Welcome
Card Acceptance for an All-Round Excellent Service
# Contents

**Service that leaves no question unanswered**
- Welcome to PaySquare a Worldline Company!  
  - Page 4

**Acceptance**
- The three steps to accepting more cards and international customers  
  - Page 5

**Transactions**
- Performing transactions securely  
  - Page 6

**Brief instructions**
- Brief instructions for contactless payment  
  - Page 7

**Security**
- Observing credit card security features  
  - Page 8
- Six rules for more security  
  - Page 13

**Just in case**
- PaySquare is PCI certified  
  - Page 14

**Chargebacks**
- Chargeback  
  - Page 16
- Excessive chargeback  
  - Page 18
Welcome to PaySquare
a Worldline Company!

Thank you very much for choosing us. In us you have chosen an acquiring company that for years has provided the reliability and service you expect. Each year, PaySquare handles more than 262 million card transactions for a total of 120,000 customers in the Benelux countries, Germany, Poland, France, Austria, Great Britain, Cyprus and Switzerland. We are pleased that you, too, have now joined us!

You will find the most important information clearly described here in your service guide and the enclosed security sheet. We encourage you to allow yourself time to read through the service guide in peace and quiet and then put it near your terminal. If you have any questions, our friendly and knowledgeable staff will be pleased to help you immediately.

You still have some questions?
We’ve got the answers!

Call us and rely on fast and dependable support. Please direct questions about formal and contractual matters, as well as the subjects of transactions and security to our contract partner service. In the case of a fault or for manual approval, please call our 24h-hour approval service. To enable us to help you even faster should the need arise, enter your contract partner number in the space below right now.

Customer service hotline:
(00357) 66 91 32 44

24h-hour approval service:
+49 (0) 69 66 57 16 84

Internet: www.paysquare.de
email: customer-service-global@de.paysquare.eu

Your contract partner number:

3003

Please enter your contract partner number here. It will then always be at your fingertips. Specification of your contract number is used for identification and accelerates the processing of your request.
The three steps to accepting more cards and international customers

Start right away or gain activation

1. **Activating the terminal**
   Please use the enclosed fax form for this. We have prepared this for you where possible. We have already done the activation for you if you are an existing customer of PaySquare. Your terminal is now ready.

2. **Accepting cards**
   Simply repeat the process a second time if the first transaction is rejected.

3. **Initiating payouts**
   On closing the cash accounts at the end of the day, you transfer all the payment data to PaySquare in the usual manner for crediting. The payout is made within the period agreed with you.

Attaching acceptance logos

Use prominently placed adhesive signs to show your customers that as Mastercard or Visa holders they are welcome in your business. The adhesive signs are enclosed with this information guide.

Security information

We recommend that you and your staff become thoroughly acquainted with the features of each type of card before you allow card payments in your company. Only then can you prevent attempts of card abuse from the outset. See pages 8-13 for detailed information on this.
Performing transactions securely

Please take the steps below if a customer would like to pay with Mastercard, Visa or debit card (Maestro or V PAY) in your business:

1. Make sure the card has the normal rectangular shape with rounded corners (see page 13 “designed card” for exceptions).

2. Check the card for damage or abnormalities.

3. Check the card’s expiry date.

4. Have the identity of the cardholder confirmed.

5. The card’s magnetic stripe is swiped through the terminal or inserted into/held on the card reader.

6. Your POS terminal dials into PaySquare and thus initiates execution of the payment process.

7. The message “Payment made” or “Payment rejected” is displayed.

8. Two slips are printed when a payment is successful. The terminal outputs only one slip if the transaction is rejected.

9. The customer’s card indicates whether PIN entry, a signature or both are required. The first slip stays with you and the second is for the customer.

10. In the case of contactless transactions, proof of identity by signature or PIN is only necessary if the amount specified by the bank was exceeded.

11. Compare the signature of the buyer with that on the card. If there are obvious differences, then you should cancel the transaction and insist on cash payment.

Cancelling payments

Credit card payments can only be cancelled before the cash accounts are closed. Please note that cancellations can only be made with the credit card used to pay for the goods. Please follow the steps shown in the operating instructions for your terminal for this.

Reversing credit card payments by means of a credit

Whether it is an exchange or return - there will be times when you would like to credit a certain amount to a customer. Please proceed as follows:

1. Select the menu item “Credit”.

2. Enter and confirm the amount.

3. Insert or swipe the card.
Brief instructions for contactless payment

1. **Important symbols for contactless payment**
   - This symbol <i>agog</i> means that a card is equipped with the contactless function.
   - And this symbol <i>agog</i> shows the customer that contactless payment is available here.

2. **Enter sum**
   - Enter the sum as usual and confirm.

3. **Cardholder makes payment**
   - Ask the customer to hold the card against the terminal with a max distance of 4cm.
   - Note: The card does not need to be inserted or swiped.

4. **Payment ensues**
   - Upon successful completion of payment, an acoustic signal will sound and the four LED lights will be activated on the terminal.
   - Note: Occasionally and for security purposes, PIN entry or a signature will be required.

5. **Receipt upon request**
   - Automatic customer receipt production is disabled for amounts totalling less than 25 €.
   - Note: If the customer requests a receipt, simply print it out.
Observing credit card security features

The security features on modern credit cards are an important contribution to the protection of consumers and merchants. You can protect yourself and your customers against card abuse if you pay attention to these details in your day-to-day business.

Visa

Visa security features

1. The Visa logo is always on the front and usually to the right.
2. On Visa, the hologram may also be replaced by the holographic magnetic stripe on the back.
3. The four printed digits must match the first four digits of the card number and start with a ’4’.
4. The card number must be arranged in blocks of four and match in terms of shape and size.
5. Expiry date of the card (month/year).
6. Name of cardholder.
7. All new credit cards are furnished with a chip.
8. On Visa, the magnetic stripe may also be a holographic magnetic stripe.
9. Signature panel for comparing with the payment voucher. On old Visa cards, the signature panel contains parts of the card number. The word “VOID” appears if the signature panel is damaged.
10. Card verification code (CVC).
11. Visa credit cards are also available in portrait format.
Mastercard

Mastercard security features

1. The Mastercard logo is always on the front and usually to the right.

2. On Mastercard, the hologram may also be on the back or replaced by a holographic magnetic stripe.

3. The four printed digits must match the first four digits of the card number and start with a “5”.

4. The card number must be arranged in blocks of four and match in terms of shape and size.

5. Expiry date of the card (month/year).

6. Name of cardholder.

7. All new credit cards are furnished with a chip.

8. On Mastercard, the magnetic stripe may also be a holographic magnetic stripe.

9. Signature panel for comparing with the payment voucher. The word “VOID” appears if the signature panel is damaged.

10. Card verification code (CVC).

11. Mastercard credit cards are also available in portrait format.
Diners Club International®

Campaigns and Bonus programmes, among other things with Tourism and Lifestyle providers, make Diners Club cards for frequent traveller’s preferred used mode of payment. Co-operations of the network with other credit card organisations extend the circle of card holders to a global native customer group.

Safety Features Diners Club

- The logo is always on the top left hand side
- All card numbers begin with 30, 36, 38 or 39
- The signature field on the back side includes the Diners Club logo, as well as the name and the world map
- The Discover, as well as the Plus logo, are always located in the lower left corner

Discover®

The Discover Card is widely popular in the USA. You can transact all cards with a Discover logo on the back using PaySquare like the BC Global Card issued in South Korea and the RuPay issued in India. Accommodate your international clients and accept this credit card.

Safety Features Discover Club

- The logo is located either on the front or back side
- The card number is 16 digit, beginning with 6011, 6400 or 6500
- The signature field on the back includes the words “Discover”, “Discover Network” or other affiliated logo
- To the right, next to the signature field is the three or four digit card ID in a separate field
- Some cards additionally have the logos of “Discover” and “Diners Club” or other affiliated logos
JCB International

JCB is the biggest credit card issuer and customer canvasser in Japan. The card is greatly popular primarily in Japan and in the Asiatic region, widespread especially Korea, but also in China, Taiwan, Thailand, and some Gulf States. In Europe, the issuance of card in Austria, Spain, Bulgaria and Russia are already begun. The acceptance is recommend especially in metropolitan regions and tourist destinations.

Safety Features JCP

- The three dimensional hologram is located on the front side
- The card number is 16 digit or 19 digit, beginning with 35
- The JCB logo is located on the front side
- The first four printed numbers must match with the first four numbers of the card number
- The three digit card verification code (security code) is either on the signature field or in a white field next to the signature field
Six rules for more security

Although card providers go to great lengths to make credit card business even more secure, black sheep find gaps time and again – to be specific, in places where card payment is handled too carelessly. However, it is very easy to play it safe. Observing a few rules will practically exclude the abuse of cards in your business!

1. Follow all the steps of the payment process described on pages 6 and 7.

2. Reject payments if the card is obviously altered or damaged.

3. Give your customer the card only after comparing signatures.

4. Fake embossing is recognisable by visible digit segments appearing behind the newly imprinted number.

5. Check the signature panel for damage – one such is evident if the word ”VOID” is visible.

6. Use the UV security features on credit cards. If the typical Visa or Mastercard holograms are not visible in the UV unit, then the card in question is counterfeit.

Do you have specific grounds for suspicion?

Please call PaySquare’s 24-hour approval service (using the reference “Code 10 request”). Act discreetly for your own protection and excuse the delay with a technical problem. Incidentally, PaySquare rewards every legitimate credit card recovery with a bonus.
PaySquare is PCI certified

The Payment Card Industry Data Security Standard (PCI DSS for short) is the common, worldwide IT security standard of the leading credit card companies. All companies that process, save or forward credit card information must demonstrate that they meet the requirements of this standard.

This is applicable to PaySquare and also to you in e-commerce, mail order or retail store.

Please familiarise yourself with the steps required to adhere to and fulfil the Payment Card Industry Data Security Standard (PCI DSS). The PCI DSS contains binding rules for merchants that offer card payments to protect data from misuse and theft.

You save, process or forward credit card information whenever you accept your client’s credit card details on your systems, be it for permanent storage or for short-term processing or forwarding to a service provider. Only if the data is sent directly to a third party without first passing through your system, you will be exempted from PCI DSS. If you are not sure whether to save, process, or forward card data onto your systems, please contact customer-service@de.paysquare.eu.

It is checked at regular intervals, whether the following twelve security requirements of the PCI standard are complied with.

In order to create a transparent security framework for the protection of payment-card information, the five largest credit card organisations have joined forces to form the so-called „PCI Security Standards Council“ (PCI SSC) and have published a common security standard: the „Payment Card Industry Data Security Standard“ (PCI DSS). This is mandatory for all parties involved in the processing, transmission and storage of credit card data. A merchant is affected by the PCI DSS as soon as they have one or more credit card acceptance agreements.

This shift away from paper and towards electronic documentation and digitized processes is how Worldline helps you transform your organization. However, it’s essential to maintain the legal standing of the documents within the system and Worldline has the experience and accreditation to see that you remain fully compliant at all times.

**Certification Authority**
ETSI 102 042, Adobe Approved Trust List

**Certification Digital Signature EAL3+**
Common Criteria

**Archiving Agreement**
for Public and Health data
The 12 points of the PCI DSS rulebook for you at a glance:

**Creation and maintenance of secure networks and systems**
1. Install and maintain a firewall configuration to protect cardholder data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.

**Protection of cardholder’s data**
3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data across open, public networks.

**Maintenance of a vulnerability management programme**
5. Protect all systems against malware and regularly update anti-virus software or programs.
6. Develop and maintain secure systems and applications.

**Implementing strong access control measures**
7. Restrict access to cardholder data by business need to know.
8. Identify and authenticate access to system components.
9. Restrict physical access to cardholder data.

**Regular monitoring and regular network testing**
10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.

**Adhering to an Information Security Policy**
12. Maintain a policy that addresses information security for all personnel.
Chargebacks are return payments of card transactions which result when the cardholder or the bank of the cardholder disagrees with the transaction. The reasons for chargebacks are varied, and may ensue on grounds of „non-delivery of goods”, „credit not processed”, „item not as described” or because the cardholder does not recognise a legitimate transaction. The most common reason for chargebacks is the misuse of cards, especially in E-commerce.

What happens when a transaction is charged back?

1. Upon request of the card holder, the amount is recalled to you.

2. Do you consider the chargeback unjustified? With the response form attached, you can file notice of your complaint via letter. Should you fail to submit any complaint within the 16 day period, the reclaim is irretrievable.

3. PaySquare assess whether your complaint has good reason within one week, on the basis of circumstance and regulations.

4. Should your complaint fail to show reasonable grounds, the reclaim is irretrievable and you will be informed in writing.

5. Should your complaint show reasonable grounds, it will be forwarded to the card-issuing bank and you will tentatively receive the reclaimed sum back onto your account.

6. The bank will then evaluate your complaint. Should the complaint be assessed as having reasonable grounds, the tentative transfer will be finalised, meaning the chargeback is permanently terminated. Should the card-issuing bank consider your complaint as having insufficient grounds, your case will be returned to PaySquare again.

7. PaySquare will assess your case again on the basis of current information. Should we find no basis for objection, the sum will be reclaimed from you with final effect. You will be informed of this in writing. Should we find a basis for objection, our assessment takes priority over that of the assessment of the credit card company. If our evaluation is approved, the disbursement is final. If the evaluation fails to receive approval, the sum is renewed and will be reclaimed from you. You will be informed of this in writing.
Process of a rejected transaction

1. Reclamation
2. Complaint filed within 16 days
3. Assessment by PaySquare
   - Not successful
     - Reclamation is final
   - Successful
     - Tentative return payment made
       - Assessment by the card-issuing bank
         - Justified
           - Return payment is final
         - Not justified
           - Second assessment by PaySquare
             - No grounds for complaint found
               - Reclamation is final
             - Grounds found for complaint
               - Assessment by the credit card company
                 - Successful claim
                   - Return payment is final
                 - Unsuccessful claim
                   - Reclamation is final

4. No complaint filed within 16 days
   - Reclamation is final
Excessive chargeback

PaySquare obliges all merchants to actively prevent chargeback. With respect to the general terms and conditions of PaySquare, PaySquare may terminate a business relationship with a merchant for good reason, if the amount of money authorised by PaySquare per card type (e.g., Mastercard, Visa, etc.) is credited in one calendar month

- one percent (1%) of the value of the transaction filings per card type or
- the total amount of chargebacks in a month exceeds the amount of EUR 1,000.00 per card type or
- the number of chargebacks per card type exceeds 0.50% of the number of transactions per card type of the previous month.

Upon termination for a good reason, an individual migration plan is agreed and implemented with the merchant involved. In addition to the termination date, the migration plan also covers all financial risks for PaySquare that exist within the framework of the merchant’s migration. Against this background, as a rule, there is an adjustment or demand for additional security deposits (retention of existing credit balances, additional security reserve, etc.), as well as the definition of the period of the required coverage. The period of coverage usually goes beyond the termination of the contractual relationship (coverage of subsequently received chargebacks, penalties, etc.).

1.1 Chargeback fees of PaySquare and penalties of card organisations in case of chargebacks and/or cheating (“Fraud”)

PaySquare charges a fee of EUR 36.00 / piece for the processing of each incoming chargeback (see price list).

In the case of excessive chargebacks, the card organisations also impose penalties, which PaySquare continues to charge to the responsible merchant. Given below is an overview of the corresponding (penalty-) programmes of the card organisations (chargeback / fraud defence). These costs would be passed on to PaySquare and respectively to the person responsible.

(Please note that the listing is not thorough. The current / valid version can be obtained at any time from PaySquare.)
<table>
<thead>
<tr>
<th>Program</th>
<th>Threshold values</th>
<th>Possible Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>VISA chargeback</td>
<td>Transaction filing without 3D Secure or partially secure transactions</td>
<td>Visa charges EUR 12.00 Scheme fee per chargeback for fraud</td>
</tr>
<tr>
<td>reduction initiative</td>
<td>Cards of European-issuers</td>
<td>This fee will be charged additionally to the actual chargeback fee</td>
</tr>
<tr>
<td></td>
<td>This leads to chargebacks for fraud</td>
<td></td>
</tr>
<tr>
<td>Visa Global Merchant</td>
<td>Number of monthly chargebacks &gt;200 pieces</td>
<td>Standard: →100% per chargeback turnover ratio</td>
</tr>
<tr>
<td>Chargeback Monitoring</td>
<td>Number of monthly chargeback-transactions&gt; 200 pieces</td>
<td>High Risk =&gt; 2.00% per chargeback turnover ratio</td>
</tr>
<tr>
<td>Program</td>
<td>Chargeback rate on purchase transactions&gt; 2.00% (in the same month)</td>
<td></td>
</tr>
<tr>
<td>Visa Global Merchant</td>
<td>Sum of the total reported frauds USD 25,000 and 1125 fraudulent transactions and</td>
<td>Standard: =&gt; USD 75.00 per chargeback and a fraudulent dollar to sales dollar ratio of 1% in one month</td>
</tr>
<tr>
<td>Fraud Program</td>
<td>Rate of fraudulent transactions to purchase transactions 2.50%</td>
<td>High Risk =&gt; USD 250.00 and 2% fraudulent-Dollar-to-Sales in one month</td>
</tr>
<tr>
<td>Mastercard Excessive</td>
<td>Excessive Chargebacks: Chargeback rate on previous month’s purchase transactions in two consecutive months ≥1.50% and</td>
<td>USD 25 per excessive chargeback that exceeds the specified threshold, and</td>
</tr>
<tr>
<td>Chargeback Program</td>
<td>Minimum 100 chargebacks in one calendar month</td>
<td>in addition a penalty depending on the respective chargeback rate is calculated by Mastercard. Unfortunately, we cannot predict the individual amount of the penalties determined. Generally the agreed penalties sums up to a four-figure amount.</td>
</tr>
<tr>
<td>Mastercard Global</td>
<td>5 fraudulent transactions and</td>
<td>USD 25,000 if merchant audit questionnaire is not sent (Refusal of information)</td>
</tr>
<tr>
<td>Merchant Audit Program</td>
<td>Minimum turnover of fraudulent transactions is USD 5,000 and</td>
<td>Complete takeover of all chargebacks marked as fraudulent, provided the thresholds are not</td>
</tr>
</tbody>
</table>
Good luck

We wish you a lot of success and a good business with Credit cards of national and international customers.

Thank you for your confidence.
About Worldline

Worldline [Euronext: WLN] is the European leader in the payments and transactional services industry. Worldline delivers new-generation services, enabling its customers to offer smooth and innovative solutions to the end consumer. Key actor for B2B2C industries, with nearly 45 years of experience, Worldline supports and contributes to the success of all businesses and administrative services in a perpetually evolving market. Worldline offers a unique and flexible business model built around a global and growing portfolio, thus enabling end-to-end support. Worldline activities are organized around three axes: Merchant Services, Mobility & e-Transactional Services and Financial Services including equensWorldline. Worldline employs more than 8,700 people worldwide, with estimated pro forma revenue of more than €1.5 billion on a yearly basis. Worldline is an Atos company.