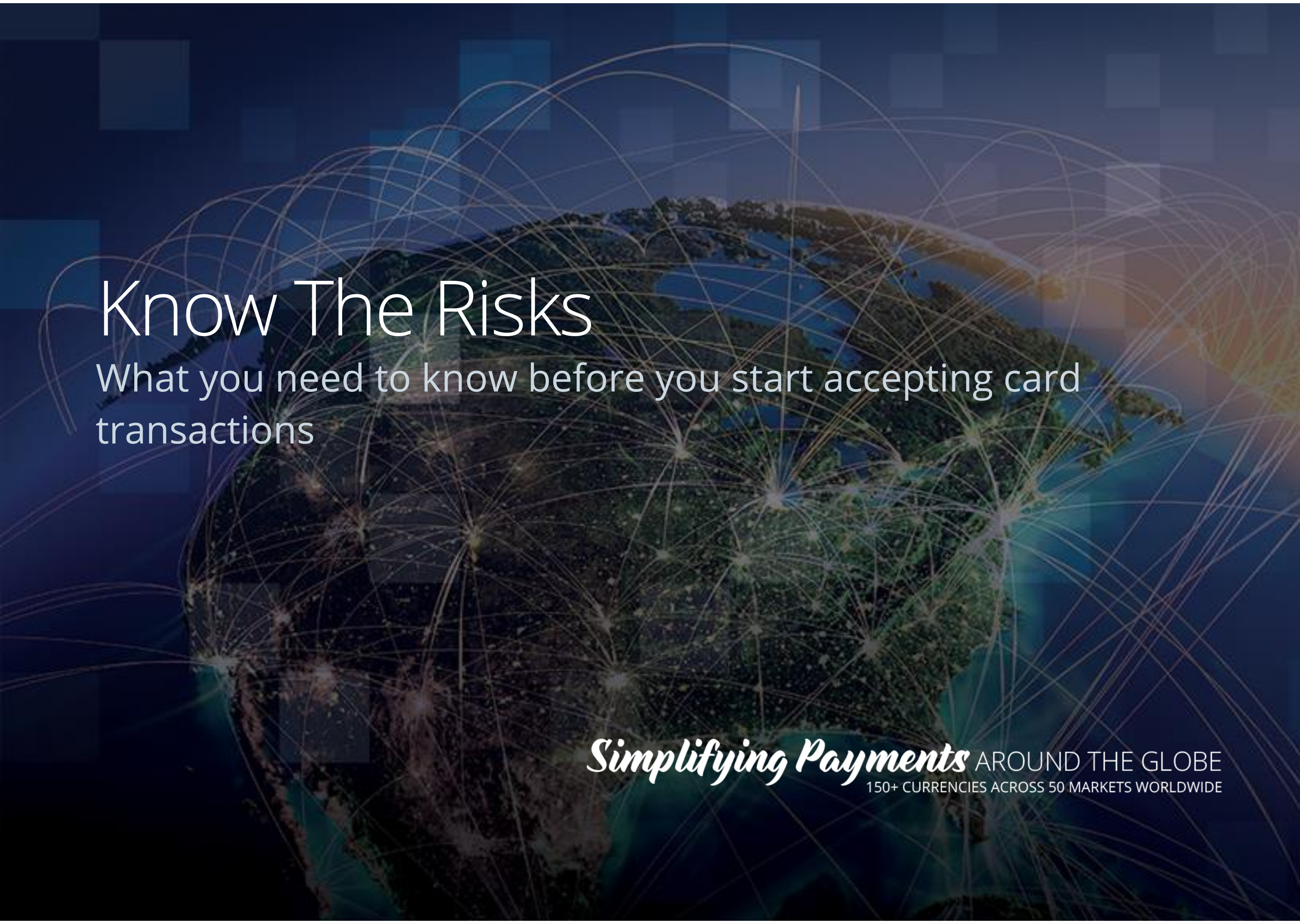
evopayments.com



Know The Risks

What you need to know before you start accepting card transactions

Simplifying Payments AROUND THE GLOBE
150+ CURRENCIES ACROSS 50 MARKETS WORLDWIDE

Table of Contents

MINIMISING RISK 2
CHARGEBACKS 2
CARD PRESENT TRANSACTIONS (CP) 3
CARD NOT PRESENT TRANSACTIONS (CNP) 5
KEEPING RECORDS 7
PROCESSING THIRD PARTY TRANSACTIONS 7
TERMINALS 7
DATA SECURITY 8
WHAT IS PCI DSS? 8

Minimising Risk

You take card payments at your own risk. Risks can exist with all types of card payments but some are higher than others (for example, cardholder not present transactions). This document includes tips on how you might identify and reduce the risk of fraudulent transactions.

If you and your staff follow the instructions in this guide carefully, the risk may be reduced, but it's important to understand that card payments are not guaranteed and that you carry the risk of chargebacks for fraudulent transactions. Even if a payment is authorised this simply means that at the time of the transaction, the card had not been reported as lost or stolen (perhaps because the genuine cardholder was not even aware of this at the time) and there were sufficient funds available to cover the transaction. Please make sure that everyone taking card payments for your business has read this guide thoroughly and practised the procedures.

We also recommend you hold regular training sessions with all your staff to refresh their understanding. Much of the information and guidance provided in this Guide is based on what we believe is current industry best practice. We hope that such practices will help you minimise possible exposure to security breaches or losses through fraud and chargebacks.

Note: Authorisations do not guarantee settlement.

Chargebacks (Cardholder Disputes)

One such risk is a chargeback (also known as a cardholder dispute). A chargeback is initiated by the Card Issuing bank; either at the request of the Cardholder or when the issuing bank sees the need to do so via the card schemes (Card schemes are the brand of the card e.g. Mastercard/Visa). EVO are governed by scheme rules and regulations. Common reasons for chargebacks are:

- Fraud related – cardholder denies participating in a transaction and claims his/her card details were used fraudulently by a third party
- Cardholder disputes the sale for reasons such as failure to receive goods or services paid for (disputes related to non -delivery of goods and services)
- Cardholder disputes the sale for reasons of quality (e.g. defective or damaged products/product or service not matching what was described by merchant e.g. wrong colour or size)
- Cardholder does not recognise a transaction on their card statement
- Processing Errors - Cardholder or issuer believes that you processed a transaction incorrectly. It may be caused by late presentment of the transaction; incorrect transaction amount or cardholder believes the transaction was processed twice in error (duplicate processing)

All Merchants accepting debit and credit card payments run the risk of being liable for chargebacks. A cardholder or card Issuer has the right to question or dispute a card transaction under the card scheme rules. A chargeback can be received up to 120 days after the card transaction was taken. In the case of goods or services being delivered, a chargeback can be raised up to 120 days from agreed date of delivery. Certain exemptions to the 120 days may apply depending on the Card Scheme and the reason for the dispute.

- When a chargeback is received EVO as the acquirer is automatically debited for the chargeback amount. This means that the card scheme gives the money back to the issuer straight away.
- The debit is passed onto the merchant since they are ultimately liable for the transaction. You will be notified of any chargebacks upon receipt via e-mail and the chargeback amount will be deducted from the subsequent settlement of any sales transactions on your facility at the time of the e-mail notification.

- Acquirer has 30 days (Visa) and 45 days (Mastercard) to dispute the chargeback on the merchant's behalf. This requires merchant cooperation as they must provide supporting documentation/information to defend the case. Adherence to timeframes is vital
- Not all chargebacks are defendable. There may be certain instances where supporting documentation/information may be insufficient to defend the case (this typically applies to fraud related disputes)
- If a merchant can defend his case within the timeframe, the Acquirer represents the chargeback, gets the money back from the issuer and credits the merchant
- If the issuer still wants to dispute, in some cases the issuer may have rights to issue a second chargeback and the process is repeated

Although rare, some disputes must be escalated to Arbitration stage during which the relevant card scheme rules on the case. Additional charges are imposed for the ruling and passed onto the losing party. During arbitration both parties may incur additional fines, if they are found to have breached regulations during the process.

Some common misunderstandings in relation to chargebacks include:

- **An authorisation is not a guarantee of payment**
  An authorisation proves the card has sufficient funds available at the time of transaction and/or the card has not been reported stolen at the time of the transaction. It does not vouch for the validity of the person using the card and is not a guarantee of payment

- **I pay the Merchant Service Charge so I will not get chargebacks**
  Chargebacks are separate to the Merchant Service Charge and are costed accordingly.

- **I should not be charged for the processing of chargebacks**
  Processing chargebacks incurs a fee due to the administrative work required on the part of EVO in requesting and providing supporting documentation to the schemes. However, most chargebacks can be avoided by Merchant vigilance and the use of fraud detection measures

Card Present Transactions (CP)

CP is where the card or Contactless payment device and the cardholder are physically present at the time of the transaction.

CP transactions can be accepted and verified in a variety of ways, including:

- Chip and PIN
- Chip and signature
- Contactless
- Magnetic stripe and PIN
- Magnetic stripe and signature

The best way to minimise the risk of CP chargebacks is to carefully follow the prompts provided by your terminal. If the terminal authorises a payment and prompts the cardholder to sign, then this should be allowed, subject to the normal checks associated with a signature-verified transaction (refer to section 4.2 'When a Signature is Needed' in the Customer Operating Instructions via https://evopayments.co.uk/wp-content/uploads/Customer-Operating-Instructions_EVO-UK-February-2021-v2.pdf).
Your terminal will automatically seek authorisation of the transaction depending on the floor limit set in the card by the card issuer and method of acceptance, for example, magnetic stripe verified by signature.

Chip and PIN and Contactless Transactions:

Chip and PIN cards and terminals have made substantial advances in preventing card fraud and are now the norm. All CP transactions must be completed using a chip and PIN terminal when presented with a chip and PIN card.

Chip and PIN and Contactless are the usual ways to accept card payments on your terminal when the card and cardholder are present. Some cardholders, however, will continue to sign to authorise payments and this could be due to an impairment that prevents them from inputting their PIN or because their card does not support Chip & PIN technology. Some cardholders will still have magnetic stripe only cards and these must not be refused at the point of sale.

A step-by-step guide (Chip and PIN)

- Following the terminal prompts, key in the full amount of the transaction
- Ask the cardholder to either insert their card into the chip reader slot on your terminal or PIN entry device
- Your terminal will now usually ask the cardholder to enter their PIN. If it doesn't, this could be because the cardholder has a card that does not support chip and PIN technology (such as a chip-and-signature or magnetic-stripe-and-signature card). Your terminal will advise which method is required – always follow the prompts on the terminal
- Ask the cardholder to check that the transaction amount is correct and to enter their PIN
- Most terminals will then authorise the transaction automatically. If the terminal prompts you, call our Authorisation Centre on 0800 0325658 immediately and follow the instructions
- Wait for the terminal to print out a terminal receipt
- Only give the cardholder the goods they are buying when you have received authorisation and completed the transaction. If authorisation is not given, do not go ahead with the transaction. Ask your customer for an alternative payment method
- Ask the cardholder to take their card from the terminal and give them their copy of the terminal receipt. Keep your copy of all terminal receipts in a secure fireproof place for at least 18 months in case there is a query later or these details are required to help defend a chargeback. Do not alter them in any way. If there is a dispute, the cardholder's copy will normally be taken as correct. Remember that even where authorisation is given, this is no guarantee of payment and the transaction is still open to being charged back (Note: Chip & Pin transactions are protected against fraud related chargebacks as the liability passes to the card issuing bank but a secure chip & pin transaction could still be open to non-fraud related chargebacks)

Contactless Transactions

Where your terminal is enabled to accept Contactless payments, the Contactless symbol will be displayed for low value transactions. The cardholder simply taps their card or Contactless payment enabled device to the reader to make the payment.

- From time to time your terminal may request that a PIN transaction is completed instead of a Contactless one, when a card is used. This is an added security feature, designed to confirm that the cardholder is in possession of their card and you must continue with a chip and PIN transaction in the usual way. Where your terminal is also enabled to accept Contactless High Value Payments (HVP), the Contactless symbol will be displayed for all transactions. HVP requires a Contactless payment enable device, for example, a smart phone. (Note: Contactless transactions are protected against fraud related chargebacks as the liability passes to the card issuing bank but a contactless transaction could still be open to non-fraud related chargebacks)

If a card isn't enabled for Contactless, the customer doesn't have a Contactless enabled payment device, or they simply prefer to use the chip and PIN functionality, then the Contactless option can be bypassed by them inserting their card into the card reader to complete the transaction via chip and PIN.

For more information on Contactless, refer to ‘Contactless Card Payments’ in the Customer Operating Instructions.

Card Not Present Transactions (CNP)

CNP is where you, the card and the cardholder are not all present together, for example, a transaction made over the internet, by mail order or telephone order (MOTO), or a recurring transaction. These situations are ideal for fraudsters because the card, signature and the personal identification number (PIN) cannot be checked. The majority of chargebacks result from transactions being undertaken fraudulently. If you proceed with a transaction that you are unsure of, you are doing so at your own risk. If the transaction has been completed, but the goods not despatched, you are still in a position to carry out a refund.

To minimise your risks:

- Be cautious of customers who give mobile phone numbers as their only form of contact (mainly for business to business customers – try to obtain a landline and verify same)
- Be wary of an order emanating from an email account where the customer’s name isn’t reflected in the email account address
- Be suspicious with transactions that have an unusually high value or volume for your type of business or the sale is ‘too easy’. In our experience these are the more likely ones to be fraudulent
- When performing a refund, always refund to the same card used for the original transaction (you could be at risk of a chargeback if the transaction is not refunded to the original card used for the sale transaction)
- Keep a database of chargeback history to help identify patterns of fraudulent transactions. If a sale seems too good to be true then it probably is. Don’t be afraid to contact the cardholder to ask further questions or request additional identification. A genuine customer should be pleased you’re security minded and trying to protect them from fraud
- Where possible, perform Address Verification Service (AVS) and Card Security Code (CSC) checks. Refer to your terminal manual or terminal supplier for assistance on using this security feature. Remember, you are not allowed to store the CSC data (CVV)
- For ecommerce transactions, an additional layer of security can be incorporated into websites known as 3D secure. Mastercard SecureCode and Verified by Visa (VbV) are versions of 3D secure and have been developed to allow customers to authenticate themselves as the genuine cardholder as part of the payment process. Where cardholders have been verified using Mastercard SecureCode & Verified by Visa (VbV) then you will be protected against fraud related chargebacks
- For virtual terminal transactions, make use of the PaybyLink feature where possible. Using the PaybyLink feature with the 3D enabled gives you the same protection as for ecommerce transactions as customers will need to authenticate themselves as the genuine cardholder as part of the payment process
- Always send goods by recorded or special delivery or by a reputable security carrier. Insist on a signed (preferably by the cardholder) and dated delivery note. Tell the courier not to make the delivery if the premises appear to be vacant. Please note that proof of delivery alone isn’t sufficient evidence to defend a chargeback
- Don’t release goods to third parties such as taxi drivers and messengers
- Be wary of requests for next-day delivery, requests to alter the delivery address at short notice, or telephone calls on the day of delivery requesting a specific delivery time
- If a customer requests to collect the goods, ask the customer to pay card present on collection through your point of sale equipment (this way you will not be exposed to fraud related chargebacks)
- Multiple or bulk orders: watch out for customers buying lots of the same item, either in the same transaction or separately
- First-time customers who place multiple orders. The risk of fraud is smaller when dealing with customers you know
- High-value orders, orders larger than normal may indicate fraud
- High-value items such as jewellery or electrical goods are often targeted by fraudsters because they are easy to resell, so take extra care with this type of transaction

- Hesitant customers: Customers who seem uncertain about personal information, such as their postcode or spelling of their street name, could well be using a false identity. Also watch out for customers being prompted when giving the requested information
- Same name, different title, could your customer be using the card of a family member?
- Sales that are too easy: be suspicious if a customer is not interested in the price and/or detailed description of the goods, but is only interested in delivery times
- Suspicious card combinations such as:
  - Transactions on several cards where the billing address matches but different/various shipping addresses
  - Multiple transactions on a single card over a very short period of time
  - Multiple cards beginning with the same first six digits offered immediately after the previous cards are declined
  - Customer offering multiple different cards one after another without hesitation when previous cards are declined
  - Orders shipped to a single address but purchased with various cards
  - Overseas shipping address – Be careful when shipping overseas, especially if you are dealing with a new customer or a very large order
  - Different shipping address – Orders where the shipping address is different from the billing address may be legitimate (for example, when sending flowers or a birthday present) but requests to send goods to hotels, guest houses or PO boxes are often associated with fraud

Non-UK issued cards being used for orders to be delivered to a UK address (consider whether it makes sense whether customers would be using a non-UK issued card (you can check where a card was issued on various websites by searching for ”BIN list lookup”
Note: If you do not take the appropriate precautionary steps to validate you are dealing with the legitimate cardholder or you and your staff do not take heed of any suspicious or fraudulent warning signs you are at risk of receiving a fraud related chargeback. We will debit the value of the transaction to your business at the time a chargeback is received.

Remember… authorisation is NOT a guarantee of payment

eCommerce Transactions

Here are some signs that an eCommerce transaction is likely to be fraudulent. Get to know them and make sure that all members of your staff recognise them too. And remember that the first sign that something is wrong can just be a general feeling of unease. If that happens, act on your instincts and carry out further checks.

-
- Multiple transaction attempts using the same or similar shopper details, such as name, e-mail address or IP address across one payment
- Different shopper details with one element the same, such as ten transactions from the same IP address giving different shopper names and e-mail addresses
- Multiple cards used by same shopper, especially where the card numbers are similar
- Obvious ‘card testing’, where the last four or eight digits of cards in a series of attempted payments contain similar numbers, or the card numbers are cycled repeatedly in a rough pattern or sequence
- Nonsensical shopper details, such as 'dgsgsgdf@dsgsd.com' as a shopper e-mail address or 'gdfgdfgfg' as a shopper name or billing address
- High-value transactions, especially where the amount is out of the ordinary for your usual daily processing amounts
- Mismatching Card Security Code (CSC) or mismatching Address Verification Check (AVS). Consider rejecting orders that carry mismatches or carry out further checks (these checks are separate to the authorization code)
- Mismatching combination of billing country, issuer country and IP country, especially, but not limited to, instances where the payment details are from any country or area which is associated with high risks of online fraud

- A delivery country that’s out of the ordinary for your business and regarded as high-risk

Keeping Records

Terminal receipts (when printed), paper vouchers and other transaction records are high-security items and access to them should be restricted. Keep your copies of all transaction details in a secure place for at least 18 months in case there is a query later or the details are required to help to defend a chargeback.

Do not alter transaction records in any way. If there is a dispute, the cardholder’s copy will normally be taken as correct. After 18 months, make sure that you dispose of all transaction records securely.

Processing Third Party Transactions

Processing transactions on behalf of another business can severely damage your financial wellbeing. If you’re either offered a lump sum for allowing unlimited access and usage of your card processing facility or a commission for each payment you process, be wary that it’s very rare for the third party to deliver the service that was promised. Often these entities, whilst appearing to be genuine and providing plausible reasons for requiring assistance, are fronts for organised criminal gangs engaged in timeshare or ticketing scams.

You must never accept transactions on this basis. These transactions are usually disputed or fraudulent and could result in chargebacks and financial losses to your business. Should this be the case you’ll be fully liable for reimbursing the cardholders where non-provision of the goods or services has occurred.

Third party processing also breaches your Card Processing Agreement with us, and identification of such activity may result in immediate suspension and eventual termination of your card processing facility. This type of processing can also lead to criminal proceedings.

If a third party approaches you, or your staff, to process their transactions, say no and contact us straight away with as much detail as possible. If you feel your business may have already succumbed to such a deception, or has recently received an approach, then please call us immediately for assistance with as much information as possible so that we can take appropriate action.

Terminals

Whether you rent a terminal from EVO Payments or another supplier, you are responsible for the terminal equipment and we strongly recommend that due consideration is given to the positioning and control of such equipment. You’ll be responsible for any losses resulting from interference by third parties not authorised to manipulate the equipment in any way other than in the normal course of the transaction, for example, entering a PIN. Therefore, please consider the length of time you give to the cardholder to input their PIN details.

Note: Ensure that any surveillance equipment you have isn’t able to record a cardholder entering their PIN.

Members of staff/customers have also been known to process refunds to their own card/s without the knowledge of the business owner.

- Make sure that you control who has access to the supervisor/refund PIN
- Change the generic PIN that comes with a new card processing terminal
- Ensure that this is changed regularly, particularly upon staff leaving
- Ensure that you have processes in place to help you spot unusual refund activity
- Check the End of Day/Z totals – ensure any refunds are for genuine customers/known transactions

Depending on your terminal type, you may be required to provide a telephone line or internet service for your terminal to connect with the EVO Processing and Authorisation Systems. If your terminal is supplied by EVO you must ensure that it is connected and powered on at all times to ensure it is available to receive important updates if required. Mobile terminals operate over GPRS (mobile data network). Whilst normal mobile phone connectivity is a good indicator of service, GPRS coverage and connectivity cannot be guaranteed.

Data Security

Security of personal data is a growing concern. Criminals are always looking at ways of getting this type of information from different sources. A vulnerable point of compromise which fraudsters have identified is card financial data which has been collected during the acceptance of cards.

The Payment Card Industry Data Security Standard (PCI DSS) is a global mandated standard which has been supported by the payment brands to bring a greater level of security to this type of data. As you're accepting card transactions, you need to be aware of the value of the data you collect when undertaking a card transaction and the need to secure it. If you were to suffer a security breach, there's a significant risk of financial and reputational loss to your business.

What is PCI DSS?

PCI DSS is a set of 12 comprehensive requirements for enhancing customer card data security, including requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.

Its purpose is to help organisations proactively protect their customer card data. Essentially, this is the personal, sensitive data stored on or in the card that is key to making a transaction. If you don't properly protect this data, fraudsters may find your system's vulnerabilities and hack in to steal it. The data is very valuable to them as they can use it to fund further illegal activity.

This is a very real risk. Every year merchants of all sizes suffer data breaches. These can result in fines from the Card Schemes because customer card data was not secured effectively and to the PCI DSS standards. These penalties start at €5,000 but dependant on the specific circumstances can be much more. In addition, there will also be remedial costs to your business. For further details on PCI DSS you can visit:

http://www.pcisecuritystandards.org – this site holds the latest version of the PCI DSS specifications and guidance on how to become compliant

https://www.mastercard.us/en-us/business/overview/safety-and-security/security-recommendations/site-data-protection-PCI/merchants-need-to-know.html

https://usa.visa.com/support/small-business/security-compliance.html

What you need to do

As a business accepting credit and debit card payments, be it over the counter, over the phone or online, you are required to comply with the PCI DSS. PCI DSS helps you reduce your risk of a successful attack by a hacker and subsequent data breach. A data breach can leave your business open to significant losses. These losses can include reputational damage, card scheme fines and costs associated with a forensic investigation of a data breach and associated clean-up. By simply completing the PCI profile designed to determine the scope of your PCI DSS assessment and attesting to your compliance and remain in compliance, you are proactively taking steps to protect your business.

Introducing Simple PCIDSS – Level 3 and Level 4 merchants

Merchants are required to comply with PCI DSS. To assist compliance with PCI DSS, EVO Payments facilitates access for merchants to an online PCI DSS compliance solution.

The Simple PCIDSS portal solution supports Level 3 and 4 merchant Attestation of Compliance by guiding the merchant through Self-Assessment Questionnaires (SAQs) and PCI DSS External Vulnerability Scanning (if required). Please note, credentials for the portal will only be issued to those merchants we require to complete a self-assessment questionnaire, or attestation of compliance.

There is a requirement to report to schemes for European merchant portfolios. The portal is the source of reporting information to support Visa Account Information Security (AIS) and Mastercard Site Data Protection (SDP) PCI Acquirer reporting. Semi-annual scheme reporting is generated on the Simple PCIDSS portal and made available for download by the relevant EVO Compliance area.

The portal is available at https://simplepcidss.eu/safemaker/login/login), which is a cyber security and compliance management solution that helps businesses to improve security, and acquiring organizations to reduce risk. The goal is to help you comply with card brands and perform a risk assessment for the customers in accordance with PCI DSS requirements. A risk assessment, as required in the PCI DSS, is a formal process used by organizations to identify threats and vulnerabilities that could negatively impact the security of cardholder data.

Level 3 and/or 4 Merchants are still required to be PCI DSS compliant and may validate compliance by successfully completing an annual Self-Assessment Questionnaire (SAQ) and quarterly network scans (if applicable) by Approved Scanning Vendor (ASV). 3 and 4 merchants may alternatively, at their own discretion, engage a PCI SSC approved Qualified Security Assessor (QSA) for an onsite Assessment and provide us with the Attestation of Compliance (AOC) form and Scan Report documentation (if applicable).

The AOC is valid for one year, after which it must be renewed - the security of card holder data is a continuous process and should be normal practice.

You will be loaded into the Simple PCIDSS portal and any merchant who has not validated by alternate means can use the portal to profile for determination of SAQ Type and to complete the validation questions.
The Merchant can contact by mail, phone or live chat support.

- set up the business profile (what kind of business do you operate? how do you accept credit cards?)
- answer SAQ questions
- the valid AOC and/or Scan Report can be uploaded by the merchant

How do you know if you already completed validation?

All merchants, at minimum, will have completed a Self-Assessment Questionnaire (SAQ) specific to their card holder data environment. In addition to completing a SAQ, some merchants are also required to perform quarterly vulnerability scanning and annual penetration testing depending on the processing environment.
If the business has completed the required PCIDSS assessment you will have within the business records a valid Attestation of Compliance (AOC), a Self-assessment questionnaire and an executive and/or Technical passing scan report (if applicable). Simple PCIDSS allows you to generate Certificate of Compliance for commercial purposes.

How long does it take to validate compliance?

The amount of time it takes for a company to validate compliance is dependent on the amount of time it takes to complete the SAQ and remediate the threats the vulnerability scan and penetration testing discover (if scanning and testing are applicable). Some businesses handle cardholder data in more complicated ways than others – this tends to increase the time involved to complete validation.

What happens if you are not compliant?

It is important to maintain compliance because it demonstrates to customers, vendors and suppliers your dedication to cardholder privacy. The PCI Council does not manage compliance programs and does not impose any consequences for non-compliance. The individual payment brands, however, have their own compliance initiatives, including financial and

operational consequences to certain businesses that are not compliant. Although validating compliance does not guarantee a business will not suffer a data compromise, which in most cases is not only financially but also brand damaging, it greatly reduces the chances of this happening.
As indicated on the merchant application, a business that does not submit proof of current compliance validation are applicable for enrollment into and billing for our sponsored validation program, Simple PCIDSS, for validation assistance and applicable fees will apply once enrolled.

What are my specific requirements for PCI DSS Compliance?

The requirements for becoming PCI DSS compliant are dependent upon the merchant level that a company falls under. Merchants are divided into four different levels based on the number of Visa or Mastercard transactions they process throughout a year and the environment in which they operate, please see table below:

LEVEL	CRITERIA	VALIDATION ACTION
1	Over 6,000,000 Mastercard or Visa transactions a year Other high risk merchants designated by a decision of the payment systems	Annual PCI DSS on site assessment Quarterly ASV scanning
2	Between 1,000,000 and 6,000,000 Mastercard or Visa transactions a year	Annual self-assessment questionnaire* Quarterly ASV scanning
3	Between 20,000 and 1,000,000 ecommerce transactions per year	Annual self-assessment questionnaire Quarterly ASV scanning (if applicable)
4	Other merchants	Annual self-assessment questionnaire (only at the request of the Acquirer) Quarterly ASV scanning (if applicable and only at the request of the Acquirer)

*merchants who meet the criteria of the self-assessment questionnaire that are type A, A-EP or D must use the services of a QSA (Qualified Security Assessor) / ISA (Internal Security Assessor) as part of the Compliance Self-Assessment Questionnaire and/or on site assessment.

Level 4 merchants are generally not required to complete a self-assessment, an automatic enrollment in the program is completed on your behalf. This registration process will deem you PCI compliant. We will monitor for change and contact you directly to inform you if a self-assessment is required at any time.

A full list of accredited QSAs can be found on the PCI Security Standards Council website:
https://listings.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors
The following website provides details on how to become an ISA:
https://listings.pcisecuritystandards.org/assessors_and_solutions/internal_security_assessors