaison with the FIU;

The MLRO within our company is a credible and respected professional, with history and vast experience in payments.

3. Key obligations

The key MLRO obligations are:

- receiving and considering reports from employees, about activities and transactions, giving rise to knowledge or suspicion of money laundering or terrorist financing;
- making onward reports to the competent FIU;
- making annual reports to our senior management;
- taking reasonable steps to establish and maintain adequate arrangements for awareness and training.

More information about how to report to the MLRO if you notice suspicious activity in relation with money laundering and terrorist financing you can find in our "Reporting Procedures", available in confluence (link).

XIII. Operations

Operations management

In our company, we have operations managers appoint to each of the business units – acquiring bank, ISO, EZW and EZC. Their responsibility is the maintenance of the working process in the respective unit and are communicating directly with the COO.

The COO of the company is also supervising the HR and Administrative Department.

HR and Administration

Within our firm, human resources is responsible for employee headhunting, retention and satisfaction. This includes organisation of interviews with potential employees, organising teamwork events and other employee retention events. It also includes keeping our company socially responsible and active within the community in situ.

Our administration team is responsible for the internal atmosphere and day-to-day administrative tasks. They are responsible for the employee private information, labour contracts and employee comfort at the working place.

XIV. Commercial department

The sales department is working on a group level. It is the initiator of merchant relationship. We can say that our sales agents are the representatives of our company to the world. Each sales agent is responsible for merchant solicitation and they are the reason behind subsequent on-boarding. With other words a sales agent triggers the process of onboarding.

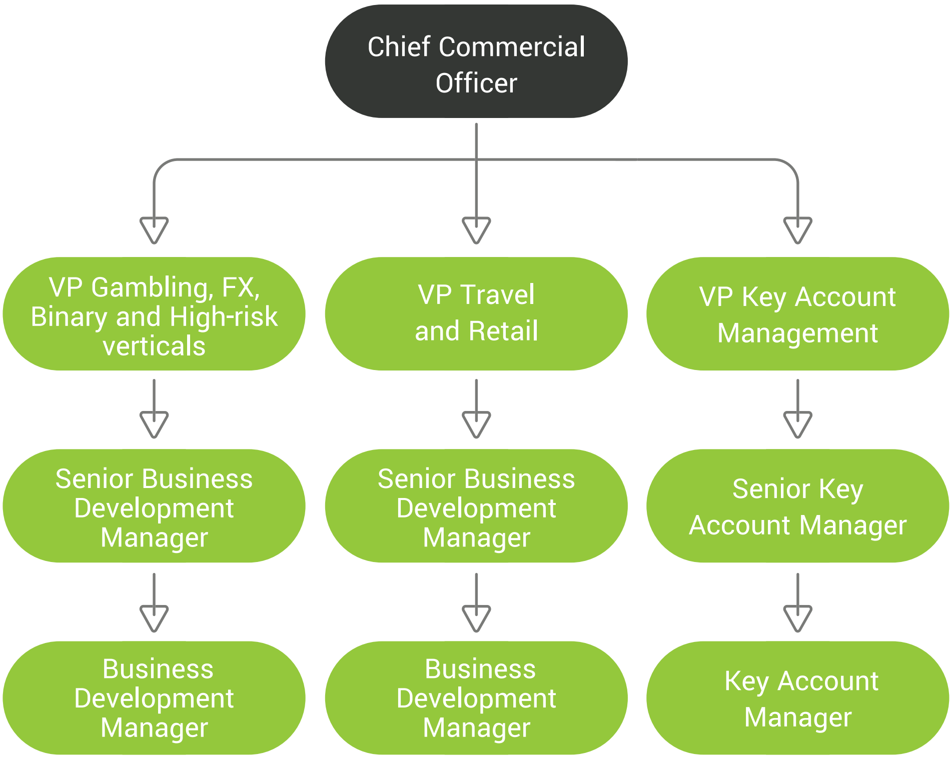

Chief Commercial Officer
VP Gambling, FX, Binary and High-risk verticals
VP Travel and Retail
VP Key Account Management
Senior Business Development Manager
Senior Business Development Manager
Senior Key Account Manager
Business Development Manager
Business Development Manager
Key Account Manager

Fig. 28 “Commercial Department hierarchy”

Sales and marketing executives are directly involved with customer solicitation. The main purpose of the latter is to make the firm`s product and services known to the public and to form the initial relationship with potential customers. The firm`s sales and marketing executives are also responsible for the retention of customers and their satisfaction with the firm`s services. The sales and marketing functions are outsourced to EMP UK.

XV. Marketing and communication department

Introduction

1. Team structure

Our marketing department works on a group level and is structured as per the below:

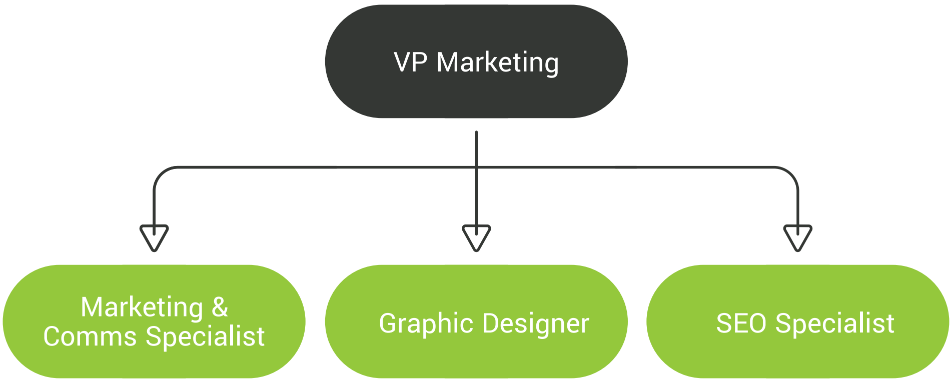


Fig. 29 “Marketing and communication Department hierarchy”

2. Objectives

The marketing team is a cross-department support function responsible for the emerchantpay brand and its entities. Its primary objectives are to increase brand awareness, enable sales and customer acquisitions and to help increase the share of wallet of the existing customer portfolio.

The team is responsible for all external communications and the overall emerchantpay suite of assets on both content and design fronts. Final approval of all externally-facing material whether content, design or both, is the responsibility of the Marketing VP. It is advised that all emerchantpay employees familiarise themselves with our PR and social policies. This and more can be found in Confluence, under the brand centre folder, as well as industry related material available the on the insight section of our website.

Activities

- Manage day-to-day design requirements/ requests;
- Manage and support UX design related work on the emerchantpay digital applications;
- Maintain, manage and remain active across all the emerchantpay social outlets to increase followership;
- Build thought leadership content in the form of news items and whitepapers;
- Manage the emerchantpay brand image through PR related activities including but not limited to: by-lines, press releases, press liaison, news hijack, publication pitch and working to secure interviews/quotes with press;
- Create, manage and deliver all external content including but not limited to: blogs, articles, case studies, social posts, web and digital content;
- Develop, design and deliver product collateral as well as branded merchandise and flyers;
- Manage, negotiate and execute all event sponsorships and attendee events;
- Manage, create and execute product campaigns and external promotions in relation the emerchantpay proposition as a whole;
- Manage SEO practices and procedures to increase traffic and ranking;
- Closely work with the various teams/ department within the business including the salesforce and webservices teams.

XVI. Sources

1. PYMNTS. “Just The (Pay) Facs, Please”, published on 13th May 2016, available at link;
2. Susan Herbst-Murphy. “Clearing and Settlement of Interbank Card Transactions: A MasterCard Tutorial for Federal Reserve Payments Analysts”, published October 2013;
3. Gulati, Ved Prakash. “The Empowered Internet Payment Gateway”, Computer Society of India, retrieved 22 May 2013;
4. Chargebacks911. “Payment Reversal”, published on 7th September 2017, available at link;
5. eMP Compliance Department. “The Payment Ecosystem”, presentation published November 2017, available at link;
6. eMP Compliance Department. “Virtual Currencies”, research published July 2017, available at link;
7. eMP Compliance Department. “Online Marketplaces”, research published January 2018, available at link;
8. eMP Group. “AML/CTF Policy”, last updated August 2017, available at link;
9. eMP Group. “Industry Policy: Digital Wallets”, last updated January 2018, available at link;
10. eMP Group. “Industry Policy: Virtual Currencies”, last updated January 2018, available at link;
11. MasterCard. “MasterCard Rules”, published on November 2016;
12. Visa. “Visa Core Rules and Visa Product and Service Rules”, published on April 2017.

emerchantpay

Copyright © 2018, emerchantpay ltd. emerchantpay limited is registered as an Authorised Electronic Money Institution with Financial Conduct Authority (FCA United Kingdom).emerchantpay is part of emerchantpay group. emerchantpay limited is a principal member of VISA and MasterCard and an acquirer in its own right. emerchantpay corporation is a registered ISO/MSP of Elavon, Inc. Atlanta, GA, a wholly-owned subsidiary of U.S. Bancorp.