



VoicePay®

Chargeback & Anti- Fraud Guide v1.1

December 2008

Table of contents

1. Introduction	3
2. Who accepts credit cards?.....	3
3. What are chargebacks and retrieval requests?.....	3
4. Time scales.....	4
• How long does a chargeback/retrieval request take?.....	4
5. Chargeback time scale formula.....	4
6. The chargeback/retrieval request process	4
• Chargebacks/retrieval requests occur as follows:	4
7. Why do chargebacks/retrieval requests occur?	5
• Fraud	5
• Product quality.....	6
• Customer service problems	6
• Refund problems	6
• Processing problems	7
8. Representments – disputing a chargeback	7
9. The good faith/collection assistance process	9
10. How you can help yourself	9
• General	10
• Website requirements.....	10
• Delivery of your product/service.....	10
• Product quality/customer service/refund policy	10
• Refunding a transaction.....	11
• Practical advice on avoiding fraudulent chargebacks.....	11
• Review transactions manually- identifying risky transactions	12
• High-risk countries.....	12
• Useful websites for further information and advice.....	13

1. Introduction

In certain circumstances a card holder may wish to dispute a transaction.

This can happen for a number of reasons, including card misuse, genuine processing errors, or the card holder being dissatisfied with the goods or level of service provided. When a transaction is disputed, the card issuer and the acquiring bank operate according to clearly defined and well-established procedures to resolve the dispute. These procedures are designed to establish whether the merchant should receive (or retain) the disputed payment or whether the funds should be returned to the card holder's account. The process of returning the funds to the card holder is known as a chargeback.

To reduce the number of chargeback's it is essential that merchants and acquiring banks carefully monitor disputed transactions and respond promptly to retrieval requests. If a merchant is receiving a large percentage of disputed transactions they are required to take corrective action to prevent disputes from arising, or they may face fines from the card schemes.

The chargeback process can be long and drawn out (due to the processes and procedures of the card issuing banks, the card schemes, and the merchant banks). Those parts of the process that are under the control of VoicePay ® are fully automated and so are as speedy and efficient as possible.

2. Who accepts credit cards?

Basically, there are two kinds of merchants that accept credit cards:

1. **Card present** – A card is swiped through an electronic card swipe machine and data is automatically sent to the processor for authorisation. Once the merchant has received the authorisation, the acquiring bank takes responsibility for any stolen cards or fraudulent transactions.
2. **Card not present (MOTO/Internet)** – The merchant gets the credit card information by phone, mail, or the internet, and the card is not swiped. These are called moto transactions (mail order/telephone order). Card holders have significant chargeback rights if they pay in this way. Internet orders also fall under this category.

3. What are chargeback's and retrieval requests?

Chargeback's are the full reversal of a transaction by the card issuer. A chargeback is generated when a card holder disputes a transaction on their credit card statement.

A request for information or documentation request is a request from the card holder's issuing bank for copies of a signed sales receipt or other suitable documentation to prove the validity of a transaction.

A retrieval request is also known as a "first request" or a "request for information" (rfi). A retrieval request is issued when a card holder does not recognise a specific transaction on their credit card statement.

A card holder's issuing bank may generate a retrieval request if it is detected as fraud.

4. Time scales

4.1 How long does a chargeback/retrieval request take?

The time scales vary for each chargeback reason and card scheme. A chargeback may be raised several months after the original transaction. The first chargeback time limit is generally calculated from one of two dates:

1. The date the transaction is processed by the card scheme, or;
2. The date of expected receipt of services (e.g., for travel services, the expected date of travel).

The first chargeback time limit begins on the calendar day following these dates, and the issuing bank has typically up to 180 days from this day to raise the chargeback.

However, chargebacks and retrieval requests can occur on various time scales depending on the reason for the dispute as well as the financial offers surrounding the transactions.

5. Chargeback time scale formula

For the sake of simplicity, VoicePay® uses the following formula for calculating the Chargeback Time Scale (CTS):

$$\text{CTS} = 180 \text{ days} + \langle \text{period between pre-payment/deposit and receipt of the product/service} \rangle + \langle \text{guaranteed/warranty period} \rangle + \langle \text{period of subscription /membership} \rangle$$

6. The chargeback/retrieval request process

6.1 Chargeback's/retrieval requests occur as follows:

1. The card holder queries the transaction.
2. The card issuer requests information about the card holder's transaction from the acquiring bank (this is known as a retrieval request). When raising a request, issuing banks do not state the reason for the request and they are not required to confirm whether the information provided is

sufficient for the card holder. A chargeback may or may not subsequently be raised.

3. The acquiring bank approaches VoicePay ® for a copy of the transaction receipt. The issuing bank provides the acquiring bank with limited information relating to the transaction. The card holder's name is not quoted. VoicePay ®, therefore, receives only the date, card number, and amount. The acquiring bank's role is to forward the retrievals to VoicePay ® and to act upon VoicePay ®' responses in a timely manner. Both VoicePay ® and the acquiring bank will represent your interests in trying to avoid subsequent chargebacks, but we need your support (as detailed below) to undertake this role.
4. VoicePay ® forwards the retrieval request to the merchant. If the merchant has already credited the transaction, VoicePay ® will notify the card issuer of this and request that the retrieval request is retracted.
5. The merchant is required to respond to the retrieval request by sending all the necessary information relating to the transaction, back to VoicePay ®. If the issuing bank does not receive a copy of the transaction receipt within the required time scale, it has the right to charge the transaction back due to non-receipt of documentation.
6. You provide VoicePay ® with the required information (see *representments* on page 8 to see what information is required).
7. VoicePay ® forwards the transaction information to the acquiring bank, who forwards this on to the card issuer. The card issuer considers the information in liaison with the card holder and determines whether the information was returned in the correct time frame and whether it satisfies the card holder's query. If the transaction is no longer disputed, the process stops here.
8. If the transaction information does not satisfy the card holder's query in accordance with the rules, or the supporting documentation fails to arrive in the specified time frame, the card issuer will raise a chargeback on behalf of the card holder and send the details of the chargeback to the acquiring bank, who will pass it on to VoicePay ®. Throughout the process, relationships are clearly defined. The card holder liaises with the card issuing bank, the card issuing bank liaises with the acquiring bank, the acquiring bank liaises with VoicePay ®, and VoicePay ® liaises with the merchant.

7. Why do chargeback's/retrieval requests occur?

There are many reasons and reason codes associated with chargeback's and retrieval requests. Generally however, chargeback's and fraud

7.1 Fraud

A card holder may have had their card information stolen and used in a fraudulent purchase. In such circumstances the reason for the chargeback could be one of the following:

1. The card holder states that they did not authorise or participate in the transaction.

2. One of these errors – invalid card/non matching/fictitious account number /unassigned card holder account number/incorrect card member account number
3. Missing/invalid signature (after a retrieval request has been responded to by the merchant)
4. Secondary identification not recorded/does not reflect the card holder (after a retrieval request has been responded to by the merchant)
5. Warning bulletin (card reported lost/stolen after authorisation)
6. Incorrect card holder name (after a retrieval has been responded to by the merchant)Counterfeit transaction

7.2 Product quality

A card holder may have purchased a product/service and:

1. It was delivered in poor condition.
2. It did not work.
3. It broke down soon after purchase.
4. The product was not as described in the sales literature.

7.3 Customer service problems

A card holder may have purchased a product/service and:

1. It was not delivered.
2. They were charged incorrectly for it.
3. They were charged more than once.
4. They were charged in the wrong currency (not the currency on their receipt).
5. There were errors in the addition of the total amount billed to them.
6. A retrieval request/rfi has not been responded to or the information provided is insufficient to justify the debit to the card holder.
7. The card holder has already/since paid by other means.
8. You have not supplied sufficient proof that the goods were despatched.
9. The card holder is in a legal dispute with the merchant.

Note: *it is important that you provide as much information as possible when you receive a chargeback/rfi and that all documentation is legible and given within the time frame stipulated.*

7.4 Refund problems

A card holder may have purchased a product/service and:

1. They were promised a refund and did not receive one.
2. The transaction was an advance booking and the card holder did not arrive.
3. The card holder has returned the goods to the merchant.

4. It was part of a recurring billing authority that is now cancelled.
5. They paid a deposit but have since cancelled the order.
6. They were promised a refund but instead were charged again credit posted as a sale).

7.5 Processing problems

A transaction may have been processed where:

1. The card had expired.
2. The total amount of the sale was split into two or more parts to achieve full authorisation (split sale).
3. The card holder was debited more than once.
4. There was a mis-post (the wrong card was debited).
5. The card was accepted before it was valid.
6. The card number is incorrect and cannot be applied to an existing account.

8. Representments – disputing a chargeback

A representment is also known as a “dispute response”. A representment occurs when a merchant disputes a chargeback with reason.

Email representment requests to: chargebacks@voice-commerce.com

Fax representment requests at: +44 (0)247 601 2136

8.1 How long do i have to dispute a chargeback or respond to a retrieval request?

From the date that the retrieval request or chargeback appears in your current account you have 5 days to dispute it formally and provide supporting documentation for the dispute. If you fail to do this within 5 days you will forfeit the right of dispute.

Note: *chargebacks can be avoided only if you have provided proof that the genuine card holder received all the goods or services ordered, in perfect condition. This includes proof of delivery signed by the card holder.*

8.2 What should i do if i do not have supporting documentation?

Provide whatever information you have. Please don't ignore the request. In addition, you may choose to contact your customer to address the inquiry.

8.3 May i issue a refund for a transaction where i have received a retrieval request?

No. It is a violation of card scheme regulations to issue a refund for a transaction that has entered the retrieval request and chargeback system.

8.4 Do all chargebacks start with a retrieval request?

No. Issuing banks are not required to submit retrieval requests for most chargeback reasons.

8.5 What is an auto-representation?

We automatically represent certain chargebacks as determined disputable by our rules. An example is when a transaction had previously been issued a full refund. Check your online statement for details.

8.6 What information is required to represent (dispute) a chargeback?

In order for a representation case to be considered for bank submission, the following details must be provided within 5 business days.

1. A faxed or scanned document (referred to as a “sub draft”) showing the card holder’s information (name, address, card number, expiry date, cvv response, phone number, email address, ip number, etc.) And a description of the goods or services provided for this transaction.
2. Any of these additional, optional items, provided to increase your chances of winning a representation case:
3. A copy of a paper sales draft or fax showing the card holder’s signature.
4. A legible photocopy of the front and back of the customer’s credit card.
5. A legible photocopy of the card holder’s passport or driver’s licence.
6. Any additional proof of the order authorisation or merchant fulfilment.

Note: if the chargeback reason code was “not authorised”, then you must include either a, b, or c from the list above in order for VoicePay® to represent the case.

8.7 How do i submit a representation case?

Email your complete case, with scanned or faxed (tiff format) attachments, to: chargebacks@voice-commerce.com

You can also fax the case at: +44 (0)247 601 2136

You will be notified, with reason, if your case is rejected by our chargeback team.

8.8 How do i know if my representation case was won or lost?

Once a decision has been made with the issuing bank you will see one of the following two items on your online statement:

1. A chargeback reversal posted as a credit to your current account indicating that your case was accepted (won) by the bank. Or
2. A lost representment will show as an “information only” record indicating that your case was rejected by the bank. The bank’s decision could take up to 180 days, but you will typically receive an answer within 10 banking days.

8.9 What is a second/final chargeback?

Occasionally an issuing bank will represent a chargeback that has been previously reversed. This process is supported by the card scheme regulations.

8.10 What information is required to dispute a second chargeback?

Reversing a second chargeback is rare. A case may be made in good faith with substantial dispute collateral. Present your case via email or fax for special consideration if you believe your case is valid.

8.11 Currency difference

According to the association regulations a merchant is required to absorb foreign currency exchange loss on any international transaction.

9. The good faith/collection assistance process

Once the chargeback process has been completed, or the card scheme time scales have expired, there is no further recourse to the card issuing bank. However, there may be reasons, outside the card scheme rules and regulations, where we would wish the issuing bank to reconsider the circumstances surrounding a chargeback.

This can be achieved by a good faith/collection assistance attempt, which is a letter to the card issuing bank, with supporting documentation, requesting that it reconsider the chargeback decision. The card issuing bank is not obliged to view the case, make payment, or even reply to a good faith/collection assistance request. This option is considered a last resort and can only be considered if you can provide evidence that the chargeback is invalid or that you have corrected the original defect.

How VoicePay® can help in order to meet association regulatory requirements and to mitigate our exposure to any additional fraud, we automatically block all new transactions for a card number previously involved with a chargeback related item.

10. How you can help yourself

It is not possible for you to avoid chargeback’s completely. However, the following tips could help you reduce the number of retrieval requests and chargeback’s you may receive.

To help in the prevention of chargeback's, we recommend that you follow the guidelines below. If you fail to follow these recommendations your transactions are more likely to be rejected or in due course charged back to you.

10.1 General

1. Ensure that you have read and understood your supplier agreement.
2. Double check all details for transactions.
3. Supply as much information as possible when you receive a request for information.

10.2 Website requirements

Your website should display the following information:

1. A complete description of the goods and services offered
2. Details of your returns/refund policy
3. Customer service contact, including email address, phone number, and address
4. Transaction currencies in which you can deal
5. Export restrictions (if known)
6. Delivery methods and timing

10.3 Delivery of your product/service

You should retain documentary evidence of the delivery, together with a description of the goods/services supplied, for a minimum of 12 months.

Do not despatch goods by whatever means (including online delivery) to a third-party address (that is, an address other than the card holder's address) – this is considered very high risk. When delivering the goods, obtain the card holder's signature to show proof of delivery. If possible, take an imprint of the card at this point.

10.4 Product quality/customer service/refund policy

You should ensure that:

1. Your products are of high quality and reflect exactly the promises made in your sales literature
2. Delivery of your product/service is prompt and within the timescales advised to the card holder
3. All card holder charges are "quality checked"
4. You have a liberal refund policy and honour it
5. You respond quickly to retrieval requests and chargeback's

10.5 Refunding a transaction

You can refund a transaction. However, once you receive an rfi or a chargeback, it is too late to refund the transaction. If you do so you risk losing the money twice. It is also a violation of card scheme regulations to issue a refund for a transaction that has entered the retrieval and chargeback system.

10.6 Practical advice on avoiding fraudulent chargebacks

There are a number of things that you can do to reduce your risk.

1. Require that the customer send in a signed fax, preferably with a photocopy of the front and back of the card, so that you can check the signature. Your web site can allow the user to automatically print the order form, so it only needs to be printed out and sent.
2. Have the customer set up an account first and either check with the issuing bank of the credit card that the provided address is correct, or have the customer fax a copy of their latest credit card statement and/or passport/driving license.
3. Confirm the use of the credit card to the customer's official address by other means than email, such as a letter, phone call, fax, or SMS message, to reduce your level of liability.
4. Implement a rule-based order-checking system to eliminate typical scams from your web site.
5. Use avs or a third-party address-checking system (e.g., Equifax, 192.com) to ensure the customer's address is verified. Avoid shipping to an address different from the billing address.

Note: *do not despatch goods by whatever means (including online delivery) to a third-party address (that is, an address other than the card holder's address).*

1. If you must send goods to a shipping address that is different from the mailing address associated to the consumer's credit card, we suggest that you call the consumer and have them fax a copy of at least one bill from the address, or a copy of the driver's license of someone who lives at the address that was provided. We recommend that you never ship to P.O boxes.
2. Check each transaction against previous transactions for a given credit card and check for any anomalies.
3. Avoid shipping to countries such as with known high levels of fraud, such as Russia and Bulgaria (see *high-risk countries* on page 15).
4. When delivering goods, obtain the card holder's signature to show proof of delivery. If possible, take an imprint of the card at this point.
5. Retain documentary evidence of the delivery, together with a description of the goods/services supplied, for a minimum of 12 months.

10.7 Review transactions manually- identifying risky transactions

Often, the most effective tool against transaction fraud is to review each transaction manually. The following suspicious circumstances may indicate a transaction fraud:

1. Being requested to ship orders outside your own country, especially to known centres of internet credit card fraud such as the ex-eastern bloc and third-world countries.
2. Orders that are outside your norm, for example multiple purchases of an item normally only ordered singly (e.g., 10 copies of the latest Britney spears CD, or even 2 television sets), or purchases that vastly exceed the average value of normal orders. Where you have regular purchasers, you should also be wary of orders outside their norm.
3. You should be wary of orders placed by purchasers in the middle of the (their) night. Again, some of these may be legitimate, but most will not.
4. A customer ordering unusually large amounts of an item without any preference for the size, colour, make, or model.
5. An existing customer who suddenly orders a substantial volume of goods.
6. A customer who provides you with more than one card to cover one order or a set of orders.
7. A customer who orders more than once in a given day.
8. A first-time customer ordering a number of goods quickly.
9. A number of large orders from customers at a trade show.
10. A customer who has attempted the same transaction more than once, with the card failing at the first attempt.
11. A customer who refuses to confirm their credit/debit card and billing address details.
12. Avoid free email addresses such as hotmail.com and yahoo.com as much as possible, as they can not be traced back to the official owner.
13. Unusual origins, e.g., a u.s.-issued card is offered during a session from an Egyptian-based customer with a delivery address in Italy.
14. Re-tries, in which a person enters multiple credit card numbers until an authorisation obtained.

10.8 High-risk countries

Customers who have purchased their goods/services from or request delivery to one of the following countries are more likely to be fraudulent:

High risk countries			
Afghanistan	Albania	Algeria	Angola
Armenia	Azerbaijan	Belarus	Bosnia-Herzegovina
Bulgaria	Burundi	Cambodia	Congo Brazzaville
Croatia	Cuba	Ecuador	Egypt
Eritrea	Ethiopia	Georgia	Guatemala
Haiti	Indonesia	Iran	Iraq
Israel	Kazakhstan	Kirghistan	Laos
Liberia	Libya	Macedonia	Malaysia
Moldova	Mongolia	Myanmar (Burma)	Nigeria
North Korea	Pakistan	Philippines	Republic of Central Africa
Romania	Russian federation	Rwanda	Sierra Leone
Sudan	Surinam	Tajikistan	Turkmenistan
Ukraine	Uzbekistan/ouzbekist	Yemen	Yugoslavia
Zaire	Zimbabwe		

10.9 Useful websites for further information and advice

1. **APACS** - the UK payments association is the trade association for institutions delivering payments services to end customers. It is also the main industry voice on issues such as electronic payments, electronic banking and e-banking fraud. APACS maintains banksafeonline.org.UK
www.apacs.org.uk



2. **Card watch** - the UK banking industry's body that works with police, retailers and organisations including crime stoppers to fight plastic card fraud
www.cardwatch.org.uk
3. **Code fish spam watch** - dedicated to following and exposing spam scams
www.codefish.info
4. **Get safe online** - sponsored by government and leading businesses providing expert advice to protect everyone against internet threats
www.getsafeonline.org

5. **Home office identity fraud steering committee** - collaboration between UK financial bodies, government and the police to combat the threat of identity theft.
www.identitytheft.org.uk
6. **Interactive media in retail group (imrg)** - imrg is the industry body for global e-retailing.
www.imrg.org
7. **Microsoft security at home** - protect your pc
www.microsoft.com/security/protect
8. **Miller smiles** - the internet's biggest archive of spoof email and phishing scams
www.millersmiles.co.uk
9. **The serious organised crime agency** - the UK agency which combats national and transnational serious and organised hi-tech crime within, or which impacts upon the United Kingdom. <http://www.soca.gov.uk>
10. **Shop safe online** – shop safe online provides online retailers with information on mastercard secure code and verified by visa -secure services that make online shopping safer. These services have been developed by visa and mastercard to provide extra protection, making the online shopping experience better for everyone: consumers and retailers alike. www.shopsafeonline.org.uk
11. **Spamfo** - spam information; a resource with information relating to spam, news, reviews, faq and useful links www.spamfo.co.uk/
12. **Stay safe online** sponsored by the **us national cyber security alliance**
www.staysafeonline.info

Note: we do not endorse any individual vendors and we are not responsible for the contents of any third party web sites or products. These are provided for information only.