



increase your resistance

How card not present gaming companies can minimise
the risk of losing money through chargebacks

protect yourself

We know that receiving a chargeback can cause concern. We also know that there are certain risks you face in your line of business which could lead to chargebacks.

As an internet Card Not Present (CNP) gaming company you're particularly prone to fraud, so you could receive chargebacks from the genuine cardholder.

This guide gives you useful information to help you protect your business from the financial losses chargebacks can cause. It also tells you what you can do to help us defend you from a chargeback if you do receive one. It could save you both time and money and help keep your business running smoothly.



The Card Scheme rules you must follow

It's compulsory to follow these rules, and it's also in your own interests because they will help reduce the risk of chargebacks.

- Regardless of the card type used (Visa/MasterCard/Maestro), each transaction will be identified using Merchant Category Code 7995. This applies to all internet gaming transactions. Failure to identify transactions correctly reduces an issuer's ability to make informed authorisation decisions and often leads to higher fraud losses.
- You must ask each prospective customer to identify his or her physical location at the time of the activity. Some jurisdictions prohibit gaming; if your customer is in one of these locations you must not proceed with the transaction. You must record the customer's response, retain it and make it available to Barclaycard for a minimum of one year after the date of the transaction.
- Gaming merchants must not sell electronic chips or electronic currency for use at internet casinos, other than that registered to you.
- You must authorise all transactions (please note authorisation does not guarantee Payment). Also, CSC validation is required.
- Visa, MasterCard and Maestro allow internet gaming transactions; Maestro can only be accepted over the internet with SecureCode authentication. Not all Maestro issuers allow their cards to be used for eCommerce transactions.
- All gaming websites must have a disclosure about specific rules related to Card Schemes, which the customer must see before they proceed with the transaction/s (see page 5 for individual scheme requirements).

The following terms and conditions apply

- JCB cards are not permitted for gaming or betting transactions and must not be accepted.
- The floor limit for all transactions will be zero.
- Multiple cards from the same customer are permitted.
- You must inform us immediately if there is any threat to your applicable gaming/trading license and supply details of any action that is being taken to preserve the license.
- You must inform us immediately of any disputes or litigation in respect of unlawful gaming, or any circumstance in which the integrity of your systems is challenged or where there is a reputational risk.
- Indemnification
You shall indemnify us against any and all claims, losses, damages, liabilities, fines or penalties, demands, proceedings and actions, charges, costs and expenses that we sustain or incur, or may incur arising out of or in relation to or by reason of any claim or legal proceedings against us or you in respect of your activities. In any proceedings brought against us where you are indemnifying us, unless we agree otherwise we will reasonably consult with you in respect of any action we take in respect of such claim
- You must operate a membership registration procedure which encompasses a comprehensive cardholder identification check, and be able to demonstrate that you have procedures in place to comply with money laundering regulations.

other requirements

In addition to the rules outlined on page 3, each Card Scheme has their own set of requirements which you'll also need to meet.

Visa



- Winnings **must** be credited to the cardholder via the Original Credit Transactions (OCT) programme (see the back of this guide for glossary).
You must have a separate merchant number for OCTs.
- The amount of the OCT must not be more than 80,000 (or the sterling equivalent) for Visa Europe transactions or \$50,000 (or the sterling equivalent) for Visa non-Europe transactions.
- If you are submitting more than one OCT in respect of a Cardholder the amount on any day should not exceed 80,000 (or the sterling equivalent) for Visa Europe transactions or \$50,000 (or the sterling equivalent) for Visa non-Europe transactions.
- You must not submit an OCT where the country is included within the VISA OCT Exclusion list.
- **No refunds are to be processed to the card for winnings** – except in the event of a game/race cancellation, or if the transaction is duplicated when the cardholder may then be refunded their stake by means of a refund back to the card number used in the original transaction. These refunds should be processed via your normal sales merchant number.

You must also display the following on your website:

- a disclosure to cardholders. Please make sure that the cardholder views this before proceeding with their transaction. You **must** include the following wording:
'Internet gaming may be illegal in the jurisdiction in which you are located, if so, you are not authorised to use your Payment card to complete this transaction.'
- a complete description of the rules of play, your cancellation policy and your payout policy
- a statement recommending that the cardholder retains a copy of the transaction details, along with the policies and rules
- the Barclaycard Payment Acceptance Identification Number 10021373 (this should be shown on your Payment page)
- country of domicile – this is to be clearly disclosed to cardholders immediately prior to completion of Payment instructions.
- a statement of the cardholder's responsibility to know the laws concerning online gaming in his/her country of domicile
- a statement prohibiting the participation of minors

other requirements

MasterCard/Maestro

- Display a notice on your website before the system allows the MasterCard number to be inserted. This must state that in some jurisdictions gaming is not lawful and suggest that the customer checks consumer law in the country of location before proceeding with the transaction.
- Any additional fee charged (whether or not it is included in the total transaction amount) must be clearly disclosed to the cardholder before completing the transaction.

MasterCard

- Internet/E-commerce, Mail order & telephone transactions-the payments of winning (and unused funds) back to MasterCard credit or debit card is permitted in the EU region only (where countries are supported by Barclaycard and MasterCard) and only by you initiating a Payment Transaction (PT)
- Payment Transactions are not permitted on corporate cards.

Maestro

- For MOTO and eCommerce gaming transactions the payment of winnings for Maestro cards must be made using an alternative method such as Payment Transaction or BACS payment. Refunds and Payment transactions will not be permitted
- The payment of winnings back to a Maestro card is permitted only by you initiating a PT subject to the following criteria for the respective transaction types:
- Internet/E-commerce-in the EU region only and only for those countries supported by Barclaycard and MasterCard
- Mail Order & Telephone – for UK, Ireland & France domestic transactions only
- A refund transaction type is permitted for the use of unused funds back to a cardholder for Maestro cards.

MasterCard/Maestro PT (only) Special Procedures

- The amount of the PT must not be more than €50,000.00 or the sterling equivalent
- If you are submitting more than one PT in respect of a cardholder, the amount on any day should not exceed €80,000 (or sterling equivalent) Please refer to limit specified under Merchant agreement.
- You may only submit a PT for those countries that are included within the MasterCard Acceptance list
- For Internet/Ecommerce transactions only you must have processed the original sale using SecureCode
- For Mail Order and Telephone CVV2 is mandatory for the original CNP Gaming transaction
- All submission methods for refunds must be submitted for an online authorisation.

Card exceptions

- Some Card Issuers won't allow gaming transactions on their cards. This will instigate a decline message as the Payment is disallowed by the issuing bank. Unfortunately, there's no definitive list of the banks which follow this practice and those who do may change from time to time.
- Some issuers will charge a 'handling fee' as the purchase isn't for actual goods but a gaming transaction which may have a return by way of winnings. There's no definitive list of the banks which follow this practice and, again, those who do may change from time to time.

general protection measures

We recommend you use the following tools and procedures to help make accepting Payments more secure and so to protect yourself from chargebacks.

Internet authentication

This is an industry-wide initiative to fight fraud and to protect businesses trading over the internet. It allows card issuers to request that their cardholders enter a password when conducting a card transaction over the internet. The version for MasterCard is called 'SecureCode' and Visa's is 'Verified by Visa'. Please note that SecureCode is mandatory for Maestro acceptance.

Velocity checks and fraud screening tools

Install a checking facility within your in-house computer system. This will keep a note of transactions for individual card numbers, cardholder names and given addresses, so you'll know when different card numbers have been used against the same address and when cards that have caused problems in the past have been used. If you'd like advice about the tools available, we can help – just ask us.

general protection measures

Asking for details

For internet transactions you must obtain the following details:

- the card number
- the card's expiry date
- CSC (this is mandatory for all non-face-to-face transactions – see back of this guide for glossary)
- the cardholder's full name and address, as held by the card issuer, including the postcode and telephone number
- the gross amount (including any added charges) of the transaction.

Please note: To comply with Payment Card Industry Data Security Standard (PCI DSS), CSC should not be retained post authorisation.

We also recommend that, when setting up the account, you request identification documents from the customer such as a passport or driving licence.

recognising transactions

Cardholders may raise a dispute if they don't recognise the details that appear on their card account statement (the statement narrative).

While Card Issuers encourage their cardholders to retain transaction details so that they can use them to check their statement, in reality cardholders often don't do this – particularly with internet transactions.

We encourage you to make sure your statement narrative is as meaningful as possible so that cardholders will easily recognise a transaction – this can prevent a dispute occurring.

If you think you're receiving a large number of requests for information or other disputes, then it may be because the narrative that appears on the cardholder's statement is misleading. To check the details that appear for your business on a cardholder's statement, please call our Customer Contact Centre on **0844 811 6666***. If you're not happy with what is shown we can amend this for you.

Below is an example of how your details should appear

First line: 18 characters maximum Second line: 13 characters maximum

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Examples																	
G	A	M	I	N	G	.	C	O	.	U	K						
1	2	3	4	5	6	7	8	9	10	11	12	13					
0	8	0	2	1	1	2	2	3	3	4	4	5					

requests for information

A 'Request for information' occurs when a cardholder raises a dispute with their Card Issuer. The Card Issuer then requests details of the transaction in order to resolve the dispute. A request for information may also be raised by a Card Issuer.

Disputes may arise for a number of reasons, including:

- the cardholder claims they don't recognise the name, address, amount and/or transaction date against a transaction on their card statement
- the cardholder claims a transaction has been duplicated (in this case you'll need to provide evidence that the cardholder entered into two or more separate transactions)
- the cardholder requires a breakdown of the charge (particularly if the charge relates to a number of bets and therefore the total charge is made up of several elements)
- the cardholder claims that their card has been used without their authority or consent (i.e. fraud has occurred).

It is critical that you supply a clear and legible copy of any transaction details as specified within 14 days of our request. Failure to do so may mean that the Card Issuer charges the transaction back to you for non-receipt.

compelling evidence

If a cardholder denies making the bet/undertaking the transaction, the onus is on you to prove that the transaction is genuine and not due to fraud.

If you are charged back, acceptable 'compelling evidence' that will help us defend you includes:

- proof that a credit or reversal was processed
- evidence that an earlier transaction with the same cardholder was fully authenticated and not later disputed
- details of a long-standing account/customer relationship between your company and the cardholder (e.g. account opening information)
- evidence of personal details you've received from the cardholder (e.g. passport, driving licence, electoral roll check, landline telephone number)
- proof that the cardholder has accepted historic winnings
- a copy of any official identification documentation such as a passport or a driving licence you may hold on your records
- email correspondence between yourselves and the cardholder.

Please note that we can't guarantee this evidence will be accepted by the Card Issuing Company and therefore the chargeback may remain on your

account. The next section details what evidence you'll need to provide for different types of chargebacks.

defending you against chargebacks

If you do find you receive a chargeback, we may be able to defend you against it if you can give us the appropriate evidence.

Reason codes Visa 83, MasterCard M37 and Maestro 37

These codes mean the cardholder denies participating in or authorising a transaction that's been processed to their account.

To defend these codes we'd need you to provide us with evidence that the genuine cardholder has authorised this Payment and participated in the transaction. You'll need to send us:

- evidence that the cardholder, with the same name and address, has used your gaming services before and they've not disputed previous betting or winnings received[†]

- details of the cardholder's identity, for example a copy of the signature page of the customer's passport or a copy of a utilities bill showing the genuine cardholder's name and address.[†]

[†] We can't guarantee that we'll be successful in defending a chargeback with this evidence.

Reason codes Visa 72, MasterCard 08 and Maestro 08

These codes mean that authorisation wasn't obtained for a transaction where a code was required.

You'll need to provide us with proof that authorisation was obtained with an authorisation code that matches that issued by the Card Schemes and shows on their authorisation logs.

Reason code Visa 75

This code means that the cardholder doesn't recognise all or part of the transaction details.

We'll need evidence that helps the cardholder to recognise the transaction. This could include:

- the name of the customer
- any other customer details
- the goods or services that they've been provided
- the date the goods or services were provided
- your outlet name, if it's different to what's shown on the customer's statement.

points to remember

- Authorisation doesn't guarantee Payment. It confirms that the card hasn't been reported lost or stolen at the time of the transaction and that there are sufficient funds on the account.
- The 14-day timescale for retrievals must be adhered to – there are no exceptions to the rule.
- When designing your site and the tool to take card Payments, you should be aware of any appropriate local laws where you are trading and how these will affect your capability to proceed with these transactions.
- Clear and informative statement narratives may reduce your volume of retrieval requests. These details enable the cardholder to view transactions on their statement that they may not have been familiar with at first. Upon viewing the statement narrative, the cardholder may familiarise themselves with the transaction. If, however, there is any cause for dispute they should come to you directly; hence you get the chance to resolve the issue before there are any chargeback and dispute procedures initiated.

glossary

Listed below is a summary of the terminology which you may hear or see quoted in documentation.

Internet gaming transaction

A transaction that is conducted over the internet with a gaming company/provider and the card is not present.

Card Security Code (CSC)

This is located on the back of MasterCard and Visa Credit or Debit cards and is typically a separate group of three digits on the right of the signature strip. On American Express cards this is a printed group of four digits on the front of the card towards the right.

Original Credit Transactions (OCT)

A Visa initiative to enable Payment of winnings to be credited back to the card number used in the original transaction, without processing a standard refund, (which is now forbidden). This was previously referred to as CFT (Cardholder Funds Transfer).

Chargeback rights are not available for winnings, unspent chips and/or residue value. Original credits may be charged back if the recipient (Card Issuer) refused the OCT or the OCT is prohibited by law.

Payment Transaction (PT)

An alternative method for the payment of winnings to MasterCard and Maestro cards.



in conclusion

If a transaction is disputed at a later date, it's imperative that you provide all of the information you hold on your records as detailed in this document. We'll do everything we can to defend chargebacks on your behalf if you provide us with the necessary compelling evidence.

For more information, please take a look at our booklet, 'Your introduction to chargebacks and retrievals', call us on **0844 755 0094*** or visit **www.barclaycard.co.uk/business/existing-customers/chargebacks**

Please ensure that all card data is protected in accordance with the Payment Card Industry Data Security Standard (PCI DSS). For further information see: www.barclaycard.co.uk/pcidss or www.pcisecuritystandards.org

This information is available in large print,
Braille or audio format by calling **0844 811 6666***

*Calls may be monitored and/or recorded to maintain high levels of security and quality of service. Calls to 0844 numbers will cost no more than 5.5p per minute, minimum call charge 6p (current at October 2013). The price on non-BT phone lines may be different.

Barclaycard is a trading name of Barclays Bank PLC. Barclays Bank PLC is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority (Financial Services Register number: 122702) and subscribes to the Lending Code which is monitored and enforced by the Lending Standards Board. Registered in England No: 1026167. Registered Office: 1 Churchill Place, London E14 5HP. BCD111605BROB5. Updated: 03/15. 24366BD.