

Anti-Fraud Help / Anti-Fraud Assistance

Card and Bank account fraud can lead to losses that can often be insurmountable for mail-order/telephone order (MOTO) and internet Merchants to recover.

When consumers dispute charges or “chargeback” for items purchased, Merchants are liable. In addition, Merchants are responsible for the Issuing Bank’s chargeback fees and other costs associated with bad transactions. In fact, Merchants with excessive chargebacks can even lose the right to accept Cards – a risk no Merchant can afford to take.

Customer not present transactions are transactions conducted via mail-order, telephone order, or the internet, for which the card cannot be seen and swiped. These types of transactions are more susceptible to fraud, and the Merchant often takes the loss from a bad transaction.

There are people out there that mean to obtain products and services by deceiving the Merchant. By using lost or stolen cards, or card numbers generated by fraud schemes, they order goods and have them shipped to an address to be picked up by them or someone they call a “runner”. Services can also be a target i.e. domain names which they use to create new websites to “cover” fraudulent transactions via a Merchant account.

When the true card holder receives their statement and sees a charge they did not make, they will request a copy of the transaction or will be charged back right away. If this is an order made over the telephone, through the mail, or via the internet, these chargebacks are very hard to fight because there is no imprint or signature. Therefore, we would like to help prevent Merchants from incurring losses due to these types of transactions.

There are characteristics that may indicate that the transaction may not be legitimate. Be alert for transactions with several of these characteristics.

- Orders that are larger than normal when you are not familiar with the customer.
- Customers purchasing several of the same items or very expensive items.
- Customers who want orders shipped "rush" or overnight.
- Orders shipped to an international address, since they can not be verified by an Address Verification Service and are very risky unless you know your customer very well.
- Orders that are shipped to the same address but made on different cards.
- Orders from internet addresses using free email services.
- Transactions charged to account numbers that are sequential.
- Multiple card numbers given from a single internet address.
- Multiple transactions charged to one card over a very short period of time.

What you can do

- Use an Address Verification Service during authorizations to verify the card holder's identity and billing address. Address Verification compares the shipping address given to the Merchant with the customer's billing address with their issuing Bank. If the addresses do not match do not ship the merchandise or you will be putting yourself at risk of taking a loss.
- To verify the card's authenticity on customer not present transactions, ask for the CVV2 code on the back of the card if it is a Visa, or for the CVC 2 code if it is a MasterCard. This information is frequently missing on fraudulent payment cards, and would be unavailable in the case of compromised card numbers or generated account number schemes. This three-digit number is found on the back of the card on the signature panel after the card number.
- Ask the customer for additional information. For example, ask for day and evening phone numbers and call the customer back later. Ask for the Bank name on the front of the card, and the Bank's Customer Service number from the back of the card.
- Separately confirm the order with the customer. If you do not use an Address Verification Service, send a note via the billing address, rather than the "ship to" address before shipping the order.

To this end, this guide should assist in reducing your minimal exposure even more, and we would advise that you implement your own checking procedures to supplement ours, using this guide as your point of reference. Where appropriate, as in country mismatch between cardholder and delivery address, we will, upon request, advise our Merchants on transactions that may warrant further scrutiny, based on the knowledge and experience we have accrued. Most semi-serious fraudsters - who obtain their Card details from lists published on web sites or by using illicit programs that produce lists of algorithmically allowable card numbers - will attempt to mask their identity from later tracing by obtaining an internet connection via an ISP utilising dynamic IP allocation (i.e., they get a different, randomly allocated address every time they log in), and by using as their email identity a free address from one of a growing number of suppliers. Included amongst these are the ubiquitous Hotmail and Yahoo Mail, but there are some 10,000 others. While most users of these free addresses are legitimate, exercise caution when an order is received where the purchaser has entered one in your payment form.

Any follow-up activities to confirm identity prior to despatch of the goods are at your discretion, and you may wish to restrict yourself to a checking a subset, based on the other criteria outlined here, if transactions of this type are common to your business.

Merchants who are particularly concerned, such as those shipping downloadable goods, may adapt their checks to have all transactions arising from users of these email addresses blocked, thereby rendering the checking automatic. This, though, could significantly affect the profitability of your business. Note that although not all users of free email addresses are fraudsters, most fraudsters use free email addresses, and most legitimate transactions use email addresses assigned by their ISP, which are normally traceable.

We recommend the capture of certain items of information on payment forms, but you may wish to reject orders from purchasers who choose not to complete the form fully, especially contact detail fields, if you feel suspicious in any way about the legitimacy of the purchaser (some pointers are given below). As a side effect, you could even be alerting a genuine card holder in advance that their card is being used illegitimately, so that they can notify their card issuer and have the card stopped.

Card Not Present (MOTO/internet) - The Merchant gets the 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. Shopping on the internet or over the telephone is still a daunting prospect to many customers. Many are apprehensive about having to enter their Card number on the internet and making it available to a company or person they do not know personally. Regardless of this fact, they will happily hand over a Card to the waiter in the restaurant who subsequently walks away with it and thereby has every opportunity to copy the details. In a card not present environment the card issuer (and thereby the card holder) has chargeback rights. It is in fact the Merchant, and not the card holder, who carries the risk on these transactions.

What products pose a risk?

Not all products or industries are vulnerable to Card fraud, but certain types of internet or mail-order sites do carry a higher risk.

- **Downloadable software** may cost several hundred dollars, but if the fraud is not detected when the transaction is being made, the fraudster can download the product and disappear before the Merchant is made aware of the problem.
- **Instant entertainment** sites are also susceptible. These sites also get a high rate of chargebacks from participants who may claim to their spouses, following a query on the statement, that they never signed up for the service. This generates an above-average level of chargebacks. Information sites are likely to receive fraudulent visits. However their variable cost per sale is very low.
- **Expensive items**, such as computers, airline tickets, and diamonds, are prime targets for thieves.

If you are not in one of these categories, chances are you will not experience as much fraud, though you will probably have an occasional fraudulent Card sale.

In a card-present environment, rates of fraud are around 0.2%. The internet Fraud Prevention Advisory Council pegs online transaction fraud rates at between 2% and 40%, depending upon the product category. Details from the Gartner Group, released in July 2000, puts internet fraud at an overall level of 1%, but the overall repudiation rate at 2.5%. Repudiation includes all queries by card holders on their

transactions, which include customer disputes and transactions people simply did not remember or recognise. Obtaining an authorisation number from the Processor provides only some simple checks. When a transaction is submitted for authorisation, the Card number is checked against a list of known stolen/fraudulent cards and the "open to buy" on their credit limit. Where applicable, an address verification (AVS) test can be performed or the user can be asked to enter their CVV or CV2 number. If the card number passes these checks, an authorisation number is generated. In addition, the amount of the sale is debited against the card holder's credit limit, but this is done in a separate action.

Identifying risky transactions

A lot of fraud is still committed in very simple ways, such as persons using a known Card number (e.g., their own) and changing a few digits until they find a number that works. Therefore Merchants need to exercise caution when accepting orders.

Look out for these typical fraud indicators

- The same Card is used for orders from different customers.
- Multiple transactions are made from the same customer.
- Transactions from known "bad" (previous Chargeback) customers.
- Illogical orders are made, e.g., someone buying three engagement rings, a person living in India buying a PC from a shop in rural Cornwall, a person booking two flights flying out of London on the same day, etc
- Check the time of day the transaction is made against the local time. Most fraudulent transactions are conducted late at night.
- 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.
- An unusual origin, e.g., a U.S.-issued card is offered during a session from an Egyptian-based customer with a delivery address in Italy.
- Re-tries, in which a person enters multiple Card numbers until an authorisation obtained.

Each of these characteristics by itself is seldom cause for alarm. However, when a single transaction shows several of these factors, there could be a problem.

How fraudsters beat the system

Fraudsters may also trick the system in several ways:

- They can generate phoney card numbers that meet the Card industry's standard for consistency. Unless numbers are reported stolen, the transaction may be authorised.
- Identity theft: card numbers and home addresses may be stolen without the card holder's knowledge. Then they may be used in one short burst of online activity, which ceases before the fraudulent charges are reported to the Bank by the card holder. This is the most common type of fraud.

Address Verification Systems (AVS)

One additional security facility is that the Bank/Processor' payment pages prompt your customers for their card billing address. This information is then compared with the card issuer's records (where available) and the results of the comparison passed back to you for consideration.

This system checks whether the billing/shipping address provided matches the address the card is registered to. The address entered by customer must be their billing address (the address where the customer's card statement is currently sent), and this billing address must match the address held by the card issuer exactly.

You can eliminate much fraud just by shipping only to the official address. Also, the customer has fewer opportunities to claim they never made the sale if they did not return the product. In several European countries such as the U.K., AVS systems are now in widespread use.

Both the Acquiring Bank to whom your transactions are passed and the card issuer must also provide/support an AVS system in order that the comparison can take place. Where either the Acquiring

Bank or the card issuer do not yet provide AVS support, a "Not Supported" message should be sent back to you.

A fraudulent user of a card is unlikely to know the billing address for the card, so submission of an incorrect billing address with an order is a significant indicator of a possible fraudulent transaction. AVS is considered such an important check that a transaction may be rejected if an AVS check produces a bad result.

Security code

To further protect against processing a transaction paid for by a stolen Card, we strongly recommend that you take the consumer's Card CVV value on all orders. The CVV value is the 3-or 4-digit number found on the Card, in addition to the card number itself, and is another security method used for card-not-present transactions. The number is not embossed on the card and hence only the cardholder would know what the code is. Since a CVV2 number is listed on the actual Card, but is not stored anywhere, the only way to know the correct CVV2 number for a Card is to physically have possession of the card itself. All Visa, MasterCard, and American Express cards made in the past five years or so have a CVV2 number.

Where is a CVV2 number?

MasterCard/Visa - This number is printed in the signature area of the back of the card. It is the last 3 digits after the Card number. If you cannot obtain a CVV2 number, you will have to ask the card holder to obtain one from their issuing Bank.

American Express - This number is printed above and to the right of the imprinted card number on the front of the card. Some card issuers refer to this number as the "Security Code" and others as "Card Verification Value" (CVV).

In addition, it may also go by the name of CVV2 for Visa cards or Card Verification Code (CVC) for MasterCard/EuroCard. The Security Code verification service enables the card Security Code entered by the customer to be compared against the card issuer's details and the results passed back to you.

Both the acquiring Bank to which your transactions are passed and the card issuer must also provide/support a security code verification system in order that the comparison can take place.

We strongly recommend that your customers are requested to submit this data upon payment. The aim is to provide you with more information so you can make an informed decision whether to fulfil the order or carry out further checks.



How you can help yourself

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

- Require that the customer send in a signed facsimile, 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.
- Have the customer set up an account first and either check with the issuing Bank of the Card that the provided address is correct, or have the customer facsimile a copy of their latest Card statement and/or passport/driving license.
- Confirm the use of the Card to the customer's official address by other means than email, such as a letter, phone call, facsimile, or SMS message, to reduce your level of liability.
- Implement a rule-based order-checking system to eliminate typical scams from your web site.
- Use AVS or a third-party address-checking system (e.g., www.equifax.com) to ensure the customer's address is verified. Avoid shipping to an address different from the billing address. 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).
- If you must send goods to a shipping address that is different from the mailing address associated to the consumer's Card, we suggest that you call the consumer and have them facsimile 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 PO boxes.
- Check each transaction against previous transactions for a given Card and check for any anomalies. Companies such as eFalcon (www.efalcon.com), Retail Decisions, and Experian provide external tools to rate a transaction.
- Implement a rule-based order-checking system to eliminate typical scams from your web site.
- Avoid shipping to countries with known high levels of fraud, such as Russia and Bulgaria (see [Be aware of high-risk countries](#))
- 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.
- Retain documentary evidence of the delivery, together with a description of the goods/services supplied, for a minimum of 12 months.

Review transactions manually

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

- Being requested to ship orders outside your own country, especially to known centres of internet Card fraud such as the former Eastern Bloc and third-world countries.
- 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.
- You should be wary of orders placed by purchasers in the middle of the (their) night. Again, some of these may be legitimate.
- A customer ordering unusually large amounts of an item without any preference for the size, colour, make, or model.
- An existing customer who suddenly orders a substantial volume of goods.
- A customer who provides you with more than one card to cover one order or a set of orders.
- A customer who orders more than once in a given day.
- A first-time customer ordering a number of goods quickly.
- A number of large orders from customers at a trade show.
- A customer who has attempted the same transaction more than once, with the card failing at the first attempt.
- A customer who refuses to confirm their credit/debit card and billing address details. As the process of reviewing each transaction by hand is both time consuming and expensive we recommend that you create your own fraud prevention rules, which flag such unusual transactions for further research.

Be aware of 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:

- Afghanistan
- Albania
- Algeria
- Angola
- Armenia
- Belarus
- Bosnia-Herzegovina
- Bulgaria
- Burundi
- Cambodia
- Congo Brazzaville
- Croatia
- Cuba
- Ecuador
- Egypt
- Eritrea
- Ethiopia
- Georgia
- Guatemala
- Haiti
- Indonesia
- Iran
- Iraq
- Israel
- Kazakhstan
- Kirghizstan
- 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
- Yemen
- Yugoslavia
- Zaire
- Zimbabwe

Refunding a suspected fraudulent transaction

You may refund a transaction you suspect to be fraudulent, however, once you have received a RFI/Retrieval Request or a chargeback, it is too late to refund the transaction. It is advisable, however, that you utilise pre-authorisation so that rather than refunding such transactions you can simply not post-authorise/Settle them.

Additional measures

You can utilize a third-party fraud-screening system such as www.retaildecisions.com or www.fairisaac.com.

Code 10 calls

Where you are suspicious of a fraudulent transaction, try contacting the card holder by telephone to clarify the purchase. Should you remain suspicious of fraud you may undertake a "Code 10" call. By undertaking this process you can verify if the card used in a transaction has been stolen and the cardholder's address.

Contact your Bank/Processor for full details.

Deferred transaction processing

Most Banks/Processors offer a service enabling credit and debit card transactions to be pre-authorised/Settled, whereby the customer enters their card details, checks are then made on the submitted details, and the transaction funds are reserved against the customer's card. The transaction is not actually committed and therefore settlement to you will not occur at this time. Pre-authorising/Settling a transaction enables you to perform any additional offline checks against the customer details, and ensure that the order can be fulfilled. Once these or any other points have been checked, you must then "post-authorise" the transaction using the Bank/Processor back office system to ensure that the customer is debited and that settlement to your account occurs. There are two main reasons why you may request (or be required by The Bank/Processor to use) deferred processing:

- The Card Association rules require/recommend two-stage transaction processing, as funds should not be taken from customers until the goods have been despatched.
- Additional checks can be made on the customer to establish that the transaction was not fraudulent before completing the payment and delivering the goods.

Transactions that have been pre-authorised are only effective for between 3 and 7 days. If you do not subsequently "post-authorise" (Settle) the transaction, it will lapse after this period. This means that the customer's card will not be debited and you will not receive settlement of funds.

We truly hope that the issues associated with international trading on the Internet do not frighten you away from operating in this truly exceptional marketplace with enormous future potential. Managing revenue and risk for your business should be the driving force behind your risk-management strategy achieving the optimum balance between revenue and risk.

If you have questions

If you have any questions about fraud and ways to avoid it, please do not hesitate to contact us.