POS card acceptance manual

Any transaction - any way **EMSpay.nl/en**

EMS

A First Data & ABN AMRO company

Contents

1. Introduction

EMS provides the processing and payment for the transactions that you accept with Visa, MasterCard, Diners, Discover, UnionPay, JCB, Foreign Maestro card, V PAY, and Bancontact cards. In order to provide you with the best possible service, we have set out all the important information for you in this manual. This manual forms part of your contract with EMS. We would ask you to read the manual carefully and then store it in a central location near your till and/or payment terminal. That way you will be sure that you have the right information to hand in the event of queries.

2. How to recognise a valid credit card

Before accepting a card, you must check that it is valid. It is easy to check the validity because all cards have standard characteristics. It is also important that you only accept cards that have been authorised by us and for which you have signed an Acceptance Contract with us. In addition, you must always process a transaction using the EMV chip. Only if the payment terminal then indicates that the magnetic strip should be used can you use the magnetic strip.

A card is strictly personal, and only the cardholder themselves may use the card. A card with no signature or more than one signature on the signature strip is not valid.

The summary below lists the most important characteristics for you.

Visa card
Characteristics of the Visa card:

1. The logo can appear in various positions on the card, both horizontally and vertically.
2. If you examine the Visa logo under UV light, the letter 'V' will be visible.
3. The Visa dove appears in the middle of the card under UV light.
4. The EMV chip. This chip is read by inserting the card in the payment terminal, after which the payment is completed. This is more secure than using the magnetic strip.
5. Visa magnetic strip. The Visa hologram with the dove can be located both on the front or in the magnetic strip or another position on the back of the card.
6. CVV2 code (Card Verification Code): the security code that is located on the signature strip. The security code can now also be located next to the signature strip instead of on it.

Visa Electron card
The Visa Electron card is a Visa card that can only be used for electronic transactions using a payment terminal and/or ATM. Every transaction is then checked, authorised, and processed immediately by the Visa systems. There are now over 394 million Visa Electron cardholders worldwide. The authenticity of this Visa card can also be checked easily using a number of standard characteristics.

Characteristics of the Visa Electron card:

1. The logo can appear in various positions, both horizontally and vertically.
2. If you examine the Visa logo under UV light, the letter 'V' will be visible.
3. The EMV chip.
4. Visa magnetic strip with hologram.
5. Signature strip and CVV2 code: the security code (CVV2) can also be located next to the signature strip instead of on it.

A sales transaction with the Visa Electron card:
This may only be performed using a payment terminal and/or ATM. Visa Electron cards may not be accepted manually, because all the data is incorporated in the card's EMV chip and is therefore not embossed on the card.

- If there is a problem the cardholder needs to use another payment method.
- The Visa Electron card's chip must always be read by the payment terminal. You may not key in the card number (if it is legible).
- A code is displayed with a rejected transaction. If you have any questions about the reason for the rejection, please contact our Client Services department using our contact form, or take a look at our support page www.emspay.nl/en/support

V PAY card
Characteristics of the V PAY card:

1. EMV chip.
2. V PAY logo. The logo can also appear in a different position on the front of the card.
3. UV light. If you examine the new V PAY logo under UV light, the letter 'V' will be visible.
4. Flat card. The card number is not embossed on the front.
5. Magnetic strip. The hologram with the dove may be optional on the magnetic strip.

All V PAY cards contain a chip. When paying with a V PAY card, the cardholder is asked to enter a PIN. This ensures a more secure payment for everyone.

MasterCard
Characteristics of the MasterCard:

Front

1. The MasterCard logo can appear in various positions on the card, both horizontally and vertically.
2. The hologram with the globes (silver or gold). Check the hologram for damage, because this can indicate that the card has been tampered with.
3. The card number always begins with the number 5 (five) or 2 (two).
4. The card number contains 13 or 16 digits, the last three or four of which are embossed in the hologram. Check that the numbers on the card are the same size, height, and style, and whether they are aligned.
5. The first four digits of the card number match the preprinted numbers on the card.
6. 'Valid thru': The date up to which the MasterCard is valid is embossed below this. After this expiry date the MasterCard can no longer be accepted (up to the last day of the month in question).
7. EMV chip.

Back

8. The magnetic strip.
9. The cardholder's signature must always appear on the back of the card. The strip on which this signature is placed must be undamaged and printed diagonally with the text 'MasterCard'. The signature strips on most current cards have a new characteristic: the strip changes colour if it is tampered with. The signature on the back of the card must match the signature on the sales voucher.
10. The security code: these are the last three numbers on the signature strip on the back of the card. This code is called the CVC2 code, which stands for Card Verification Code.

Foreign Maestro card

The foreign Maestro card is a card that can only be used for electronic transactions using a payment terminal and/or ATM. Every transaction is then checked, authorised, and processed immediately by the Maestro systems. The authenticity of this card can also be checked easily using a number of standard characteristics.

Characteristics of the foreign Maestro card:

Front

1. EMV chip
2. Card number or bank account number (both can appear on the card)
3. Cardholder's name
4. Expiry date
5. Maestro Logo. The logo can also appear in a different location on the card.

Back

6. Cirrus brand name. Does not need to be present.
7. Logo of the acceptance mark
8. Signature strip
9. Magnetic strip

A sales transaction with the foreign Maestro card:

This may only be performed using a payment terminal and/or ATM. Foreign Maestro cards may not be accepted manually, because all the data is incorporated in the card's chip and is therefore not embossed on the card. If there is a problem the cardholder needs to use another means of payment. The foreign Maestro card's chip must always be read by the payment terminal. You may not key in the card number (if it is legible). Make sure that the foreign Maestro card that is presented matches the characteristics listed. In the event of doubt please contact our Client Services department.

UnionPay card

Characteristics of the UnionPay card

Front

A. Card number, 16 or 19 digits.
B. Cardholder's name (on some UnionPay cards the cardholder's name is not shown on the card. However these cards are still valid).
C. Expiry date, the embossed date up to which the credit card is valid. After this expiry date the credit card can no longer be accepted (up to the last day of the month in question).
D. UnionPay logo. The card can display an old type of logo (only Chinese lettering) or a new logo (see example).
E. The card may also be equipped with a chip on the front. If this is present, the chip must be used. Important credit card data is stored on this chip.

Back

F. The cardholder's signature must always appear on the back of the card. The signature on the back of the credit card must match the signature that the cardholder signs on the sales voucher. If there is a discrepancy, the card may not be accepted.
G. 24-hour Customer Service Hotline, the number for UnionPay's 24-hour customer service line
H. 24-hour Customer Service Hotline, the overseas number for UnionPay's 24-hour customer service line.
I. Last 4 digits of the credit card number. These 4 numbers must match the last 4 digits on the front of the credit card.
J. CW2 Code, the security code: these are the last three digits of the number on the signature strip on the back of the card.
K. UnionPay credit cards always feature a hologram on the front or on the back. This hologram is not present on a UnionPay debit card.
L. The magnetic strip.

Diners Card
Characteristics of the Diners Card:

Back
- The card has a holographic magnetic strip and the symbols on the magnetic strip change if it is tilted.
- Is there an undamaged signature on the back of the card, and is 'Diners' repeated multiple times in the signature field?
- Are the full card number or the last four digits of the card number shown in the signature field followed by the three-digit security number?

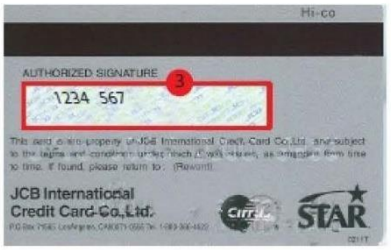
Front
- Is the card neatly printed, free of discolouration or other deviations?
- Cards where the card number and the expiry date are printed on the front of the card should only be used using the EMV chip, and no imprint may be taken of them.
- Do the last four digits of the card match the last four digits recorded on the sales voucher?
- Does the signature on the sales voucher match the signature on the back of the card?

Discover card
Characteristics of the Discover card:

Front
- Is the card neatly printed, free of discolouration or other deviations?
- Do the last four digits of the card match the last four digits recorded on the sales voucher?
- Does the signature on the sales voucher match the signature on the back of the card?

Back
- Does the card have a holographic magnetic strip and do the symbols on the magnetic strip change if it is tilted?
- Is there an undamaged signature on the back of the card, and is 'Discover' repeated multiple times in the signature field?
- Is the three-digit security number shown in the signature field?

JCB card
Characteristics of the JCB card:

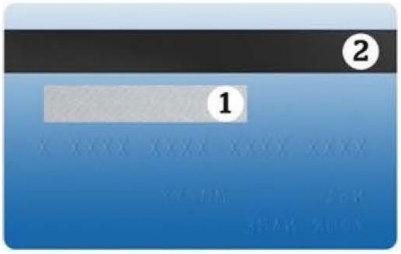


logo 1

logo 2

1. The card must feature the hologram and the JCB logo on the front;
2. and an embossed J
3. The signature field on the back features the text 'JCB' and an authentication number.
4. The card can feature 2 different JCB logos

Bancontact card
Characteristics of the Bancontact card:



Front
1. The card number is a number made up of 17 digits
2. The card's expiry date in month and year (2 digits for each)
3. The cardholder's name (in capital letters)
4. The chip on the card is used by a payment terminal's card reader or your bank's card reader

Back
1. The zone for the cardholder's signature
2. The magnetic strip

3. Acceptance using the payment terminal

Accepting cards using the payment terminal is quick, cheap, easy, secure, and customer-friendly. Virtually all payments terminals that accept debit cards are also suitable for accepting credit cards and foreign Maestro and V PAY cards. This chapter tells you all about electronic card acceptance. For information about how to operate your payment terminal, please see your payment terminal's user manual. It is important that you have this manual in your possession and that your employees are informed about error and/or fault messages.

Accepting transactions

1. Check the characteristics of the card. Only continue if you are satisfied with the checks. After all, your payment terminal does not carry out all the required checks.
2. Place the card in the payment terminal's chip card reader. If the payment terminal cannot read the card or a fault has occurred with the payment terminal, please read the 'procedure in the event of a fault with the payment terminal' later in this chapter.
3. Enter the amount and check whether the transaction has been approved.

4a If the card has a chip, this must be read in the chip card reader.
The customer must then enter their PIN. The sales voucher does not need to be signed and does not need to be kept. If the payment terminal does produce a sales voucher with a request for signature, ask your customer to sign on the sales voucher as verification. Check the signature against the signature on the back of the credit card. You should keep this voucher in case there is a dispute later.

4b If the card does not have a chip, the card can be read using the magnetic strip. The customer must enter their PIN. If the terminal does not ask for a PIN, the cardholder must sign the sales voucher.

5. Retain the original voucher (for at least 18 months as requestable proof of your transaction) and give the copy to the cardholder.
6. Only then should you return the card to the cardholder.

Authorising transactions

The request for an authorisation (approval) for a card payment via an online payment terminal happens automatically. You therefore do not need to do anything.

The authorisation is given

Follow the instructions on the payment terminal, since these differ according to the payment terminal.

The authorisation is refused

In order to safeguard the cardholder's privacy, EMS will never tell you the reason for refusal over the phone. In that case you can ask the customer to use another means of payment.

If a cardholder cannot remember their PIN:

1. Remind the cardholder that it may be the same PIN that they used to withdraw cash from an ATM.
2. Remind the cardholder that they can contact the card-issuing bank for help.
3. If the cardholder cannot remember their PIN code the cardholder needs to make payment by other means.

Submission of accepted transactions

The card transactions via a payment terminal are automatically submitted to EMS because the payment terminal has a direct link to our systems. You therefore do not need to send off the signed sales vouchers, but you should keep them for at least 18 months in case of chargebacks. You will also receive payment for the transactions automatically.

Cancelling card transactions

You may need to cancel a transaction in full or in part. In some cases you can cancel the transaction on the spot by cancelling the transaction on the payment terminal. This can only be done on the same day and for the full amount if your payment terminal is set up for this. Please consult your payment terminal's manual for this. In the case of a partial cancellation or cancellation on a day other than the day on which the transaction took place, you must cancel the transaction using a refund. Please consult your payment terminal's manual for this.

If you have entered a cancellation for a transaction on your payment terminal, this will be submitted to us automatically via the systems. You do not need to send us anything else.

If the payment terminal cannot read the card, you can follow the following procedure:
- Always use the EMV chip by inserting the card in the chip card reader.
- You could also ask the cardholder to pay by other means.

After EMS has processed your transactions you will receive payment for them within the agreed number of working days.

4. Payment

We will list all information about the transactions—such as quantity, gross amount, commission paid, and date—on the bank statement. You will therefore not receive a hard-copy itemisation from us. You can find detailed information and various reports about your transactions in our online reporting tool. For further information please see www.emspay.nl/en

Queries about payments
We would ask that you notify queries about payments to EMS in writing or by phone as soon as possible, and definitely within three months of the credit card transaction in question. You should always include your merchant number.

5. Retrieval requests & chargebacks

This chapter describes the procedure that you must follow for retrieval requests and chargebacks. It also contains tips that can help you to avoid chargebacks.

Do not forget that you are responsible for chargebacks, even if you have been given authorisation for a transaction. See Clause 25.2 in our General terms and conditions.

A cardholder has the right to ask about a transaction. The cardholder can also indicate that they do not agree with the transaction. These requests will always be submitted to EMS via the card issuer, and can be submitted (in most cases) up to 180 days after the transaction has been debited from the cardholder's account. A transaction is only completed when all the goods or services have been delivered and the 18 months therefore apply from this date. We therefore recommend that you always retain the original documents for at least 18 months.

Retrieval requests
A cardholder may always request a sales voucher to verify that a transaction actually took place. The cardholder will notify this to their bank. The bank submits the retrieval request to EMS. EMS will then ask you for a copy of the sales voucher showing the transaction in question. We will send you this request by e-mail or by post according to your preference. However you bear the risk of the post not arriving. We therefore recommend that you communicate about a retrieval request by e-mail.

This e-mail/letter will ask you to send us the relevant copy of the sales voucher within 7 days. You are responsible for sending this copy of the sales voucher to us within this period.

If for any reason you are unable to provide copies of the requested information, you will risk a chargeback of the transaction in question. If the card issuer makes a chargeback because of the failure to provide the requested documents in time, this cannot be undone by submitting the documentation later. It is therefore extremely important that you reply to and/or resolve a retrieval request as soon as possible because of the time limits imposed by Visa, MasterCard, Diners, Discover, JCB, and UnionPay. The more information we have available to us, the better we can protect your interests. We recommend that you include all documents relating to the transaction (e.g. associated invoices/purchase notes) as proof of the transaction, including all documents signed by the cardholder.

Differences between a retrieval request and a chargeback

A retrieval request does not have direct financial consequences. Only if a chargeback is actually submitted on the basis of the retrieval request can there be financial consequences for you such as the disputed amount, scheme costs, and EMS's costs. This depends on whether the bank accepts the information provided by you, the reason for the chargeback, the costs that the scheme charges, and the costs that you paid to EMS (if a chargeback is lost).

Chargeback

If we receive a chargeback from a card issuer we will inform you of this by means of an e-mail notification. If EMS can challenge the chargeback you will receive a letter giving the reason for the chargeback and what information we need from you in order to actually be able challenge the chargeback with the bank. We will also provide the transaction details so that you can trace the transaction (more) easily in your records. You then have 7 days to provide the requested information.

If the information provided by you is adequate and received within the permitted time limit, we will defend the chargeback for you where possible. This depends on the rules stipulated by Visa, MasterCard, Diners, Discover, JCB, and UnionPay. You will then receive no notification from us.

If the information is not adequate, we will contact you to ask you to provide the missing documents.

If this is still not adequate, we can unfortunately not defend the chargeback for you, and you will have to pay the chargeback costs. Obviously we will do everything possible to avoid this.

Read through the example situations below. These described the most common reasons for chargebacks and how they can be avoided.

Reason	How to avoid chargebacks
Cancellation not processed—the cardholder claims the transaction should have been cancelled/refunded.	Make sure that your refund and/or cancellation is processed immediately. Refunds must be made to the same card number that the cardholder used for the original purchase. Do not make refunds in cash or cheques.
Transaction not authorised.	Authorise all transactions and use the correct authorisation method.
The accepting merchant does not respond to requests for a copy of the sales voucher.	Ensure clearly legible duplicate sales vouchers and store them in a secure and orderly way so that you are able to respond to retrieval requests within the required time limit.
The cardholder does not agree with the transaction because the amount has been debited twice.	If you notice afterwards that you have received a double payment, it is important that you make a refund within 14 days. Otherwise the cardholder can initiate a chargeback, and this can involve more costs.

6. Secure acceptance

Accepting credit cards via a payment terminal is quick, secure, and efficient. But there may still be an attempt at fraud at your business. The guidelines below can help you assess whether a transaction is suspicious or not. It is important that you and your personnel read, understand, and apply these guidelines about accepting credit cards.

How can I identify a potentially fraudulent transaction?

- The person offering the card does not ask about the price of goods and is buying products that can easily be sold on;
- The purchase amount is much higher than your average purchase amount (e.g. you usually sell for an average amount of € 40 per transaction and this is a purchase for € 400);
- The customer takes a long time to place their signature on the sales voucher;
- The customer has one or more credit cards casually loose in a jacket or trouser pocket instead of in a wallet;
- The customer tells you that they have already had problems earlier with the credit card being accepted and ask you to try again for a lower amount;
- The customer asks you to split the amount into portions or to divide the amount across different cards.
- The customer comes back to you several times in a short period, possibly with different credit cards.
- Even if the customer has entered a PIN they can still be required to sign the sales voucher. You should therefore always check the sales voucher carefully.

The situations described above can indicate a fraudulent transaction. If the offered credit card look suspicious or the person offering the card shows unusual behaviour (irritated/hurried/nervous), do not hesitate to contact our Client Services department. For more information about recognising and preventing fraud please visit our website www.emspay.nl/en/support

Other important information about fraud

- An authorisation code merely shows that the cardholder's credit is available and that the card was not blocked at the time of the transaction. The PIN does not guarantee that the person using the card is the legitimate cardholder.
- Do not process transactions for businesses other than your own business. Some fraudsters offer money for processing transactions.

Fraud prevention

In order to protect your business against financial losses it is very important that you and your personnel comply carefully with the contents of this manual at all times. If you are the victim of a fraudulent transaction, we will do everything possible to help prevent you from suffering financial loss. But often the results are dependent on the degree to which you have followed and complied with the procedures and guidelines contained in this manual.

If you think that your business is vulnerable to attempted fraud, possibly because of the nature or location of your business or because you have heard it on the grapevine, please contact us and ask for the Risk department. They are happy to help you with advice on preventing fraud.

In order to be able to provide you with the best service, it is important to comply with a number of basic rules stipulated by Visa, MasterCard, Diners, Discover, UnionPay, JCB, and Bancontact.

- If you have entered into a Cards Acceptance Contract, you are required to display the logos of Visa, MasterCard, Diners, Discover, UnionPay, JCB, and Bancontact in a clearly visible place so that your customers know which cards you accept.
- You are not permitted to use the logos of Visa, MasterCard, Diners, Discover, UnionPay, JCB, and Bancontact card in such a way that it gives the impression that these companies recommend your goods and services.
- You may not charge a fee for card payments.
- At least one copy of the sales voucher must be given to the cardholder.
- You may not stipulate any special conditions for accepting a card, such as minimum or maximum spends.
- You cannot carry out a transaction or sale for which a chargeback has been made in the past.
- You are not authorised to accept transactions for third parties and/or to give cashbacks unless you have obtained express written permission for this from EMS.

7. Inform us about changes in your business details

It is important that you keep EMS informed about all changes within your business. It is particularly important that you inform us of the following changes:

1. Change of address.
2. Closure of the business or change of owner; you cannot pass your Acceptance Contract on to someone else under any circumstances without EMS's written permission. If you do not inform us that you no longer own a business, you will still remain liable for any debts incurred by the new owner.
3. Changes in your business relating to the legal form and/or signing powers.
4. Change of Chamber of Commerce number.
5. Change of products or services offered; when you join EMS you must provide us with details of the various products that your business offers so that we can categorise your business accordingly. It is therefore important that you inform us in writing if the nature of your business changes, for example if a product or service changes or if you expand your activities with activities in another sector.
6. Change in the method of accepting credit cards. If you wish to change your acceptance method either to 'Cardholder Not Present' or to 'Acceptance via the Internet', you must request a separate Acceptance Contract for this from us.

You must notify all these changes to us in writing, and always quote your merchant number. Our website http://www.emspay.nl/en provides standard forms that we have developed for the most common changes.

8. Payment Card Industry Data Security Standard

The Payment Card Industry Data Security Standard (PCI DSS) is a globally required security standard that is provided by the credit card companies to protect and secure card payment data. Any entity that collects or stores card payment data is responsible for the protection and storage of that data. Failure to comply with this standard can have serious consequences, including possible fines and penalties from the card organisations. In some cases they may even withdraw your right to accept credit cards. You are obliged to inform EMS immediately of the identity of any third party that you use or wish to use to process and/or store card payment and account data, either directly or indirectly, regardless of the method or duration of such activities. Such parties are called Data Storage Entities (DSE) and must also comply with PCI rules.

PCI DSS offers a coordinated approach to the protection of sensitive data for all card types and meets the need for streamlined requirements for the entire payment industry. EMS offers its merchants a PCI DSS programme at a heavily discounted rate. The PCI DSS Protection Programme enables merchants to easily comply with the PCI DSS standard. For more information about the EMS PCI DSS Protection Programme, please visit our website www.emspay.nl/en

Card organisations must ensure that all outlets and businesses that store, process or send card data comply fully with the PCI standard and that this is regularly tested.

MasterCard PCI Rules

MasterCard can impose fines in the following situations.

- Fine for (ongoing) failure to comply with the PCI standard.
  The fine starts at USD 5,000 or USD 25,000 depending on the number of transactions that an outlet or business accepts annually. If there is ongoing failure to comply with the PCI standard, MasterCard can impose additional fines. MasterCard can also stipulate that the outlet or business can no longer accept MasterCard transactions.
- In the event of the theft of card data if an investigation reveals a failure to comply with the PCI standard. Even if the merchant refuses to cooperate with the investigation as a result of the theft. The fine is determined by the characteristics of the card data that has been stolen.

If the merchant does not cooperate in accordance with MasterCard's guidelines and timescales, MasterCard can impose an additional fine of USD 25,000 per day until the rules have been fully met. These rules also include the obligation to report the theft. MasterCard can recover all investigation costs and other related costs. In addition, the card issuers can charge a fee of USD 25 per card for the cards that have been compromised by the theft. Any waiver of (part of) the fines is entirely at MasterCard's discretion. If the outlet or business was not compliant with the PCI standard at the time of the theft, there will be no waiver. MasterCard can also stipulate that the outlet or business can no longer accept MasterCard transactions.

Visa PCI Rules

Visa can impose fines in the following situations.

- (Ongoing) failure to comply with the PCI standard. The fine starts at USD 5,000 and can rise to USD 25,000 per month as long as the failure to comply with the PCI standard continues.
- In the event of the theft of card data if an investigation reveals a failure to comply with the PCI standard. If the merchant refuses to cooperate with the investigation as a result of the theft. A fine is imposed depending on the number of cards compromised by the theft. The fine starts at USD 2,500. After 90 days it becomes USD 5,000. After 4 months it is USD 10,000. After 5 months it is USD 15,000. After 6 months the amount is fixed at USD 15,000 per month until the situation within a business is resolved. In the event of the theft of card data, fraud perpetrated with stolen card data can also be reclaimed from the business.

9. Important addresses and contact information

For all your questions

Website:	https://emspay.nl/en
Contact form:	https://emspay.nl/en/contact-us
Support environment	https://emspay.nl/en/support
E-mail:	contact@emspay.eu

Correspondence address

European Merchant Services
P.O. Box 22764
1100 DG AMSTERDAM
The Netherlands

Appendix A - Card organisations' rules and provisions

MasterCard, Visa, Diners, Discover, UnionPay, and JCB have drawn up rules aimed at protecting and enhancing the integrity and reliability of payment traffic. If these rules are not followed, a number of procedures will take effect and they reserve the right to impose fines.

The most common fines are listed in this appendix. It does not offer a comprehensive list of all the fines applied by the card organisations. If you would like further information, please contact EMS.

MasterCard rules in the event of a chargeback

MasterCard reserves the right to impose fines if an outlet or business has:

- a percentage of chargebacks of 1.50% or higher during 2 successive months;
- the number of chargebacks is at least 100.

The percentage is calculated on the basis of the number of chargebacks in a month multiplied by the number of transactions in the previous month.

EMS is obliged to register the business or outlet with MasterCard. MasterCard charges a fee of USD 500 and a monthly fee of USD 100 for the registration. The registration remains in force until the percentage and/or the number of chargebacks for the business or outlet is less than 1.50% or 100 chargebacks during two successive months.

The registration period also applies as the liability period—the period within which MasterCard may impose penalties.

MasterCard penalty clause if rules are breached

MasterCard has two types of penalty that it can impose (concurrently). This involves a payment to the card issuer and a fine payable to MasterCard itself.

The calculation takes place from the first month of the breach, and the fines apply throughout the general liability period.

The level of the penalties is calculated per month as follows.

- Card issuer payment: this is the total number of chargebacks above the percentage of 1.50% x (times) 25 USD (so the number of chargebacks below the percentage of 1.50% are not included).
- Fine payable to MasterCard: this is the total amount of the payment to the card issuer x (times) the total percentage in that month (is therefore at least 1.50%).

The total fine amount per month is the sum of the payment to the card issuer and the fine payable to MasterCard. The amount can be increased if MasterCard suspects or has proof that the business or the outlet has knowingly initiated credits in order to prevent chargebacks. All credits will then be viewed as chargebacks and included in the calculation of the fine.

Visa rules for chargebacks
Visa reserves the right to impose fines if the following results occur at a business or outlet:

- the percentage of non-domestic chargebacks during 1 month is 1% or higher.
- the number of chargebacks is 100 or more.

The percentage is calculated on the basis of the number of chargebacks in a month divided by the number of transactions in the following month.

Visa penalty clause if rules are breached
Visa imposes a fine of up to € 85 per chargeback for every month that the ratio specified above is breached.

In addition, if it cannot be satisfactorily shown that the business or outlet has taken steps to reduce the number of chargebacks, Visa reserves the right to increase the penalty per chargeback and impose a supplementary fine of up to € 65,250 per month.

In the case of an Internet business or outlet, these transactions may also no longer be offered on Verified by Visa terms. This rule will only be lifted if the ratio for the business or outlet is below 1% for two successive months.

Appendix B - EMS special terms for payment methods

Words that are capitalised in a sentence have the meaning as specified in Clause 2 of the general terms and conditions.

CARDS

1 General

1.1 You may never accept a Transaction (and submit Transaction Data about that Transaction for processing) if:

1.1.1 the validity period specified on the Card or by the Buyer has expired;

1.1.2 you have good reasons for doubting whether the person presenting the Card is also the Buyer;

1.1.3 the Transaction has not been carried out between you and a Buyer in good faith;

1.1.4 the Transaction has previously been charged back by the Buyer.

1.2 You may not accept a Point-of-Sale Transaction (and submit Transaction Data about that Transaction for processing) if:

a. the Card does not meet the requirements for the validity of the Card specified in this Manual;

b. the Card does not have the authenticity characteristics specified in this Manual;

c. the Card is damaged as a result of which the information is no longer clear or if alterations have been made to the Card;

d. the signature on the Card does not match the signature on the Point-of-Sale sales voucher or if there is no signature on the back of the Card;

e. the Card Number printed on the Point-of-Sale sales voucher does not match the Card Number on the front of the Card.

1.3 If you have doubts about a presented Card or the Buyer's proof of ID or in the event of an unusually high spend you must contact EMS.

1.4 You may not split the purchase sum for particular goods and/or services to be supplied to a Buyer into various transaction amounts.

1.5 You may not accept a Card for the sale of goods and/or services that breaches the law or that could harm or endanger the reputation of the Payment Schemes. You may not accept a Card for the display of images that show or suggest illegal acts or for images that show or suggest sexual acts by and/or with minors and/or animals or images that show or suggest sexual acts in conjunction with violence. You may also not accept a Card for payment for storage media in any form on which situations as described in the previous sentence are displayed.

1.6 You acknowledge that you are not permitted to obtain or download details of the Card via e-mail or the Internet and enter the Transaction manually via a Point-of-Sale terminal or virtual terminal.

2 Other

2.1 Other conditions that the Payment Schemes stipulate and that apply to you (alongside these terms and conditions) can be obtained from EMS or from the website of the Payment Schemes:

2.1.1 http://www.mastercard.com/nl/merchant/index.html

2.1.2 http://www.visaeurope.com/en/businesses retailers/retailers_and_merchants/security/handling_visa_payments/card_not_present_sales.aspx

If you have any questions for EMS
Please contact us on:
+31 (0) 20 66 03 120 or contact@EMSpay.eu

Any transaction - any way **EMSpay.nl/en**

P.O. box 22764
1100 DG, Amsterdam
The Netherlands

EMS
A First Data & ABN AMRO company

2019KC15_NL