Paysafe:

Payment Processing European Acquiring

Merchant Operating Guide

Version 2.4
Latest Update: 16 January 2023

Table of Contents

1.0 Important information

The contents of this guide form part of your contract with Paysafe. Failure to comply may result in the termination of our contract (the "Merchant Terms").

This guide covers core acquiring services requested by your business on your original application form, as well as other options you may not have selected. For more information about other productsand services, such as alternative payment methods, please contact uk.customerservice@paysafe.com.

You must only accept card payments for goods and services as detailed in your original application form, or with prior written agreement from Paysafe.

2.0 Purpose of this guide

Welcome to the company trusted to move billions of dollars around the world.

We are pleased you have chosen us as your payment processing partner. Our goal is to ensure that your business achieves maximum benefits from our card payment acceptance capabilities. Choosing Paysafe means that you are working with one of the biggest providers of payment solutions in the world, trusted by businesses and consumers in over 200 countries and territories. We believe that the point of every payment should be relevant, simple, fast, efficient and safe, and we have flexible products to suit your needs right across the payments value chain.

The purpose of this guide is to ensure that you understand the procedures which must be followed to ensure efficient processing of card transactions, and to explain your responsibilities in this process. We want to help you process card transactions without any issues and ensure you understand how to minimise the risks to your business, both in terms of, security, fraud and user-error.

Our consultative approach is valued by our customers who rate us highly on our level of support; so please contact us if you have any queries or would like to understand more about our suite of flexible solutions.

3.0 CNP transaction (card not present) – e-commerce, mail & telephone order

The Payment Services Directive requires Strong Customer Authentication (SCA) to be applied to all electronic payments within the EEA and UK (where SCA is regulated and mandated) except for some transaction types that are exempt from SCA (as detailed further below).

CNP fraud: prevention and detection

Card Not Present (CNP): neither the card nor the Cardholder are physically present when you process the transaction.

Accepting CNP transactions, via the internet, by phone or mail order does have risks attached. It is important that you understand these risks and can take appropriate precautions.
Unlike in a face-to-face transaction, you are unable to check whether the card is genuine, and therefore it is possible for a fraudster to provide a card number that they have stolen from a genuine Cardholder. For this reason, we provide additional tools to authenticate the Cardholder for e-commerce transactions such as 3D Secure, which is described below.

Checks to identify potential fraud are outlined in the rest of this section and are suggested by Visa and Mastercard. Note that these checks will not be 100% effective and do not shift the liability for fraud or subsequent chargebacks (that is, the liability will remain with the merchant).

For more information about fraud prevention and to raise awareness for your staff, visit Financial Fraud Action UK: http://www.financialfraudaction.org.uk/Retailer-internet-mail-phone-advice.asp.

Fraud tools and real-time screening solutions

To reduce the risks of fraud to your business, Paysafe's processing platform was developed to include fraud detection and prevention functionalities. There are also several third-party providers in the market that can provide you with additional fraud prevention tools and advice.

Our platform includes the following standard fraud-prevention features at no cost to the merchant (some require set-up as detailed below):

3.1 3D Secure

The 3D Secure protocol is known by the card schemes as Verified by Visa and MasterCard/ Maestro Secure Code respectively. This online Cardholder authentication works in a similar way to checking a PIN at the point-of-sale. Cardholders register with a password they choose. Requesting additional information including the customer's 3D Secure password aims to check the Cardholder is genuine so that you can be assured the card information relates to the genuine Cardholder. For information about chargeback protection for 3D Secure transactions see Section 6.3.

Our processing platform supports 3D Secure authentication at multiple levels. Our APIs and back-end integrations with downstream processors support all data elements generated during the 3D Secure interaction scenarios. We also provide a simplified API allowing you to easily take advantage of the benefits of 3D Secure without the complexity of a full merchant plug-in (MPI) integration. For more information about how to set-up 3D Secure contact uk.customerservice@paysafe.com.

Note: You must enroll with Mastercard SecureCode if you would like to accept e-commerce Maestro.

3.1.1 SCA Exemptions

Low Value Transaction Exemption

One type of transaction that is exempt from SCA is a transaction that is equivalent to or less than 30 EUR, (or currency equivalent) ("**Low Value Transaction**"), and so does not require the completion of 3DS authentication.

A Low Value Transaction must meet the following criteria to be exempt from completing 3DS authentication:

- A transaction must be equal to or less than 30 EUR (or its equivalent in alternative currency).
- The total number of transactions exempted from SCA cannot exceed 5 consecutive transactions. The issuer will perform the velocity check per PAN.
- The total amount of 5 consecutive transactions, exempted from SCA cannot exceed a total amount of 100 EUR. The issuer will perform the velocity check per PAN.

If a transaction is more than 30 EUR or if the total of the last five consecutive transactions exceeds 100 EUR, the Issuer can request for a full SCA to be performed, in such cases you will receive a soft decline (**Decline code 3060**) To complete the transaction you will need to complete a 3DS2 authentication, followed by a re-authorization.

If you provide a Low Value Transaction exemption flag and 3DS authentication details, Paysafe will reject the transaction as you can only opt to:

A. Process the transaction without SCA; or
B. Go through the 3DS authentication process.

Paysafe will apply the Low Value Transaction exemption indicator automatically on the payment authorization for transactions that:

- Do not Indicate any other exemption flag
- Do not have a 3DS2 authentication flag
- That are below 30 EUR, (or equivalent in alternative currency).

If you would like to disable the service for Low Value Transactions, please contact customer support at: uk.customerservice@paysafe.com .

If the transaction does not qualify for a Low Value Transaction exemption or you decide to authenticate the transaction, then the Low Value Transaction exemption indicator will not be applicable and nor will it be assigned automatically.

Remember, for any transaction processed without SCA unless such transaction is exempt, the merchant shall be liable.

3.2 Card Security Code (CSC) / Card Verification Value (CVC) and Address

Using AVS/CSC does not require any additional set-up for merchants and these services can help reduce fraud by requesting additional information from the Cardholder:

For Visa and MasterCard cards, the Card Security Code is either the last three numbers on the card's signature panel, or the three numbers found in box adjacent to the panel. For American Express cards, the Card Security Code can be found on the front of the card and is the four digits printed above the Primary Account Number (PAN).

Our platform supports all variants of card verification number processing to help ascertain that the customer placing the order did possess the card.

AVS allows you to check the numerical details in the Cardholder's address and postcode with their card issuer.

These are recommended fraud prevention tools, and for certain card types are mandatory to obtain authorization. For more information about using CSC contact uk.customerservice@paysafe.com.

Remember: do not store the CSC after the transaction is authorised.

3.3 Negative List

Our platform uses automated third-party feeds, proprietary historical transaction processing data, and information provided by our internal Risk Management team to feed our global negative database. We also support merchant-specific negative lists.

No set-up is required. For more information about using Negative lists contact uk.customerservice@paysafe.com.

3.4 Order Velocity Monitoring

We can monitor the frequency of transactions meeting specific criteria within specific time windows, e.g., the number of unique card numbers originating from a given IP address within the past hour. If the frequency exceeds a configurable threshold, then subsequent transactions can be declined for a configurable period. We can do this at a merchant-specific level, as well as a global level.

There is no charge for using our order velocity monitoring tool; however, this will need to be set-up specifically to suit your business. For more information about how to set-up contact uk.customerservice@paysafe.com.

3.5 IP Address and Block Lists

Our platform validates the source IP of a transaction Cardholder which merchants can use in their risk- based decision making. We can also block transactions based on IP address or range, issuing BIN, or location data derived from either of these sources.

3.5.1 Reducing risks

As the card and Cardholder cannot be verified at the time of the transaction, CNP transactions carry increased risks. There is no guarantee that the person undertaking the transaction is the genuine Cardholder, which means you may be at risk of chargebacks from fraudulent transactions. There are several simple ways you can reduce the risks for your business.

> Remember, authorisation confirms the Cardholder has sufficient funds and that the card has not been reported as lost or stolen at the time of the transaction. Authorisation doesn't guarantee payment.

Note: You must enrol with Mastercard Secure Code if you would like to accept e-commerce Maestro.

DO	Get the Cardholder's full name, phone number and address including the postcode (as recorded by their card issuer). *Note: If the delivery address is different, ensure that you also get the delivery address and name of the person receiving the goods or services.*
DO	Make sure you get the card number, expiry date and the card security code (CSC). Also, known as: • CVC or CVC2: card verification code • CW or CW2: card verification value • CWC: card verification value code • CCV: card code verification • V-code or V code: verification code • SPC: signature panel code
DO	Before taking payment, make sure you confirm the gross amount inclusive of all costs (e.g. delivery, packaging, VAT etc.).
DO	Record the customer reference number, if quoted – for a Visa transaction only.
DO	For mail order transactions, get the Cardholder's signature.

DON'T	Allow a Cardholder to collect goods in person which were purchased via a CNP transaction.

3.5.2 Suspicious transactions

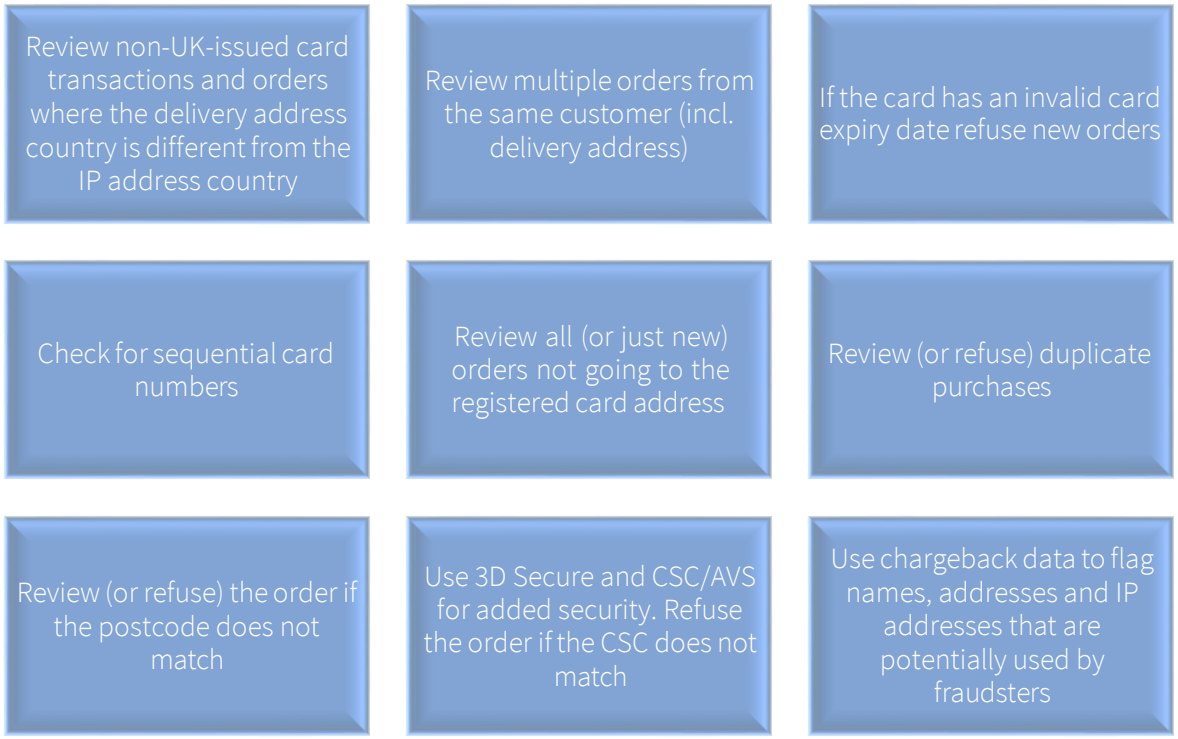
The following scenarios should be considered as warning flags, and we suggest that you initiate additional checks in these circumstances:

- Does the order seem unusual – particularly large volume or value?
- Is the address in any way suspicious? Has it been used by a different customer before?
- Is the customer using more than one card to pay for a single order?
- Does the customer lack details of their account (incl. their contact details) or previous orders?
- Has the customer admitted to using a card on someone else's behalf?
- Does it sound like the customer is being prompted or using a script or notes?
- Is the order made up solely of goods which can be easily re-sold?

For further assistance please contact our Merchant Support team at uk.customerservice@paysafe.com.

3.5.3 Additional checks for e-commerce

The following are recommended checks and steps merchants can make to help prevent fraud:



Always make sure that goods are sent to the person named on the order; never release goods to anyone else (including delivery firms hired by the customer).

3.5.4 Further advice

If you are still unsure about a transaction, or you require further information about any of our fraud tools or the checks recommended by the card schemes, contact your account manager or uk.customerservice@paysafe.com.

3.6 Authorising transactions

A CNP transaction must be authorised at the time of the transaction. This can either be an authorisation of the full amount or a pre-auth for the anticipated transaction value (such as for a hotel room booking).

3.7 Shipping goods and providing services

Mastercard	Visa
The transaction amount must not exceed the authorised amount.	Authorisation for a Visa transaction is valid if the amount is within 15% of the authorised amount. The additional 15% must only be to cover the cost of shipping.
The transaction date is the date goods or services are provided or shipped	The transaction date is the date goods or services are provided or shipped.
You must obtain authorisation for MasterCard transactions on the day the Cardholder places the order. The transaction should be processed when the goods or services are ready to be delivered. If you do not ship goods within seven days, youmust obtain a second authorisation. Quote theoriginal auth. code, and keep both for your records.	A Visa transaction can be authorised up to seven calendar days before the transaction date.

3.8 Recurring transactions

Recurring transactions are used by a wide variety of merchants such as utility companies and those providing memberships or subscriptions. A recurring transaction is where the Cardholder consents to having their account charged on a pre-agreed condition (e.g. the balance on a prepaid card drops below a certain amount) or frequency (e.g. monthly or annually). Once the Cardholder has agreed, they can continue to receive the goods or services without having to worry about payments as this is taken care of by the merchant.

The following rules must be observed:

When carrying out a Recurring Transaction, a Merchant must:

- Obtain prior permission (in writing or electronically) from the Cardholder to periodically chargefor recurring services; and
- Retain a copy of that permission for the duration of that Recurring Transaction and provide it to the Issuer upon the Issuer's request.

- Ensure transactions are not more than 365 days apart.
- Ensure the correct card expiry date must be provided for each transaction.

When entering a Recurring Transaction Agreement, a Merchant must:

- Obtain express consent from the Cardholder at the point of checkout or sale; and
- Provide the Cardholder with the following information when obtaining that consent:
- The amount of the Recurring Transaction;
- Whether the amount is fixed or variable;
- The date of the Recurring Transaction;
- Whether the date is fixed or variable; and
- An agreed method of communication for all future Cardholder correspondence

3.9 Merchant-Initiated Transactions Mandate

We are required to set up a Merchant-Initiated Transactions (MIT) Mandate if you operate in a business model where the final amount is not known at the time of authentication. [Add further wording to explain what is a Merchant-Initiated Transactions (MIT) Mandate.]

MIT Mandate (with proof of authentication)

An authorization request (either an authorization request or account status inquiry) is required to set up an MIT in order to allow the issuer to validate the authentication value generated for the agreement.

To set-up each individual MIT, you are required to:

- put in place an agreement with the cardholder specifying the reason for the payment and the payment amount (or an estimate) when the precise amount is not known);
- request an authorisation request (either an authorization request or account status inquiry) from the [cardholder/issuer]; and,
- apply SCA on each of the transactions.

Paysafe can only apply Merchant Initiated Transactions (authorization requests with an MIT exemption indicator) when:

- The transaction is triggered by you when the cardholder is off-session (off-session means the
- cardholder is not interacting with the merchant page or the merchant app to initiate the transaction), or
- The transaction is triggered by you as it could not have been triggered by the cardholder during
- checkout, because:
    - The final amount is not known during the checkout (for example, online groceries shopping), or
    - An event triggered the transaction after the checkout (for example, miscellaneous rental or service charges), or
    - The transaction is part of a recurring payment arrangement, or
    - The transaction is broken down into different payments happening at different times (for example, instalments, travel bookings, marketplaces), or
    - The transaction is a staged-wallet funding transaction where the funding is triggered without the
    - involvement of the cardholder (e.g. “top-up” scenario), or
    - The transaction follows upon a declined authorization at a transit validator but the traveller has completed a billable journey (Transit Debt Recovery)

Exemptions/Exclusions

We are only permitted to submit MIT payment authorisations without proof of authentication with either the standard MIT identification or one of the existing MOTO flags if you indicate to us that the transaction was initiated with an MIT agreement.

Please be aware that authorisation approval rates may be influenced by the MIT indication and absence/presence of proof of authentication. The MIT exclusion cannot be used to bypass the PSD2 SCA requirements for transactions for which card data has been registered on file with the merchant and the cardholder triggers the payment (Card-on- File).

3.9.1 Account Updater

The Account Updater service allows you to request and receive automated payment card (both credit and debit card) updates from Visa and Mastercard for their customers' recurring billing and tokenised accounts. Account Updater allows the continuous processing of recurring billing and subscription services without the need for you to contact or be contacted by the Cardholder if payment card details have changed in any way.

Main benefits

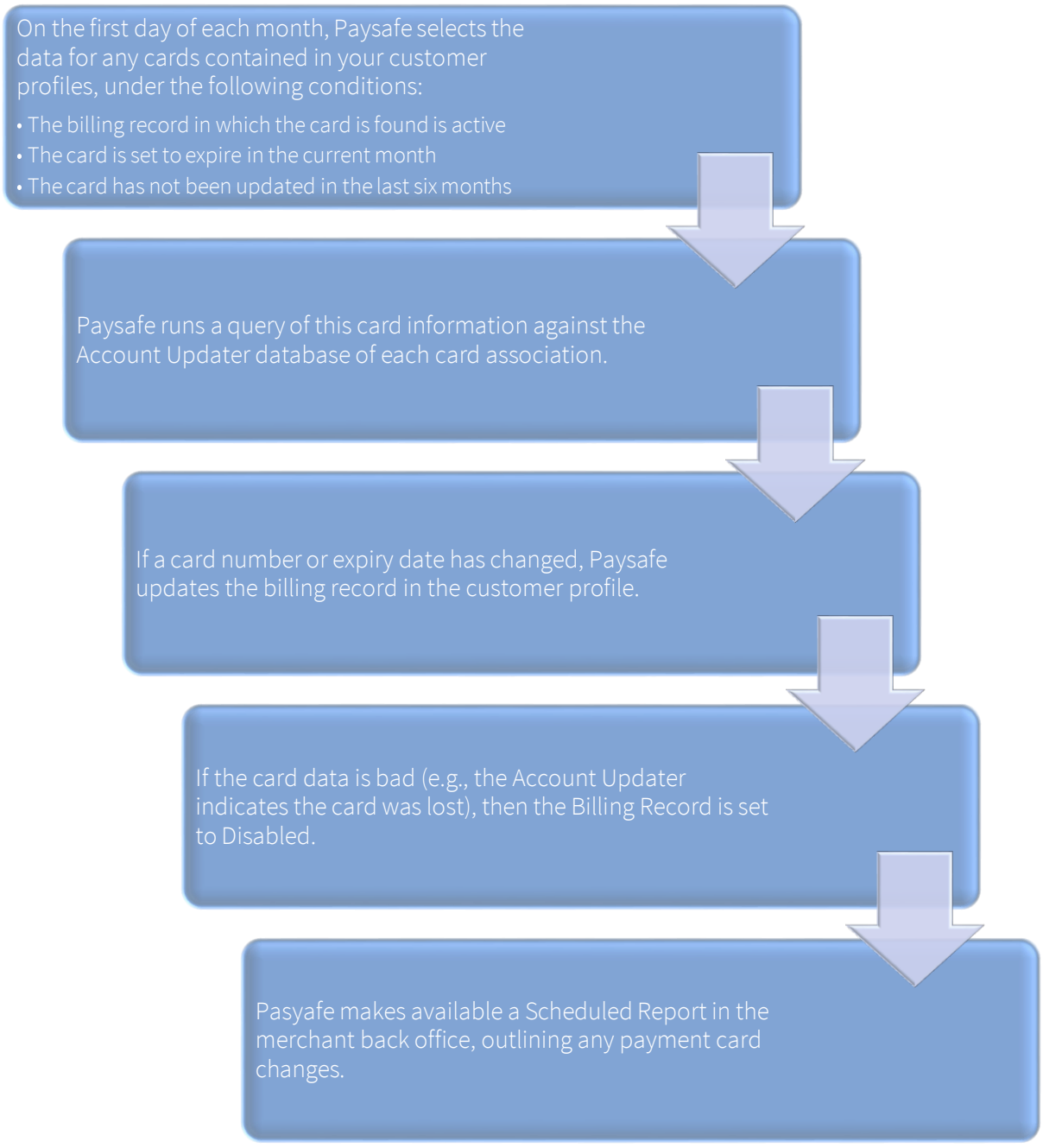
Implement easily
Unlike most Acquirers we have the service integrated into our gateway

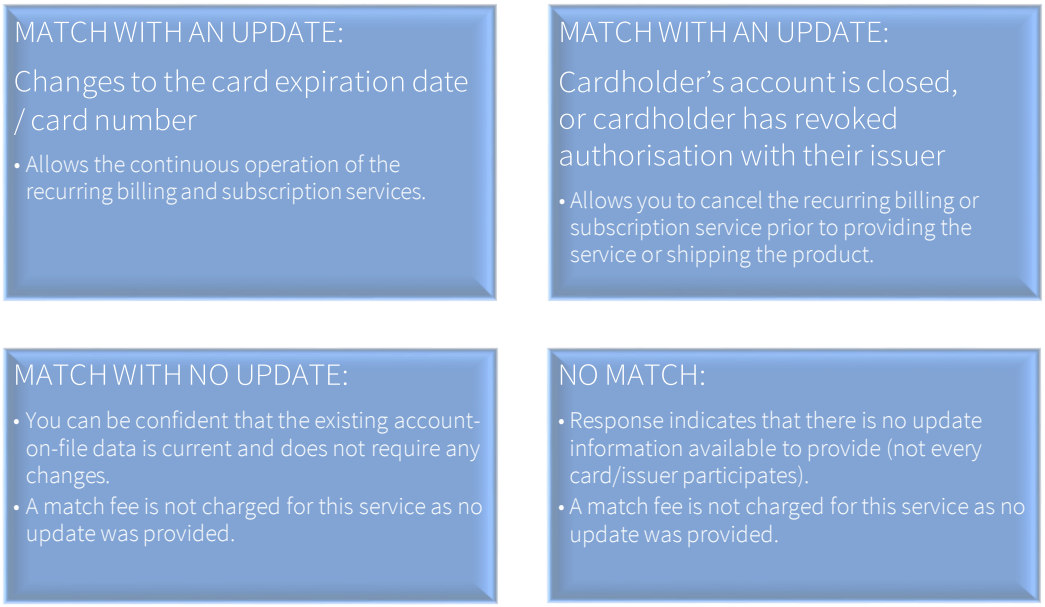
Save time
This service is automated as our gateway recognises recurring transactions and runs the necessary checks

Reduce workload
It reduces declines and increases the number of transactions processed

Save money
Visa offer discounted interchange rates on transactions using this service

3.10 Account Updater – 5 step process





3.11 Merchant requirements

When using the account updater service, the Merchant must:

- Ensure they are registered by Paysafe for services with each card association
- Be passing card data or integrated into the Customer Vault API
- Update databases containing the account information within five working days of receiving results of the Account Updater service, so that the latest updates are used for the next billing run
- Have ongoing communication with Cardholders who have card account number and expiry date on file, and where the customer has an active recurring billing or subscription service with the merchant
- Remove account information from database of any account if receive 'Contact Cardholder' or 'Closed' responses from the Account Updater service. Upon receipt of such responses, the Merchant must:
- disable the billing service for that account
- Halt the pending shipment of goods
- Contact the Cardholder to request new card information to use.

3.12 Service Options

3.12.1 Request file with a clear-text card number and expiration date

A merchant may use this method if they have access to clear data and their PCI compliance is at the highest level. The merchant submits an encrypted request file via SFTP prior to a pre-determined cut-off time and receives a response 24 hours later for pickup on SFTP.

3.12.2 Profile payment methods and billings

A scheduled job identifies merchant accounts which have Account Updater enabled and identifies the following record types and statuses:

a. Payment methods with no billing records

b. Payment methods with billing records that are not disabled

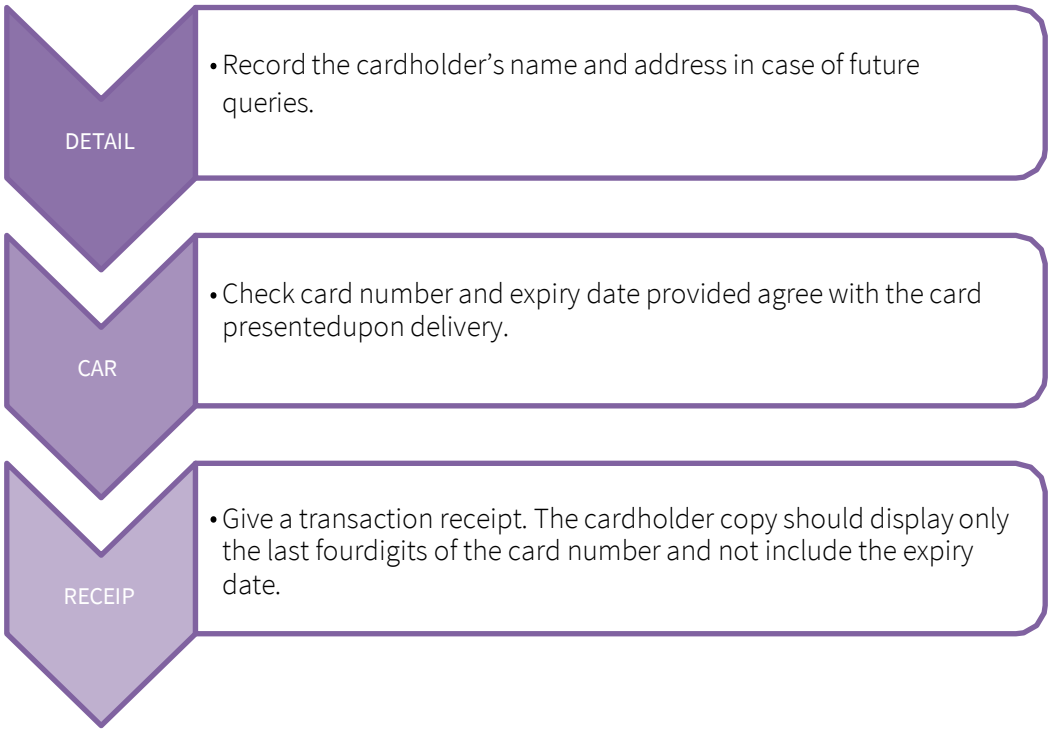
The job shall collect card data for the following two conditions and update their card or expiry date if there is an update or disable the payment method if there is a closed account or similar response.

a. Card is set to expire in the current month
b. Card has not been updated in the previous 180 days

Important note: for both file-based methods, it is recommended that the merchant perform an update on (a) the 1st day ofexpiry month, and (b) one time every 180 days (as required by Visa and Mastercard), whichever comes first. However, the merchant may perform the update as often as they wish.

3.13 MOTO: Mail Order and Telephone Order

Merchants processing MOTO transactions must:



Note: You may be at greater risk of fraud and chargebacks if you key a transaction following a telephone order as it will not be possible to check that the customer is the genuine Cardholder with additional authentication.
Note: Maestro cards can only be used for domestic transactions in the UK, Ireland and France.

Remember, authorisation confirms the Cardholder has sufficient funds and that the card has not been reported as lost or stolen at the time of the transaction. Authorisation doesn't guarantee payment.

3.14 Payouts Service - Visa Direct

The Original Credit Transaction (OCT) is a VisaNet Transaction that can be used to send funds to an eligible Visa account. Merchants can use the OCT to enable Visa Direct services such as Money Transfers, Funds Disbursement, prepaid loads, and credit card bill payments.

Visa Direct services are available to Paysafe merchants who are registered in the following countries:

- Austria
- Belgium
- Denmark
- Estonia
- Finland
- France
- Germany
- Hungary
- Ireland
- Italy
- Malta
- Netherlands
- Norway
- Poland
- Portugal
- Spain
- Sweden
- Switzerland
- UK

3.14.1 OCT Funding Options

Paysafe and its merchants determine how senders of Money Transfers can fund OCTs (e.g., cash, bank account, digital wallet, or Visa account) and are responsible for ensuring that sufficient funds are available.

If the OCT is funded using a bank account or digital wallet, Paysafe or the merchant may use a proprietary message to debit the sender's account for the money transfer amount.

In the European Economic Area (EEA) and UK (and Gibraltar, where relevant), Paysafe must ensure that the source of funds used for the Money Transfer is in the same EEA country or UK (or Gibraltar, where relevant) as the recipient cardholder.

3.14.2 OCT Processing Rules by Business Application Identifier (BAI)

Processing Rule	Money Transfer (BAI = AA, BI, CD, FT, PP, or WT	Funds Disbursement (BAI = FD, GD, GP LO MD, or OG)	Prepaid Load (BAI = TU)	Credit Card Bill Payment (BAI = CP)
Transaction Types	Merchants must initiate OCTs as 0200 messages or use the Visa Direct APIs.	**General:** Same as Money Transfer **Cross-border**: Merchants may send OCTs as TC06s.	**General:** Same as Money Transfer	Same as Money Transfer
Reversals and Adjustments	Merchants sending 0200 OCTs are not permitted to initiate OCT reversals. Good faith adjustments may be used.	**General:** Same as Money Transfer **Cross-border**: if a merchant sends a TC06, reversals are allowed only for processing errors and within 1 business day of the original.	**General:** Same as Money Transfer	Same as Money Transfer
Disputes	Only dispute reason codes 12.4, 12.6, and 13.7 may be used. OCT dispute reversals are only allowed within **one business day** of the dispute.	Same as Money Transfer	Same as Money Transfer	Same as Money Transfer

3.14.3 Card Acceptor Identification Code (CAID)

Merchants must use a unique Card Acceptor Identification Code (CAID) in the OCT authorization request message to identify the merchant that is disbursing funds to Visa account holders. The unique CAID from the original transaction message is required in any subsequent messages, including reversals, disputes, and dispute responses.

Before submitting an OCT, it is recommended that the merchant perform checks on the destination Visa account to determine eligibility to receive OCTs and Fast Funds posting capabilities.

3.14.4 Customer Access Channels

Merchants must develop and manage user interfaces for each of the funds transfer customer access channels they plan to support, such as Internet/online banking, bank branches, ATMs/unattended kiosks, and phone and/or mobile banking. Merchants should implement a customer experience that is simple, straightforward, and streamlined, especially important for ATMs, internet, and mobile channels.

Merchants should minimize the number of steps and screens presented to the user and track the access channel used as this information may be valuable in customer service and during disputes. Customer user interfaces should address authentication and branding, obtain information (e.g., sender, recipient, and money transfer amount), and provide transaction confirmation, receipt information, disclosures, and customer service details.

3.14.5 Consumer Data Collection and Sender Authentication

Merchants must collect sender and recipient data and are responsible for verifying the sender, regardless of the payment method or the access channel, for the purpose of risk, sanctions enforcement and anti-money laundering and anti-terrorist financing control. merchants must ensure that the collection of sender and recipient data and the processes implemented to enable sender authentication are compliant with the Payment Card Industry Data Security Standard and applicable laws.

Merchants should consider how they would collect sender and recipient data and verify sender data in each customer segment supported. The sender authentication method should be appropriate to the access channel and should follow regulatory and industry standards and best practices. Examples are government-issued photo identification, ATM PIN, Internet banking identification and password, and telephone banking PIN/password.

When enabling channels such as ATMs and mobile devices, merchants may want to consider requiring senders to register, either online or at a bank branch, prior to the use of these channels.

When collecting card account data, merchants should consider performing a Modulus-10 Check to ensure the sender's and recipient's payment credentials have been entered correctly.

Merchants' risk and compliance teams should review sender data collection and authentication methods to ensure they follow internal requirements, applicable "Know Your Customer" (KYC) procedures, and applicable local laws and regulations.

Recipient card account holder address, card expiration date, or CVV2 are not required to be collected to initiate OCTs.

3.14.6 Transaction Screening

Merchants must implement transaction screening procedures to flag high-risk transactions for review prior to submission. These should include limits (such as count, amount, and rolling limits), and other checks to determine whether the sender and/or the recipient are on any applicable government or bank-specific blocked lists.

Merchants approved by Visa to offer domestic Money Transfer programs via OCTs must also ensure that both of the following entities fall within the same country:

- The sender's source of funds for the Money Transfer, and
- The recipient's account.

Merchants offering these programs are required to carry out this validation prior to initiating the OCT, as part of the conditions of their program approval.

3.14.7 Confirmation of Funds Transfer

Depending on the type of payment, (e.g., P2P Money Transfer, Funds Disbursement, prepaid card load, Credit Card bill pay, etc.), merchants may need to provide senders or customers with a way to confirm the payment including the amount, currency conversion rates, and recipient details prior to executing the payment. This is an important step as it allows the sender or customer to confirm all details are correct and it helps reduce customer service issues and disputes.

All fees, currency conversion rates, and any foreign exchange markup must be disclosed to the sender or customer in accordance with applicable laws and regulations.

3.14.8 Transaction Receipt and Notifications

Merchant transaction receipts must comply with Visa Core Rules and Product and Service Rules, and applicable local laws and regulations.

Merchants may want to consider including the following information in either the actual receipt or a separate transaction record:

- Sender name
- Recipient name
- Sender's payment credential (masked and/or truncated)
- Date and time of transfer
- Amount of transfer in the sender's currency and/or recipient's currency
- Total amount paid (i.e., amount of transfer plus any fees)
- Fees associated with the transaction
- Foreign currency conversion rates for cross-border transactions
- Sender Reference Number
- Description (e.g., Money Transfer)

Merchants should consider providing senders and recipients with notifications related to funds transfer transactions. Notifications are defined as emails and/or SMS/text messages to senders and recipients to provide them with the status of the transfer. They are particularly important for web and mobile channels. Within the transfer process, merchants should ask senders if they want a notification provided to them or the recipient and capture sender and recipient email addresses and mobile phone numbers (if available):

- For sender notifications, merchants should consider providing date and time, amount, recipient name, transfer status, and other related information.
- For recipient notifications, merchants should consider providing date and time, amount, sender name, and other related information.

3.14.9 Recipient Registry and Recurring Transactions

A sender may send funds to the same recipient on a regular basis. This can be set up as a recurring transaction. To facilitate recurring transactions, merchants should consider the following to allow the sender to quickly and easily send funds to one of their frequent recipients:

- Set up a recipient registry with the recipient's name and payment credential
- Provide easy access to the registry to look up the recipient
- Specify the funding account
- Define the interval for sending funds.

3.14.10 Providing Description of Fees (Mandatory)

Depending on the type of payment, (e.g., P2P Money Transfer, Funds Disbursement, prepaid card load, Credit Card bill pay, etc.), merchants must provide senders or customers with information related to fees and other material terms in connection with their OCT-based service. A clear itemized description of all merchant-assessed fees, including foreign exchange fees, if applicable, associated with the transaction must be communicated to senders or customers. Senders or customers must be provided with the opportunity to agree to the fees and proceed with or cancel the transaction.

When different sender and recipient currencies are involved, merchants should provide senders or customers with the currency conversion rate, if known, or an indicative rate. All fees, currency conversion rates, and any foreign exchange markup must be disclosed to the senders or customers. Merchants should consider notifying senders of the following:

- Base exchange rate
- Currency conversion markup fixed by the acquirers, service providers, or merchant
- Final currency rate offered to the sender or customer
- Foreign currency fees that were incurred by the sender or customer in the transaction

3.14.11 Terms and Conditions (T&Cs)

Merchants must provide the T&Cs for their program to the customer. It is strongly recommended that merchants prompt senders to agree to the T&Cs prior to sending any transactions and retain evidence of such consent.

The terms and conditions provided to customers should include, but not be limited to, the topics described in Table 2-10.

Table 2-10: Terms and Conditions Considerations

Topic	Considerations
Product/Service Description	Merchants should provide clear description and details of product/service functionality and features.
Security of PINs and Passwords	• Customers should protect PINs and passwords. • Merchants should provide customers with customer service contacts should the security of PINs/passwords be compromised.
Limits	• Merchants to apply maximum transaction and/or volume limits • Details of limits
Fees/Charges	• Sender agrees to pay fees (set out in transaction fee schedules) • Fees may include service fees, cancellation fees, fees for returns and refunds, and foreign exchange fees • Sender should be aware that the issuer may charge fees to the recipient, in accordance with the Cardholder agreements.

Topic	Considerations
Use	• Who can participate • Whether the service is domestic, cross-border, or both and, where applicable, which currencies are supported on cross-border transactions • How the transaction may be funded (e.g., cash, bank account, Visa account) • What channels are supported (e.g., Internet, kiosk, ATM, mobile), including any restrictions/terms of service • Right of refusal (e.g., merchant may refuse to accept the funding source without reason or explanation) • How the sender will be informed if a funds transfer is not possible and what this means to the sender's account • P2P Money Transfers are not to be used by merchants as a replacement for purchase transactions.
Sending Funds	• The sender will not send funds for illegal, unlawful, or fraudulent activity. • The sender is wholly responsible for providing the correct payment credential of the recipient as well as the correct Money Transfer amount.
Compliance	Merchant reserves the right at any time to block or reject transactions that would or may infringe on legal or regulatory requirements in either the sender's or the recipient's country.
Liability	• Merchant and sender liability associated with the transaction • Merchant policies in the case of sender error (i.e., sender initiated the transaction to the wrong payment credential or sent the wrong amount)
Use of Sender's and Recipient's Personal Information	• Personal information collected from a Visa cardholder as part of a Visa Direct service must only be used for activities related to the Visa Direct service. • The following information can be requested from senders using a Visa card to fund a Visa Direct transaction for use in card and cardholder verification: • Cardholder address (for account verification check) • Merchants are prohibited from storing the CVV2 information following authorization of a Visa transaction. If card payment credential and expiration date are stored, data must be stored in accordance with the PCI DSS. • Recipient card accountholder address, card expiration date, or CVV2 are not required to be collected to initiate OCTs.
Dispute Policies and Procedures	Clear dispute policies and procedures including information to the sender in case of a dispute such as a customer service telephone number or an email address.
Funds Availability	• Any delays in availability of funds • Sender should contact the service provider or merchant if the recipient has not received funds within the specified timeframe. • Recipient should contact the issuer. If non-delivery of funds is due to cardholder limits, the cardholder can ask the issuer to adjust.
Contact Information	Merchants should provide relevant customer service information, such as phone numbers, website URLs, and/or an email address to the sender.

3.14.12 Fraud Detection and Prevention

Fraud prevention should occur on both the funding transaction (e.g., AFT or on-us proprietary message) for Money Transfer programs as well as on the OCT for all types of programs.
The merchant has little recourse with the issuer if the funding transaction proves fraudulent. Risk management tools for the funding transaction should be built into processing systems to detect and prevent fraud, errors, sanctions, violations, and money laundering and terrorist financing.

Such tools include government-issued photo identification, ATM PIN, Internet or telephone banking identification and password, CVV2 verification in the AFT, Visa Secure, Address Verification Service (AVS), negative files and screening, and systems control tools to identify processing errors and suspicious activity.

While fraud reporting on an OCT is generally low, merchants must still have processes in place for monitoring OCTs to recipient accounts to identify suspicious activity, potential fraud, and misuse of OCT programs.

3.14.13 Transaction Limits

Merchants should confirm that the funds transfer amount is equal to or less than the Visa limits.
For domestic and cross border Money Transfer OCTs, merchants cannot send more than US$2,500.00 in a single OCT, unless Visa permits a higher country limit.

For other OCTs, the VisaNet system edit/transaction limit is US$125,000.00, although lower limits may be defined on a country or program basis.

Merchants should ensure that they are not allowing senders to send OCTs to single recipient accounts in excess of the VisaNet limits. Limits are outlined in Table 2-11.

Table 2-11: Transaction Limits - Velocity Limits

OCT Transaction Type	Transaction Category	Time Period		
		One-day	Seven-day	Thirty-day
Domestic	Money Transfer OCT	150 transactions or USD 20,000	250 transactions or USD 50,000	750 transactions or USD 100,000
	Non-Money Transfer OCT	150 transactions or USD 100,000	250 transactions or USD 250,000	750 transactions or USD 500,000
	Non-Money Transfer (Europe/Intra-EEA)	150 transaction or USD 250,000	250 transaction or USD 600,000	750 transactions or USD 1,250,000
U.S. Domestic Me-to-Me (BAI AA)	Money Transfer OCT	150 transactions or USD 100,000	250 transactions or USD 250,000	750 transactions or USD 500,000
Cross-border	Money Transfer OCT	30 transactions or USD 10,000	50 transactions or USD 25,000	150 transactions or USD 50,000
	Non-Money Transfer OCT	30 transactions or USD 50,000	50 transactions or USD 100,000	150 transactions or USD 200,000

3.14.14 Transaction Monitoring and Controls

Merchants must establish controls and monitor transaction activity for signs of misuse of the OCT for the payment of goods and services.

Controls and monitoring for fraud money laundering and terrorist financing, should include:

- Transaction controls and velocity limits based on transaction risk (e.g., by use case – P2P Money Transfer vs. Funds Disbursement, domestic vs. cross border transactions, etc.)
- Suspicious activity monitoring, for example:
  - A significantly large number of transactions initiated by a single sender to multiple recipients within a specified time period.
  - A large number of transactions from multiple senders to the same recipient account within a specified time period.
  - A high number of OCTs followed by disputes, especially involving the same sender and/or recipient.
- Corridor definition for payments and sanctions screening:
  - Define the countries to which OCTs will be allowed to be sent.
  - Screen senders and recipients against relevant lists per applicable local laws and regulations. Specific issuers, countries, or products may be blocked from receiving OCTs in VisaNet.
  - Ensure that the sender and the recipient are not on any applicable government or bank-specific blocked lists (e.g., Office of Foreign Asset Control (OFAC) list or United Nations list). If the sender is already a customer of the acquirer, service provider, or merchant, he/she may have already been screened as part of the acquirer's, service provider's, or merchant's ongoing customer due diligence program and may not need to be screened again.
  - Include sender and recipient data as required in the Money Transfer regulations.

To mitigate against the risk of the misuse of the OCT for the payment of goods and services (OCTs alone cannot be used for the payment of goods and services), merchants must establish and enforce per transaction and cumulative velocity limits for OCTs. Limits may include, but are not limited to:

- Per transaction count and amount limits by day, week, and month.
- Set limits on the number of P2P Money Transfers that can be initiated and sent from/to any single account in any given day, week, or month.

3.14.15 Sanctions Screening for Merchants

Merchants must screen senders and recipients against relevant lists per applicable local laws and regulations, such as government or bank-specific block lists.

Merchants should check whether the issuer can receive OCTs. To comply with local regulations, specific issuers, countries, or products may be blocked from receiving OCTs in VisaNet.

At their discretion, merchants can define the countries to which they will allow OCTs (i.e., corridor definitions).

On cross-border transactions, merchants should check to ensure that the country that the recipient resides in is part of the merchant's program (as defined in the acquirer submitted PIF).

Merchants should ensure (per applicable local law or regulation) that the sender and the recipient are not on any applicable government or bank-specific blocked lists (e.g., Office of Foreign Asset Control (OFAC) list). If the sender is already a customer of the merchant, he/she may have already been screened as part of the merchant's ongoing customer due diligence program and may not need to be screened again.

4.0 Compliance

4.1 Paysafe Website Requirements

Please ensure that your website is fully compliant as per our requirements. Your funds will not be remitted until we are satisfied that these requirements are in place. Should you have questions regard Website Compliance please contact our Customer Services team immediately.

The rules of Website Compliance are that you must clearly display your:

- **Company's details, including:**
  - Your company's legal name
  - Your company's registered office address (incl. main country of domicile)
  - The address of your permanent headquarters
  - Your company's registered number
  - A contact telephone number or contact email address
- **Terms and Conditions of sale**
- **Company Policy**
  - Covering refunds, returns and cancellations and a 'Click to accept' button, or other acknowledgement, evidencing that the Cardholder has accepted the return/refund policy on your check out page
- **Consumer Data Privacy Policy**
- **Security Capabilities and Policy**
- **For the transmission of payment card details**
  - Shipping Policy – if applicable
- **Including delivery methods and timing and any export restrictions**
  - Description
- **An accurate description and pricing (including currency) for all goods and services which are available to purchase on your website**
- **Currency of transaction**
- **Your outlet country**
  - Either on the same screen view as the payment page used to present the final Transaction Amount; or within the sequence of web pages the Cardholder accesses during the payment process.
- **Paysafe Logo (optional)**

4.2 Key Scheme Requirements

- Website(s) - Must be fully functional and must contain at a minimum the following:
  - Clear card scheme information. Both card schemes need their logos to be displayed on e-

commerce payment pages as evidence that they take part in the service. Merchants should note that card scheme logos must be used in accordance with the guidelines established by the card schemes and must not be modified or distorted in any way. Merchants are responsible for their own compliance with the card schemes' guidelines. For full MasterCard (and Maestro) guidelines and logo files visit: **www.mastercardbrandcenter.com**

- Visa Brand Mark in full colour to indicate acceptance of all Visa Cards should be included, or, effective from 9 June 2016, the Visa Mark that represents the Product Category(s) that the Limited Acceptance Merchant has chosen to accept for payment. We have available several different Visa logos (including the standard Brand Mark and Verified by Visa) in various file formats, along with guidelines for use which can be sent on request. Please email uk.customerservice@paysafe.com with details of your requirement.

- Contact Information

  - It is a requirement of Visa and MasterCard that if you are carrying out mail or telephone orders, you should include a contact number rather than location within the description.

    For instance – 'Sally's Shop, London', should be shown as 'Sally's Shop, 01408 123 4568'. This encourages customers to call you to help identify their transaction, rather than disputing with their card issuer.

    With e-commerce transactions, you must display your internet website address or email address on Cardholders' statements so that customers can contact you.

- PCI DSS

  - See Section 4.1 for more details.

- Fraud Monitoring

  - You must use security checks, as recommended by the card schemes, as they can help you identify possible fraudulent transactions. However, they do not prevent fraud or shift the legal responsibility for fraudulent transactions, which may result in chargeback claims. Further information can be found below in section 4.1.

- 3D Secure Cardholder Authentication

  - Cardholder authentication generates new message values to show the level of security being used, plus the result of the authentication. You must make sure that you fully understand the responses sent to your authentication solution by the card schemes.

- Merchant Classification code

  - You will be allocated a Merchant Classification Code (MCC), which identifies your business type, for example Andrew Holidays would be given a 'travel' MCC code. If the business, then decided to diversify and start selling bicycles a new processing arrangement would need to be agreed.

- Further information

- The above has outlined the key points required by the schemes for full details of their rules and operating regulations you can refer to the scheme guides: **https://www.mastercard.com/us/merchant/pdf/BM-Entire_Manual_public.pdf**

5.0 What is PCI DSS?

From the world's largest corporations to small Internet stores, compliance with the PCI Data Security Standard (PCI DSS) is vital for all merchants who accept credit cards, online or offline, because nothing is more important than keeping your customer's payment card data secure. The size of your business will determine the specific compliance requirements that must be met. See Section 8.1 below for more details.

PCI DSS requirements are regulated by the PCI Security Standards Council (PCI SSC). The Council's five founding global payment brands - American Express, Discover Financial Services, JCB International, MasterCard, and Visa Inc. - have agreed to incorporate the PCI DSS as the technical requirements of each of their data security compliance programs. The standards inform mandatory information security requirements to protect sensitive Cardholder information while storing, processing and transacting data.

The PCI Security Standards Council provides a Quick Reference Guide to the PCI Data Security Standard to inform and educate merchants and other organisations that process, store or transmit Cardholder data.

You are required to be PCI DSS certified at all times and must let us know by email uk.customerservice@paysafe.com immediately if you are not certified at any point during your relationship with us. We will work with you and our third-party supplier to regain compliance.

The PCI DSS follows common-sense steps that mirror security best practices. There are three steps for adhering to the PCI DSS – which is not a single event, but a continuous, ongoing process.

Paysafe partners with Sysnet, a provider of security and compliance management software which helps to assess and monitor compliance on your merchant account. For more on Sysnet, see section 4.1.

PCI DSS is designed to protect your business and customers against data security risks, and you must take steps to ensure that you are compliant always to ensure you and your customers are protected. Customers will need to certify compliance on an annual basis; as an acquirer, Paysafe is responsible for quarterly reporting of our customers' PCI-compliance status to Visa and MasterCard.

Customers who are non-compliant are at risk of Paysafe monthly non-compliance / service fees. Paysafe is charged directly by the Card Schemes for merchant non-compliance, and will re-charge the following fees to the merchant immediately upon receipt:

- Card Scheme non-compliance fees;
- Card Scheme fines for storing Sensitive Authentication Data (SAD) post- authorisation e.g. (Card Security Code); and
- Card Schemes fines (for loss of card data, associated fraud spend, loss of business and reputation) in the event of a data breach.

5.1 Sysnet

Sysnet is a third-party company that specializes in PCI compliance management. Depending on the frequency and volume of transactions, each account will be assigned a unique classification. Based off that classification, Sysnet will identify which steps may be required for the account to be certified compliant. These steps may include system scans (which Sysnet's software can complete) and will always include regular questionnaires.

5.2 PCI Classification

All merchants will fall into one of the four merchant PCI levels based on card transaction volume over a 12-month period. The table below describes the levels and the associated PCI requirements.

<table>
<tr><th>Level 1</th><th>Level 2</th><th>Level 3</th><th>Level 4</th></tr>
<tr><td>Over 6 million Visa or MasterCard transactions a year</td><td>1 to 6 million Visa or MasterCard transactions a year</td><td>20,000 to one million Visa or MasterCard e-commerce transactions per year</td><td>less than 20,000 Visa or MasterCard transactions per year (e- commerce only)</td></tr>
<tr><td>Annual on-site audit carried out by a Qualified Security Assessor (QSA), providing a Report on Compliance (ROC)</td><td colspan="2">Annual Self-Assessment Questionnaire (SAQ)</td><td>Annual SAQ recommended</td></tr>
<tr><td colspan="2">Quarterly vulnerability scan by an Approved Scan Vendor (ASV)</td><td colspan="2">Quarterly vulnerability scan by an Approved Scan Vendor (ASV) – if applicable</td></tr>
<tr><td colspan="3">Attestation of Compliance Form</td><td>Compliance validation requirements in Sysnet</td></tr>
</table>

Remember: It is your responsibility as the merchant to take steps to ensure that you are PCI compliant and always to ensure you and your customers are protected.

6.0 Legislation

6.1 Distance Selling Guides

If you sell products or services to customers where they do not have the opportunity to physically see the goods or discuss services face-to-face, then both the Consumer Contracts Regulations (CCRs) and E-commerce Regulations (ECRs) apply. This is the case for both e-commerce and MOTO transactions.

The European Consumer Rights directive aims to ensure that there is a minimum level of consumer protection across the European Union. In the UK, the Consumer Contracts Regulations implements this directive in UK law. Remember – these are legal requirements: not only will failures to comply mean your contract with us may be terminated; you could also be taken to court.

6.2 Three key facts about the CCRs

- You cannot charge customers for additional items by using a pre-ticked box.
- You must allow customers the option of cancelling a service contract online, such as a gym membership.
- You must refund customers within 14 days of cancellation, or from the date goods are returned.

6.3 You must provide customers with the following information before the transaction:

- a description of the goods or service, including how long any commitment will last on the part of the consumer
- the total price of the goods or service, or the manner in which the price will be calculated if this can't be determined
- cost of delivery and details of who pays for the cost of returning items if you have a right to cancel and change your mind
- details of any right to cancel - the trader also needs to provide, or make available, a standard cancellation form to make cancelling easy (although you aren't under any obligation to use it)
- information about the seller, including their geographical address and phone number
- information on the compatibility of digital content with hardware and other software is also part of the information traders are obliged to provide

You must ensure that you are familiar with the latest rules and regulations relevant for distance selling. It is your responsibility to know and comply with your obligations. For more information visit:

https://www.gov.uk/online-and-distance-selling-for-businesses

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/429300/bis-13-1368-consumer-contracts-information-cancellation-and-additional-payments-regulations-guidance.pdf

6.4 CNP refunds

- It is recommended that you reference the ECRs and CCRs in your refunds and returns policy.
- Refunds must be processed using the same card as used for the original transaction; in the event the card account is closed another card may be used. Failing this, a credit can be made to a bank account. Ensure that your procedures in this case are clear.
- A refund amount must not exceed the amount of the original transaction.
- A refund must not be made to credit winnings from gaming

7.0 Chargeback and retrievals

When a Cardholder queries a transaction with their card issuer, that issuer will investigate, and in the event they find the transaction to be invalid they will refund the amount and initiate a chargeback. Following the procedures set out in this guide will help you to prevent chargebacks and the associated costs (both time and money).

Our dedicated chargeback team will be in touch once you go-live to ensure that you are familiar with the processes and will provide you with contact details should you have any future queries.

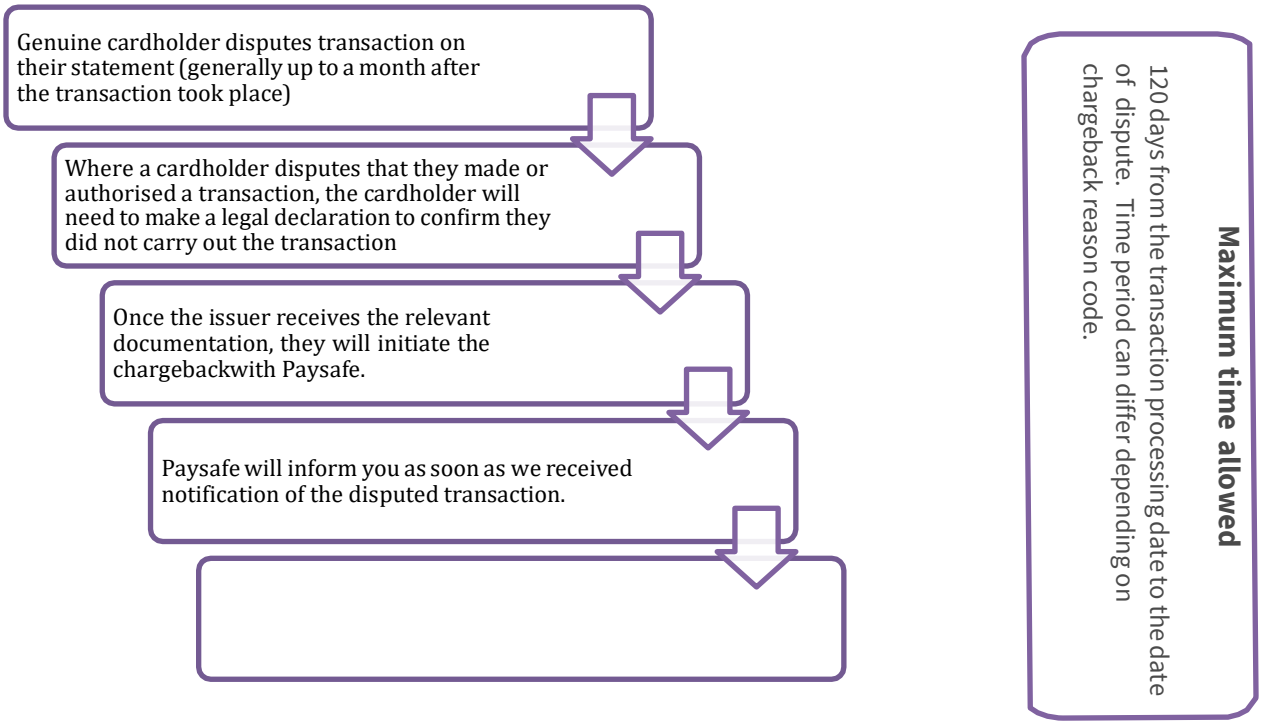
7.1 Common chargeback reasons

- The Cardholder claims they did not undertake the transaction (they claim fraudulent use)
- Goods or services not as described, faulty or not receive
- Failure to respond to a retrieval request on time
- The card date was invalid at the time of the transaction i.e. before card was live or after expiry.
- Technical reasons such as duplications
- Failure to comply with procedures in the Merchant Terms e.g. failing to obtain authorisation
- The card was not valid for CNP transactions (e.g. ATM-only card)
- You exceeded your agreed floor-limit without authorisation (either with asingle transaction or a split transaction)

7.2 Reducing the risk of chargebacks

- Only accept card types outlined in the Merchant Terms.
- Process transactions correctly in accordance with card type.
- Keep records of all transactions for a minimum of 13 months.
- Ensure your returns policy is clear and easy for your customers to access

7.3 Chargeback process



Note: Paysafe will automatically reject any chargebacks which are not within card scheme time limits,or where the correct documentation is not provided.

7.4 Request for information

A request for information (RFI), also known as a retrieval request, is when a card issuer asks for a copy of the transaction on behalf of the Cardholder.

An RFI may be requested when the Cardholder does not recognise the transaction on their statement; often this is because the description on the statement does not match the company name. Paysafe is pleased to process auto-fulfilments for its merchants, meaning that they do not need to provide any transaction information unless specifically requested.

To prevent unnecessary RFIs by encouraging customer contact, both Visa and MasterCard require that:

- Merchants predominantly undertaking MOTO transaction should include a contact number in their description; and
- E-commerce merchants must display an email or web address in their description.

7.5 When responding to RFIs or chargebacks requested by Paysafe, be sure to:

- Reply by the date quoted, by the agreed channel;
- Provide clear, legible information; and
- Send all documentation to support the transaction, including details of authorisation codes, time and date of transaction, terms and conditions etc.

Always respond promptly to 'request for information' letters, as you may be able to prevent a chargeback. Failure to supply a legible copy of the transaction within the stated time (usually 14 days) may mean a chargeback is initiated.

Remember, an RFI does not represent a loss to your business; a chargeback does!

7.6 Chargeback protection

Since e-commerce transactions do not allow the Cardholder or card to be verified at the point of sale, they have historically carried a higher risk than face-to-face transactions. For this reason, the Card Schemes introduced the use of 3D Secure.

Using 3D Secure allows you to prove that the Cardholder used their card at the time of the transaction. Without this, you would not be able to provide evidence that the genuine Cardholder was using their card, and the issuer would chargeback the transaction to you.

It is important you continue existing fraud checks to reduce the risk of fraud as far as possible. Failure to do so could result in chargebacks.

7.7 Protection levels

Where you adhere strictly to the protocol, using 3D Secure (see Section4.1) helps prevent chargebacks where cards are used fraudulently, or where the Cardholder denies using the card; liability shifts from you the merchant, back to the card issuer.

Whether you are protected from chargebacks by the card schemes will depend on the card being used AND the type of authentication.

- Visa Credit, Visa Debit, Visa Electron and Visa Commercial (European-issued cards):
  - Global transactions with full or successfully attempted authorisation.

- MasterCard Credit:
  - Global transactions with full or successfully attempted authorisation.

- Maestro applies different rules for UK and internationally issued cards. Where both the Card Issuer and the Merchant are in the UK
  - Global fully-authenticated transactions
  - UK-domestic transactions with successful attempted authorization

8.0 Changes to your business

We know that contact details can change, so it is important for Paysafe to have a full and complete list of key contacts within your business. This is so that we can keep you advised of any regulatory information and system updates but also to let you know of any changes to our products and services.

8.1 Service changes

You must inform us by email (uk.customerservice@paysafe.com) if you change any of the following:

- Your website address (including addition of new websites)
- The number of sites you have
- The warranties or guarantees for your products or services
- The nature of your business (e.g. a change to the goods or services you provide)
- The legal entity of your business (e.g. moving from sole trader to limited company)
- The terms on which you sell products/ goods (e.g. changes to delivery times, refund process, or deferred payments)
- Any other information from your original application; or if
- You no longer wish to accept card payments.

8.2 Contact changes

You must inform us by email (uk.customerservice@paysafe.com) if you change any of the following:

- Contact numbers
- Bank account details
- Postal addresses
- Email addresses
- All contact names (including partners, directors and owners); or if
- A new partner/director joins or a partner/director leaves

8.3 Financial information

You must inform us by email (uk.customerservice@paysafe.com) if any of the following events occur:

a) an Insolvency Event (as defined in the Merchant Terms);
b) change of control in you or your parent company;
c) change in your trading terms, directors, other officers, business or trading name, legal status, business or trading address or in any of your other details that you have provided to us; and
d) sale or other disposal of all or any material part of your assets which may result in a material adverse change to your Business

9.0 Merchant Back Office

For information about our Merchant Back Office, please see the Getting Started guide which can be downloaded here.