ADCB Merchant Services - Business Solutions

بنك أبوظبي التجاري
ADCB
MERCHANT SERVICES

CONTENT

PROTECT YOUR BUSINESS

Merchants face various risks when accepting credit card transactions. This brochure has been developed to assist you to understand the types of risks you face and actions that should be taken to reduce the risk of loss.

One of the greatest risks to merchants is that of fraudulent transactions. If you are not careful, fraud can cost your business significant amounts of money. Certain types of merchants – based on the type of goods sold – are more prone to fraudulent transactions than others. Merchants should understand their likelihood of being targeted by fraud.

It is essential for merchants to have a sound understanding of credit card fraud, how it can be detected and how it can be prevented. These concepts are discussed below for the three broad types of credit card transactions:

- Card present (face-to-face) merchants;
- Internet merchants; and
- Mail Order/Telephone Order (MOTO) merchants.

Internet and MOTO merchants are commonly referred to as "Card Not Present" merchants where the credit card and purchaser are not physically present in the merchant's shop at the time of purchase.

Examples include purchases where your customer provides their credit card details over the Internet, by fax, phone, or through the mail.

Note: Under no circumstances should you request that a customer provide credit card details via email for payment of the provision of goods and/or services.

Many fraudsters prefer to make Card Not Present purchases due to the anonymity afforded by these payment methods. Also, Card Not Present situations enable fraudsters to place orders over the Internet or via MOTO all over the world.

If they reside overseas, the chance of criminal prosecution is much lower, which is an added incentive to this type of fraudulent behavior. A large amount of credit card fraud is committed in Card Not Present situations and the volume of this type of fraud is increasing at a rapid rate.

HINT: Always adhere to the Terms and Conditions of your merchant agreement and to the Card Scheme rules.

AUTHORIZATION

It is essential that you understand the term 'authorization' – what it means, and what it does not mean.

What authorization does mean

- The account number is valid;
- The card has not been reported lost or stolen (although it may in fact be lost, stolen or compromised [card details improperly obtained or copied] and the card owner is unaware);
- There are sufficient funds available to cover the transaction.

What authorization does not mean

- An authorization does NOT confirm that the person providing the card number is the legitimate cardholder. The risk remains that the person providing the credit card number has either stolen or improperly obtained the card;
- There is also the risk that the purchaser has compromised (improperly obtained) the card number, without being in possession of the card.

Although it is important to obtain an authorization for each transaction, it does not protect you from the risk of fraud or chargeback. Risk of fraud remains even though authorization has been obtained.

HINT: Authorization will not guarantee payment if the transaction is not made by the rightful cardholder.

CHARGEBACKS

As a merchant, you face the prospect of receiving chargebacks. A chargeback occurs where the cardholder (or their bank) raises a dispute in connection with a transaction made through your business. If the dispute is resolved in favor of the cardholder, the transaction is charged back (debited) to your account.
In other words, you lose the full sale proceeds.

Common reasons for chargebacks are as follows:

- Cardholder did not make the transaction (frequently an indication of fraud);
- Cancelled recurring transaction;
- Goods not as described;
- Goods faulty or defective;
- Failure to respond to voucher requests.

Chargebacks may also be made for a number of other reasons, including, but not limited to:

- Goods/services not received;
- Exceeding merchant floor limit without obtaining authorization.

Chargebacks can generally be made by either the cardholder or their bank up to a maximum of 12 months from the transaction date, or from the date the goods or services should have been provided, where delivery was expected subsequent to payment.

Card Not Present merchants face additional chargeback risks that do not apply to merchants transacting in a card present environment. Specifically, due to the purchaser not signing a sales voucher or entering their PIN at the Point of Sale. If the cardholder subsequently denies having made the transaction, you will generally be liable for the chargeback. This follows from the fact that you are unable to prove that the cardholder made the purchase.

For this reason, it is essential that Card Not Present merchants take steps to identify the purchaser, and ensure that the transaction is legitimate. The ways in which you can do this are discussed over.

HINT: Minimize the risk of chargebacks by becoming aware of how and why they occur.

VERIFICATION OF PURCHASER

At all times, the onus is on you to verify the purchaser is the genuine cardholder. This applies to all merchants irrespective of the method by which credit card payments are accepted.

It is particularly important for Internet and MOTO merchants to identify the purchaser; however, ADCB recommends that merchants accepting credit card payment in a card present environment also take steps to verify the purchaser, especially for large purchases.

If you sell goods to a purchaser who is not the genuine cardholder, you may be liable for the chargeback.

It is emphasized that authorization does NOT constitute verification of the purchaser – the transaction may be fraudulent even though authorization is obtained.

CARD PRESENT TRANSACTIONS

When the card is present at the point of sale, take a good look at the card to ensure that it is genuine. Ensure that you maintain possession of the card until the transaction has been completed.

Review the Payment Card

- Does the card appear genuine? Is the embossing clear and even and does the printing look professional?
- Embossing - the card numbers should be raised, clear and straight
- Visa and MasterCard have the first four card numbers printed under the embossing

Note - The numbers are often mismatched or altered on counterfeit cards

- Check the front and back to ensure the card contains:
    - Card Issuer's logo
    - Cardholder name
    - Card number
    - Expiry date
    - Signature
    - CVV2/CVC2 – The 3 digit value located on or near the signature panel of the credit card.
    - Holograms should appear three-dimensional and change color when tilted, look for the Visa Dove or MasterCard Worldwide Map
- Check the cardholder's signature on the receipt against the actual credit card.
- Signature Panel - the words `MasterCard` or `Visa` are printed repeatedly at a 45 degree angle - the panel is designed to reveal tampering
- Check expiration dates on all credit cards. Never accept an expired credit card.
- Ensure the number embossed on the front of the card matches the truncated number on the receipt.
- Does the name match the customer? Does the gender of the presenter match the name printed on the card? Ask for photo id to confirm details if suspicious.

Always swipe or dip the payment card

Never manually enter the credit card number. Take extra caution if the customer requests you to manually key a transaction

Terminal Location and PIN Chip card processing

Chip cards are MasterCard and Visa (credit and debit) cards that are embedded with a security chip that provides further protection to assist in decreasing the risk of fraudulent transactions and chargeback disputes. Look at the card and if there is a chip, always insert the card into the chip reader at the first instance. As with any other transaction, a degree of caution must also be exhibited when processing chip card transactions.

If,

- The terminal displays 'Insert Chip' when the card is swiped through the terminal and the card in question does not have a chip on it, do not proceed with the transaction
- The terminal displays 'Insert Chip' and the chip when inserted cannot be read by the terminal, do not proceed with the transaction

What to look out for

Being vigilant about unusual credit card spending can help you avoid becoming a victim of a potential fraud attack. Look out for:

- Customers who appear nervous or anxious, or hurry you at closing time.
- Customers who order for the types of goods detailed in the 'Types of goods fraudsters target' section;
- Unusually large orders
- Customers who purchase multiple numbers of the same item without regard to size, color, style or price. Merchants should ask themselves whether it is likely that an individual would purchase a large number of a particular item;
- Customers who seem to not care about the item they are purchasing. For example, those who do not check the size or the price of an item, grab several items quickly, or do not worry about the warranty.
- Customers who request immediate delivery, that is, they want to take large and expensive items immediately.
- Customers purchasing large or bulky items, but refusing home delivery despite its inclusion in the price. It may be that the customer doesn't want the merchant to know their address due to the purchase being fraudulent;
- Customers who request you to manually key the card number.
- Customers who make repeated purchases in a short period of time;
- Customers who appear anxious, nervous or impatient;
- Customers who try to distract you at the time of processing the transaction, especially where the transaction is large;
- Where a large purchase is made on a newly valid card. The reason is that credit cards are sometimes stolen while being sent from the bank to the rightful cardholder.
- Multiple cards presented. Be wary of customers who give you more than two card numbers, or try to split the order.

Do not Double swipe at the terminal

Double swiping refers to the act of a merchant completing a second swipe of a card at the terminal after the card has already been swiped and the transaction is being processed. Double-swiping has been identified as the root cause in several large data compromise events globally. Merchants may be subjected to fines and other recovery fees by ADCB if they are found to be conducting this type of activity.

Further instructions

- Do not accept declined transactions. Do not split a declined transaction into smaller amounts.
- Be on the alert for counterfeit cards. Check the chip on the card to ensure that it is embedded in the card and not protruding on the surface. You can conduct a simple test by running your finger across the surface of the chip.
- Customers who present a card not in their name and when questioned advise that it is their partner's or friend's card.

If the customer does not cooperate or the details do not match, do not proceed with the transaction and ask for another form of payment.

In the event that a customer or transaction appears suspicious, before deciding whether or not to proceed with the transaction, the staff member should contact ADCB Card Center.

HINT: If your customer behaves in a suspicious manner, remember that it is better to lose a sale than to lose the sale and the proceeds.

CARD NOT PRESENT TRANSACTIONS

Card not present transactions are those where neither the card nor the cardholder are present at the point of sale, such as internet or mail order/ telephone order purchases. Merchants who accept card not present transactions face a higher risk of becoming victims of fraud as the anonymity of card not present transactions make them appealing targets for fraudsters. The following tips may help reduce the possibility of fraudulent card not present transactions:

- Obtain as much information as possible: the credit card number, name of bank, full name, address, expiry date, CVV2/CVC2 and contact telephone number (including landline). If processing the transaction via a terminal ensure you enter the card details correctly as per the operating guides for MOTO transactions.
- Use some form of additional validations, such as the electronic white pages to cross check details provided.
- Call the customer on the quoted contact telephone number to confirm details of the order, especially for large and/or suspicious orders.
- Request further identification such as a photocopy of the front and back of the card.
- This will ensure the person has the card in their possession. Ensure it is a genuine photocopy, not a photo shopped image.
- If you take payments via a website, contact your gateway provider and see if they have any fraud prevention software which you can utilize.
- Keep all copies of correspondence including invoices, emails, quotations, faxes, proof of delivery etc.

Always obtain authorization for all card not present transactions, regardless of value, and for the full amount of the transaction.

Remember, an authorization only confirms that funds are available at the time of the call and that the card has not been reported lost or stolen. It does not guarantee that the person quoting the card number is the owner of the card or is entitled to use the card.

What to look out for

- Items ordered of an unusual quantity or multiple orders of the same item.
- Big ticket items or orders that are larger than normal for your business.
- Orders requested as urgent or for overnight delivery.
- When orders are cancelled and customer is requesting a transfer of money to a card or method other than back to the original credit card. (e.g. Money order, money transfer). This is not permitted.
- Different cards are provided (including different cardholder names) but same delivery address given.
- Multiple cards presented.
- Orders for the types of goods detailed in the 'Types of goods fraudsters target' section;
- Customers who place a number of orders within a short space of time;
- Orders placed where the first card offered is declined, and a second card is immediately offered;
- Orders shipped to a country where the goods could easily be purchased locally. The question must be asked why the purchaser is prepared to pay the shipping expense, and wait longer for the goods to arrive;
- Orders from Internet addresses using free email addresses;
- Orders requesting the goods to be shipped to a third party;
- Orders where the only contact number provided is a mobile phone;
- Orders made within a short period of time on credit card numbers that are very similar, such as where only the last four digits differ;
- Orders for goods not normally supplied by your business.

Further instructions

- Take note of varying delivery addresses for repeat customers
- Be mindful of your states crime hotspots and delivery of goods to these hotspots
- Exercise caution when taking foreign orders, such as orders from Asia, the Middle East and Africa which may present a higher risk.

Remember, the liability for all card not present transactions rests with the merchant. Therefore the more information you gather to satisfy yourself that the transaction is valid the more chance you have of identifying fraud and reducing the chargeback risk.

HINT: Merchants suspicious of either the purchaser or the transaction are recommended not to ship the goods, even though the transaction has been authorized.

TYPES OF GOODS FRAUDSTERS' TARGET

Due to their high value and ability to be re-sold, the following types of goods are frequently targeted by fraudsters:

- Electrical goods;
- Household appliances;
- Jewellery;
- Computers;
- Furniture;
- Goods which are easily disposed of for cash.

If you are selling any of these types of goods, we urge you to be extremely careful before handing over/shipping goods. In particular, take all possible steps to confirm that the purchaser is the genuine cardholder. This applies to all merchants whether selling in a face-to-face or Card Not Present environment.

HINT: Fraudsters often target high value goods which are easily re-saleable.

PROTECTING YOUR BUSINESS AGAINST FRAUD
PROTECT YOUR BUSINESS AGAINST CARD PRESENT FRAUD

Apart from being alert to potentially suspicious transactions, merchants' main defences against fraud in card present situations are to carefully inspect the card to ensure it is genuine, insert the card when prompted by the payment terminal, authenticate the transaction using a PIN or signature as prompted by the payment terminal, and where applicable check that the signature on the back of the card matches the purchaser's signature on the sales voucher.

Payment terminals will prompt for authentication by PIN, or authentication by signature, or note that authentication is not required, depending upon the nature of the transaction. Merchants should follow terminal prompts at all times and refrain from hand keying transactions for any reason when the card and purchaser are present, particularly where this is suggested by the purchaser. Hand keyed transactions shift liability to the merchant in respect of fraud chargeback reason codes because this practice circumvents security and authentication features on the card and the terminal. The following security checks should also be performed:

- Closely inspect the card. Check that the 'valid from' and 'valid through' dates include the current date;
- Check that the card has the appropriate security measures;
- Check that the first four digits of the embossed account number match the four digits printed immediately above or below the embossed number;
- When tilting the card, the hologram on Visa and MasterCard® credit cards should move and/or change color;
- Where possible, always present the card as instructed by the terminal, being dip, swipe or tap. When manually processing a transaction, ensure that you take an

imprint of the card, and have the purchaser sign the sales voucher. Check that the signature on the sales voucher matches the signature on the back of the card;
- On the signature panel on the back of the card, check that the words 'Visa' and 'MasterCard' appear repeatedly at a 45 degree angle;
- Check that the abbreviated credit card number on the sales receipt matches the corresponding digits on the card. If the digits don't match, this is a clear indication the card is counterfeit;
- Closely inspect both the front and back of the card to determine whether any part of the card appears to have been altered.

HINT: Never process a refund transaction to a different card, in cash, by cheque or by electronic money transfer.

PROTECT YOUR BUSINESS AGAINST INTERNET AND MOTO FRAUD

Merchants can minimize the possibility of fraudulent purchases and chargebacks from Internet and MOTO transactions by implementing the following measures:

- Request the purchaser to provide the CVV2 (Visa) or CVC2 (MasterCard) three digit number located on the signature panel of the credit card. If the purchaser is not in possession of the card, it is unlikely they will know this number.
- Request the name of the cardholder's bank. Fraudsters who have compromised account details will not have this information. If the purchaser hesitates in advising the name of their bank, caution should be exercised;
- Request the purchaser to provide a fax copy of their driver's license;
- Ensure the customer's billing address and delivery address is consistent;
- Check the telephone book to verify address and phone numbers provided;
- Never forward goods to a Post Office Box;
- Obtain a signed receipt from the cardholder when the goods are delivered;
- In the case of orders for a large number of different goods, telephone the cardholder after the order is placed to confirm the order. Also, have the purchaser read back all details of the order. Frequently, where an order is fraudulent, the purchaser will be unable to confirm these details, as they were ordering at random, with no record of what they ordered;
- Be suspicious where multiple cards are used for a single purchase;
- Don't continue to attempt authorization after receiving a decline;
- Exercise particular caution in relation to overseas orders. Large orders should in all cases be held back for shipping while the above enquiries are made into the legitimacy of the purchaser. Merchants should not ship goods until satisfied that the purchase is legitimate.

HINT: Never process a refund transaction to a different card, in cash, by cheque or by electronic money transfer.

PROTECTING YOURSELF FROM FUNDS TRANSFER FRAUD

What is it?

Funds transfer fraud, sometimes referred to as 'Nigerian Fraud', continues to be a widespread issue for merchants. It involves the use of stolen credit card information and seeks to obtain funds via money transfers.

How does it work?

The ultimate goal of the scam is to trick you into providing funds to fraudsters or an unfamiliar third party (who is often working for or has been set up by the fraudsters) through another form of payment, such as a different credit card, cash, cheque or other form of electronic money transfer. This alternative form of payment may take the form of a refund or request to organize shipping with a specific courier that doesn't actually exist.

Example

In this context, fraudulent cards are used to purchase goods/services, and then the (supposed) cardholder requests a component of the card transaction value be paid to an associated third party. For example, AED 4,000 of Clothes and accessories are purchased via a telephone order and the cardholder asks the merchant to cover the AED 1,000 cost for courier services, taking the total transaction value to AED 5,000. The merchant pays the courier AED 1,000 by money/bank transfer, which becomes a straight loss. The rightful cardholder then claims the transaction is invalid (or disputes liability) and the transaction is reversed and AED 5,000 is charged back to the merchant's account. The merchant will incur an additional loss, if the goods were exchanged.

Note: This is only one example of a fraudulent transaction. Fraudsters are creative and will present different scenarios to merchants, however, one common element is the transfer of funds to the cardholder or a third party by other means, usually electronic money transfer.

What should I do?

- Use your instincts, if the sale seems too good to be true then it often is;
- Only process refunds to the credit card used in the original transaction;
- Refrain from sending funds by electronic funds transfer in this context;
- Review transactions that carry an increased fraud risk, including overseas orders from West Africa and Eastern Europe;
- Be wary of 'hard luck scenarios', often these scams seek to take advantage of your goodwill.

HINT: Never process a refund transaction to a different card, in cash, by cheque or by electronic money transfer.

OTHER RISKS MERCHANTS FACE

Laundering of sales (3rd party processing)

The term 'laundering', in a merchant context, refers to a situation, such as, where a business with a valid merchant facility accepts transactions on behalf of another business. Disreputable individuals sometimes approach legitimate merchants to process their credit card transactions, generally paying the Merchant a percentage of the amount processed. Apart from constituting a serious breach of ADCB's Terms and Conditions it is also an extremely dangerous practice opening up a merchant's business to significant risk of loss.

Merchants engaging in laundering/processing transactions on behalf of another business are liable for all chargebacks arising from these transactions. In many cases, the individual approaching the merchant to process their transactions is unable to obtain a merchant facility of their own, possibly due to previous improper merchant practices. Consequently, the chance of fraudulent transactions being processed is extremely high.
A merchant must not, process transactions on behalf of someone else or in connection with a transaction that did not involve them directly selling goods or services to their customer.

HINT: Laundering, in a merchant context, is an extremely dangerous practice which may lead to significant loss.

Fraudulent refund transactions

A common type of fraud involves employees issuing credits (refunds) to their own account.

To avoid detection, they may create a large debit transaction on a fraudulent card and an offsetting credit on their own card. In this type of situation, it is likely to take weeks, even months, before the fraud is detected. To guard against this type of fraud, we recommend that merchants closely monitor all credits, and check that all credits and corresponding debits relate to the same card number. Particular attention should be paid to large credits.

Another way in which merchants can protect themselves from this type of fraud is by regularly changing their terminal or user password(s), especially after an employee has left.

HINT: Ensure your password is changed regularly to prevent unauthorized use.

Online authentication of purchasers

The primary risk facing merchants accepting Internet transactions is the difficulty faced confirming the purchaser is the genuine cardholder. Where a cardholder disputes having made an online purchase, irrespective of whether this is actually the case, the merchant is generally liable for the chargeback.

Visa and MasterCard have jointly attempted to overcome this burden placed on Internet merchants by developing an online cardholder authentication service known as 'Verified by Visa' and 'MasterCard® SecureCode™'. A term called '3D Secure' refers

to the technology platform through which this service is offered.

Verified by Visa and MasterCard SecureCode works as follows:

- A cardholder registers with their bank;
- The cardholder creates a password (similar to an ATM PIN);
- Cardholder browses merchant website and selects goods/services to purchase;
- When a cardholder attempts to make a purchase, the cardholder is asked to enter the password they previously created when registering with their bank. The 3D
- Secure software can detect if a card is enrolled or needs to be enrolled. The standard authorization process is followed for cards that are not able to support this service;
- When the cardholder enters the password, the information is routed to the cardholder's bank for verification. The result of the password verification check is then sent to the merchant, advising whether the purchaser entered the correct password. If the wrong password is entered, it is likely that the purchaser is not the rightful cardholder and the merchant should not proceed with the transaction as liability then shifts back to the merchant.

The primary benefit to merchants of these verification processes is the chargeback liability shift that occurs. Subject to a few exceptions, if a merchant attempts to authenticate a purchaser using 3D Secure, both the cardholder and their bank lose the right to make a chargeback claiming the cardholder did not make the transaction. This is irrespective of whether the cardholder or their bank subscribes to 3D Secure – all that matters is that the merchant has implemented 3D Secure, and attempted to verify the cardholder's password.

Of course, if the password verification check fails (the purchaser entered the wrong password), you should not proceed with the transaction. If you proceed with the transaction after a cardholder has failed the verification check, you will incur the liability should a chargeback result.

HINT: Never process a transaction after a cardholder has failed the verification check.

RISK MITIGATION FOR ONLINE MERCHATS

Secure your customers' data

At ADCB we are committed to providing our merchants with every assistance to help protect their business, and their customers, from the growing threat posed by high-tech criminals. Without a doubt this is one of the biggest challenges faced by business today.

If you are a merchant who has access to, or stores credit card details in any format, or if you use a service provider who does, it is your responsibility to ensure that your customers' payment details remain secure.

It is important that you understand the measures which need to be taken to ensure the security of highly sensitive personal financial information.

HINT: Be aware of the importance of data security and your responsibility to ensure that your customers' data remains secure.

WEBSITE REQUIREMENTS

All merchants using an Internet Merchant Facility must comply with ADCB's website standards.

ADCB reserves the right to decline, deactivate access or terminate merchants who do not comply with these requirements for the duration of the facility.

1. Your website must satisfy all of the following criteria:

- The trading name and the URL must not have any substantial differences in wording.
- This will maintain consistency and reduce any potential cardholder confusion;
- A clear description of the goods and services offered for sale;
- Contact information – trading name, contact number, address;
- Telephone number and fax number where available;
- A clear explanation of shipping practices and delivery policy/timeframe;
- Transaction currency: ADCB merchants can process AED amounts only and may settle into AED accounts only;
- Total cost of the goods or services purchased, inclusive of all shipping charges;
- Card Scheme brand marks are displayed wherever payment options are presented;
- Export restrictions (if any) – countries to which the merchant does not ship;
- A clear refund/return policy;
- Consumer data privacy policy – advises what you plan to do with information collected from your customers;
  Security capabilities and policy for transmission of payment card details;
- Each merchant domain name must utilize separate payment pages. It is necessary to check that website links do not go to another domain name from which payments can be made in relation to goods or services offered through the first website;
- All information must be accurate in all respects.

2. Your website must not:

- Contain anything that constitutes or encourages a violation of any applicable law or regulations, including but not limited to the sale of illegal goods or the violation of export controls, obscenity laws or gambling laws;

- Contain any adult or pornographic content;
- Offer for sale goods or services, or use to display materials, that may be considered by a reasonable person to be obscene, vulgar, offensive, dangerous, or are otherwise inappropriate;
- Use unaccredited payment pages.
- Fail to use digital certificates to establish a secure browser session.

3. Payment pages must be accredited by ADCB or a ADCB accredited service provider and must adhere to our security requirements.

4. You must use digital certificates to establish a secure browser session between you and your customer.

5. You should not change the types of goods or services sold through your merchant facility without first providing ADCB with written notice, and then receiving written consent from ADCB confirming the change has been approved.