Abu Dhabi Islamic
Merchant Acquiring Company

أبوظبي الإسلامي
ميرتشنت اكوايرينغ كومباني

Welcome to the world of ADIB Merchant Services

Merchant Best Practice Guide

Merchant Best Practice Guide - V6 /Jan 2024

💻 adib.ae

☎ 04 806 1212

INTRODUCTION

All businesses are generally exposed to elements of Fraud and Merchant Acquiring Business is not an exception. Hereon, within context of this document, the aim is to share best practices to be applied to prevent fraudulent threats, exposure and in part- deterrence strategies that have been proven based on industry knowledge.

Covered/Credit Card Fraud is reality and is increasing in the retail market environment, exposing merchants to potential losses that could be damaging to their business.

At ADIB MERCHANT SERVICES our aim is to assist merchants to minimize fraud through the use of sophisticated fraud detection tools and pro-active merchant education.

Please make the time for you and your staff to review this Card Fraud Protection Booklet.
The more you know about the potential risks the more you'll be able to protect your business against chargebacks and fraud.

TYPES OF CARDS

Covered/Credit Card: A Covered/Credit Card is issued by a financial institution or other Covered/Credit Card company (called the Issuer). Visa and MasterCard Covered/Credit Cards (often referred to as "Bank Cards") are issued by banks, while American Express, Discover Network and other Covered/Credit Cards may be issued by the Card Company itself or in some instances by other financial institutions. There are many Issuers that offer Discover Network, Visa and MasterCard Covered/Credit Cards making it possible for a Cardholder to have several different Covered/Credit Cards, each of which represents its own line or credit.

Debit Card: A debit Card is issued by a financial institution. Purchases made with Debit Cards result in the immediate withdrawal of funds from the Cardholder's bank account. Debit Cards do not represent a line of credit they can only be used of the extend the Cardholder has available funds in the account associated with the Debit Card. Discover Network, Visa and MasterCard offer Debit Cards in addition to Covered/Credit Cards. Debit Cards that are processed in Covered/Credit Card Association networks are typically signature-based Debit cards, while Debit Cards that are processed on EFT Networks are generally Personal Identification Number (PIN)-based Debit Cards.

Automated Teller Machine (ATM) Card: An ATM Card is a plastic card issued by a financial institution that allows a Cardholder to withdraw funds, make deposit, make purchases or perform other banking functions against the Cardholder's bank account through an ATM or POS Device.

Electronic Gift Cards (EGC): EGCs are issued by Merchants at a set amount for future purchases. When a Cardholder uses an EGC to make a purchase the Transaction total is deducted from the value remaining in the Card until the pre-paid amount is spent.

HOW TO BEST PROTECT YOUR BUSINESS

Make sure the sale counts

It is easy to get carried away in the moment when customer wants to buy large quantities of stock and doesn't try to bargain the price down. The bad news is that when it seems 'too good to be true' it probably is. You should always be on the lookout for any unusual behavior.

It is important that you train your staff well and teach them to trust their instinct. Being vigilant about suspect behavior and unusual spending is your first time of defense. If a Covered/Credit Card payment turns out to be fraudulent, it could end up costing you more than the original sale was worth.

Know the consequences

It is important to be aware of how accepting a fraudulent transaction can affect your business. Some forms of payment carry an increased risk and you as the merchant could be liable for transactions when the cardholder disputes them.

High-Risk Transactions

- Card Not Present
- Card number is manually keyed in
- Foreign issued cards
- No authorization obtained
- Card is not swiped through POS Terminal
- Fall back transactions using the magnetic stripe of a Chip card
- Split Transactions
- Multiple Transactions at same time

Lower-Risk Transactions

- Card Present
- Card is CHIP read through POS Terminal
- Verified by Visa/MasterCard SecureCode and JSecure Transaction in case of e-com transactions

High chargeback levels and/or the acceptance of excessive fraud could attract penalties from the Card Schemes (Visa, MasterCard or the other card schemes) and in some cases this could even result in the termination of your merchant services facility by ADIB MERCHANT SERVICES.

Merchants should be aware of their responsibilities under the conditions of the merchant agreement. At all times it is your responsibility as the merchant to

RESPONSIBILITIES

verify that the purchaser of goods and services is the genuine cardholder.

Your merchant agreement specifies that you are responsible for preventing fraud occurring via your services, ensuring the physical security of your merchant equipment and protection of cardholder information. For this reason it is essential that you understand:

- How your business can become a target of fraud.
- How fraud can be detected.
- Your liabilities.
- Precautions you need to take.

Third Party Transactions

At no time should merchant process transactions on behalf of a third party. Not only will you pay the merchant service fee but you will also be liable for any chargebacks that arise from these transactions. Processing transactions on behalf of a third party without prior authority from ADIB MERCHANT SERVICES, is a breach of your merchant agreement and may result in the termination of your acceptance facility. In addition you may also be open to possible fines for breaching the card schemes rules.

Proprietor Transactions

Funds transferred from a Covered/Credit Card in the proprietor's name via their merchant services to their settlement account are classified as a Proprietor Transaction. Transferring funds in this manner is not only costly (you will be charged a merchant service fee for each transaction) but a breach of your merchant agreement. For Transactions such as transfers and bill payments you will need to utilize other banking services.

Split Transactions

If a transaction is declined, it is generally for a good reason. Do not lower the sale amount in an attempt to complete the sale on one card or split the sale over two or more cards. A transaction may be considered invalid and may be charged back if an attempt has been made to split a purchase, effectively avoiding your floor limit.

Securing Your Equipment

You are responsible for the physical security of your merchant services. It is important that you secure POS terminal equipment safely and never leave your terminal unattended during trading hours. You should never allow a cardholder to instruct you on how to process a transaction or have access to your terminal except for PIN input.

Fraudsters may approach your business posing as a terminal, electrical or phone line technician advising that they need access to your terminal. They may then process refund transactions or insert card readers into your terminal that will enable them to steal cardholder information whenever the card is swiped.

Always check the identification of technicians attending your premises and never reveal any passwords. If suspicious contact your relationship manager.

Changes to Your Business

As a merchant, it is also your responsibility to advise ADIB MERCHANT SERVICES of any significant changes to your business. This may include but is not limited to the business address and location of the POS TERMINAL equipment or a change in business name. If you would like to change the types of goods services your business provides, you must obtain prior approval from ADIB MERCHANT SERVICES.

SHARI’A COMPLIANCE

As ADIB MERCHANT SERVICE is based on principles of SHARI’A Law, you as a Merchant are requested to follow ADIB’s Shari’a Compliance policy while using it’s terminals and to avoid using its terminals for non-Shari’a products/Services. Not following this rule will lead to violation of SHARI’A principles, such violations may lead to the termination of the merchant agreement.

You are requested to use POS Rolls provided by ADIB Merchant Services only. Use of other bank stationery or/and promoting other banks products and services through ADIB terminals is not allowed & merchants found doing these activities will be advised to stop as such activities may lead to the termination of the merchant agreement.

REFUND FRAUD

A common type of fraud involves employees issuing credits (REFUNDS) to personal/own accounts via the POS TERMINAL. To avoid detection they may create a large sale on a fraudulent card then process a refund to their own card. Refunds may also be processed to their own cards without a corresponding sale. To guard against this type of fraud we recommend you to closely monitor all refunds, checking that all refunds correspond to a legitimate sale and are refunded back to the original purchase card. Particular attention should be paid to large or multiple refund amounts.

Ensure only authorized staff are aware of your refund limits and refund password. Your refund password should be changed when your terminal is installed. It should be unique, changed frequently and kept secure.

CHARGEBACKS

You as the merchant may be faced with the prospect of incurring chargebacks, which can have a financial impact on your business.

A chargeback occurs when the cardholder (or their bank) raises a dispute in connection with a Covered/Credit/ Debit Card transaction. If the dispute is resolved in favor of the cardholder, the transaction is charged back to the merchant and debited to your settlement account. In other words, you as the merchant could possibly lose the value of the sale and incur a chargeback fee.

Common reasons for chargebacks include but are not limited to:

- Cardholder does not recognize the transaction (business name on statement is not recognized).
- Cardholder did not authorize the transaction (frequently an indication of fraud).
- Cancelled recurring transaction.

- Goods/services not as described.
- Goods/services not received.
- No authorization obtained
- Refund not received.
- Transaction processed more than once (Duplicated).

Disputes can generally be raised by either the cardholder or their bank for up to 18 months from the transaction date or from the date the goods or services should have been provided. For this reason you are required under your merchant agreement to retain all sales vouchers and information for a minimum of 18 months.

Charge Back Process

Once a transaction is disputed a 'Retrieval Request' will be sent to you, the merchant, to request transaction evidence such as a signed POS transaction receipt to support the sale, including but not limited to providing sales invoices You then have 3 days from the date of the notice to respond with the relevant information.
Responsibility lies with you, the merchant, to provide satisfactory supporting documentation to prove that a valid transaction occurred and/or that the cardholder authorized the transaction. If you cannot provide evidence to support the sale, liability for the chargeback lies with you.

It is important that you respond to all retrieval requests including valid supporting documents promptly and within the time frames specified. Late or no response to a retrieval request or invalid documents provided will result in a chargeback being debited to your settlement account.

Refunds should not be attempted once a retrieval request has been sent or a chargeback has been processed as this may result in your settlement account being debited twice.

Attempting to re-process a transaction once it has been charged back violates card schemes regulations and could lead to termination of your merchant service account.

CARD PRESENT TRANSACTIONS

While trusting your customers is important this should not be at the good business sense. This means ensuring that whenever the card is present staff undertakes additional security measures to ensure the card is not a counterfeit (fake) and that the purchase is the genuine cardholder.

Check the card back and front:

- Is the embossed card number clear and aligned?
  (Although most cards are embossed there are some exceptions).
- Can a ghost image be seen?
  (Original embossed details on the card that have been flattened).
- Do the first four digits of the embossed card number match the pre-printed four digits directly below the embossing?

Check the hologram or the holomag:

- Does the image appear three-dimensional and change color when tilted?
- Can it be scratched or does it lift off?

Check the card number:

- Does the entire or abbreviated (i.e. first six and last three digits) card number match the printed receipt?

While checking the above features, take note of the customer's behavior. Some of the below situations on their own may not cause for alarm but in combination they could be an early indicator that something is not quite right.

Be wary in situation where:

- Customers appear nervous or anxious or hurry you at closing time.
- Customers make indiscriminate purchases possibly with a newly valid card without regard to size, style, colour or price.
- Customers purchase a large item and insist on taking it with them, refusing delivery.
- You are requested to split transactions over two or more cards or number of cards are presented with multiple declines.
- Customers who are quick to take the card back from you preventing you from

checking the security features.

- Customers who choose an item in store and tell you that they will phone through a card number and provide a delivery address.
- Customers who will make numerous purchases under your floor limit.
- Customers who ask you to manually key a transaction providing the card number from memory, a slip of paper or an old sales voucher.
- Customers who need to see the card in order to sign the sales receipt.

It pays to insert the card in the POS TERMINAL

Always attempt to insert the card into CHIP reader through your POS terminal when the opportunity serves. Manual Key Entry of the card number greatly increases your exposure to chargebacks as there is no proof that the card was present during the time of transaction. For high transaction amount and/or suspicious transaction ask for ID proof (copy of original passport or any other photo ID which matches details with card details).

Remember, if you are suspicious of a transaction:

- Contact your relationship manager.

If you cannot confirm the transaction beyond your suspicious:

- Decline the transaction or ask for another form of payment

If you have identified the transaction as fraudulent:

- Contact your relationship manager.
- Attempt to retain the card

Don’t Hesitate! Call in a Code 10

If you ever have doubts about something, whether it is fraudulent card, signature or customer’s behavior - call in a Code 10.

With Code 10 you can call for an authorization without customer becoming suspicious.

Contact your relationship manager and inform him of a Code 10. Your relationship manager will put you through to the correct person who will ask a series of “Yes” or “No” questions. Hold on to the card if possible while making the call.

If the operator decides something is amiss, he or she will deny authorization.

A Code 10 can be used any time when you as merchant feel that transaction may not be legitimate, even if the transaction is approved or if the customer had already left the premises.

When to Call in a Code 10:

- When embossing on the card is illegible.
- When the last few numbers are not embossed on the hologram, or if these numbers do not match the account number on the sales draft of at the POS device.
- When there is no Bank Identification Number (BIN) above or below the first four digits.
- When the name on the card does not match the signature or there is a misspelling.
- When holograms are not clear or the picture in the hologram does not move.
- When the card does not have an expiration date.
- When the card does not start with the correct numeric digit (all Visa cards should start with the number four (4) , all MasterCard with the number five (5)).
- Be aware of cards that don’t swipe, check these cards for other security features.
- If a card is swiped, make sure the card number and the number that appears on the POS device match.
- If the message is other than “approved” or “declined”.

Remember your safety comes first don’t take any chances.

CARD NOT PRESENT TRANSACTIONS

Internet and mail order/telephone (MOTO) transactions are commonly referred to as 'Card Not Present' transactions.

Merchants that accept Card Not Present transactions are at a greater risk of becoming victims of fraud, as fraudsters take advantage of the anonymity Card Not Present purchases provide. Fraudsters are able to make purchases anytime, with or without a physical card, from anywhere in the world making Card Not Present transactions a preferred method of trade.

For this reason it is important you understand the possible warning signals to identify suspicious or unusual transactions for your business. We suggest that you undertake additional security measures whenever you accept a covered/ credit card for payment in a Card Not Present environment.

When Taking an Order

- Obtain the Covered/Credit Card number, name of the bank, expiry date, full name, address and contact phone numbers, including landline contacts (not mobile contact).
- Conduct a check on the details provided to verify name and telephone number.
- Confirm the order by calling the landline number provided and/or send confirmation of the order to the billing address, not the shipping address.
- Make sure a reputable courier engaged by you makes the delivery. Use a courier that does not allow shipping re-routes.
- Ensure delivery is to physical address. Never send deliveries to a hotel, motel or PO Box.
- Ensure that the person making the delivery does in fact deliver the goods to a person inside the premises.
- Do not continue to attempt authorization or split a transaction after receiving a decline.

Suspicious Orders – What to Look For

Being vigilant about unusual spending can help you identify early warning signals that something may not be right with an order. While aspects of the following *situations may occur during a valid transaction combinations of these may be cause for alarm.*

Be wary in situations when:

- You are requested to split transactions over a number of cards.
- Multiple cards are presented with multiple declines within a short period of time generally via your Internet payment page. These cards may have the same BIN (first six digits) or may appear to be sequential with only the last four digits changing.
- Items that are ordered in unusual quantities and combinations and/or greatly exceed the average order value.
- Orders marked urgent or shipped overnight to deliver fraudulently obtained items as soon as possible for quick resale.
- Orders from Internet address using free email services.
- Order placed where the initiator of the order admits it is not their card being used.
- Orders shipped to international destinations you may not normally deal with.
- Order received from locations where the goods or services would be readily available locally.
- Orders for additional products you do not normally sell.
- Orders are cancelled and refunds are requested via telegraphic transfer to an account other than the original purchase card.
- Goods or services have been ordered over the phone to be collected in person at a later date. (Make sure you sight the card and swipe or take an imprint with signature upon collection of the item).
- Orders for high value goods placed over the phone where the buyer sends a taxi to pick them up.

International Orders

We suggest that you express caution when receiving any international orders particularly from countries you do not normally deal with or if you do not normally trade internationally.

Suspicious of the Transaction?

If you cannot verify that the payment details provided are genuine or you are suspicious of the purchaser or the transaction, ask for an alternative form of payment such as a telegraphic transfer. If the customer refuses, we recommend that you process a refund to the card and DO NOT send the goods.

Remember it is your responsibility to confirm the purchaser is the genuine cardholder before providing the goods and service as you may be liable for the transaction if it is disputed.

Reducing the Risk of Internet and MOTO Fraud

Now that you aware of how you can become a target for fraud you may be asking yourself 'How can I reduce the risk?'. You can minimize the possibility of becoming a target for fraud by implementing the following measures:

1. Develop a standard Covered/Credit Card transaction checklist that all staff must use when taking an order.
2. Consult with your Bank to make sure your card absent transactions are correctly classified with accurate MO/TO and ECI indicators.
3. Create a secure customer database. Include relevant information such as IP addresses, and abbreviated card numbers etc. and link these to transactions marked as suspicious or that have been charged back.
4. Advertise that you will prosecute identified fraudulent activity on your website. This may help in deterring fraud.
5. Discuss additional security with your service provider or an IT expert to help you redevelop your web/payment page. This could include blocking IP addresses, BINranges, CVV2 acceptance, Verified by Visa and MasterCard secure code.

If you suspect that your website has become a target for fraud, we suggest that you shut the site for a short period of time and conduct an investigation on where the fraud is coming from. If it is possible, block the IP address from which the orders are originating.

Verified by Visa (VbV) and MasterCard SecureCode

Verified by Visa (VbV) and MasterCard SecureCode are online cardholder authentication programs developed by the card schemes.

VbV and SecureCode work in the following way:

- A cardholder is registered with their issuing bank.
- The cardholder then creates an authentic password (similar to that of an ATM PIN).
- When a cardholder makes a purchase via your web page they are requested to input their online password.
- The details are then sent through to the cardholder's issuing bank for authentication.
- If the password is incorrect we recommend that you do not proceed with the transactions.

SECURING YOUR CUSTOMER'S DATA

Merchants that do not keep cardholder data safe and secure open themselves up to possible legal action and fines if cardholder data is compromised and liable for all transactions performed.

As a merchant you are always dealing with sensitive cardholder information. ADIB MERCHANT SERVICES recommends that you are pro-active in safeguarding all customer data held either electronically (e.g. a computer database) or manually (e.g. transaction receipts).

If data is held electronically, a merchant should comply with the Payment Card Industry Data Security Standard (PCI DSS). The PCI DSS contains requirements and guidelines and is endorsed by all major credit and charge card payment brands including Visa, MasterCard, American Express, Diners, CUP and JCB.

It is a requirement that paper records and transaction documentation is stored for 18 months. This information is to be stored securely with restricted access. Any theft must be reported to the ADIB MERCHANT SERVICES immediately.

How do you protect customer information?

- Ensure that all computer systems have a unique password.
- Conduct a network scan on all your external facing IP address.
- Protect systems that store and/or transmit card data with Anti-Virus software.
- Utilize firewall with stringent and granular security rules at all entry points Intrusion Detection Systems should be strategically placed with the network as needed.
- Do not store Card data on Internet facing systems.
- Encrypt data maintained on database or files and any data sent across networks.
- Securely destroy data when it is no longer needed for business reasons.
- Limit access by your employees to account data on a need-to-know basis and remove access to your network and premises if an employee leaves your business.
- Ensure files and transaction documentation is kept out of reach of customers.

DO NOT STORE THE FOLLOWING CARD HOLDER DATA:

- Sensitive Data i.e. Track Data from Magnetic Stripe of Card.
- Card Verification Number (CVV2/CVC2/CID).

(Three digits on the back of the card or four digits on the front of the card for AMEX).

Remember: Store only the customer's account information that is necessary for your business and only with the cardholder's knowledge and consent (e.g. name, address or email address).

Destroy Cardholder Information after Use

When you utilize sales receipts printed through POS device make sure that the details are unreadable. This is to ensure that the sales receipt cannot be retrieved from the rubbish, enabling fraudsters to use the data.

Report All Security Incidents

You are required to immediately notify ADIB MERCHANT SERVICES if it is identified that transaction data has been accessed or retrieved by any unauthorized entity. This allows procedures to be implemented immediately to reduce the usage of compromised data protecting your customers but also reducing the potential financial losses for you and others.

Ensure your business complies with the full PCI Standards by completing the SAQ available on any of the websites of the card schemes listed.

UNIONPAY

UPI - Union Pay International (formerly known as China Union Pay (CUP)) is a card scheme that originates from Mainland China & operates worldwide with acceptance and issuance ability of both Debit & Credit card ranges that can be accepted at selected merchants across UAE and the Gulf

When accepting payment on a UPI cards remember the following:

- All UPI cards MUST be inserted or swiped through your terminal and PIN authenticated to obtain online authorization.
- Neither fallback nor manual processing is allowed.
- UPI cardholders must sign the transaction receipt and enter a PIN for all UPI card types.
- Behavior and card security checks should always be conducted as per the Card Present section in this booklet and the Card Security Features document. If a UPI card is presented and the transaction is declined due to incorrect PIN, decline the transaction. ADIB MERCHANT SERVICES - HELPDESK does **NOT** support authorization requests. If a transaction is declined you cannot accept the card for payment. Advise the cardholder to contact their bank.

Co-Branded UPI Cards

UPI credit cards can also be co-branded with MasterCard or Visa and will display the logos of both schemes i.e.: UPI and Visa Logo or UPI and MasterCard logo will appear on the front of the card. Co-branded can be accepted as per the above procedures and must be authorized with both PIN and signature.

EMV CARDS

An EMV or CHIP card contains a smart chip loaded with the information normally contained within the magnetic stripe of a card. The chip also contains further enhanced security features which may include a PIN to complete the transaction, making the production of counterfeit cards more difficult.

Chip cards have been introduced to limit the impact of the counterfeit card activity and have now replaced magnetic stripe based cards which are still vulnerable to card skimming. However, chip cards are also produced with a magnetic strip.

AUTHORISATION

An authorization confirms the following information at the time of the transaction:

- The card has not been reported as lost or stolen.
- There are sufficient funds to cover the purchase.

An authorization does not confirm payment or that the person providing the card details is the genuine cardholder. A risk remains that the purchaser has improperly obtained the card or card details. This risk is increased for Card Not Present transactions.

Suspicious Cardholder

If you are suspicious of:

- The cardholder
- The card

Dial the ADIB relationship manager and state “CODE 10”. (You will be transferred to an operator who will assist you).

Remember:

- Only use ‘Code 10’ if you are suspicious of the transaction. Do not use ‘code 10’ if you simply need to obtain an authorization.
- Authorization for UPI card transactions cannot be obtained by contacting ADIB MERCHANT SERVICES Call Center. If a transaction declines you cannot accept the card for payment. Advise the cardholder to contact their bank.

Debit Cards and Charge Cards

Fraudulent transactions can also occur on Debit and Charge Cards (AMEX, Diners and JCB). Ensure that you apply the pre-cautions enclosed within this booklet to all Debit and Charge Card transactions.

For further enquiries on these types of transactions contact your relationship manager.

PROTECTING OUR MERCHANTS FROM FRAUD

ADIB MERCHANT SERVICES Fraud Detection Team proactively monitors irregular trading patterns. So that when a transaction occurs outside the normal behavior of the merchant and is identified in our systems it will be brought to the attention of a fraud analyst who assesses the transaction and follows-up where necessary.

However, our Fraud Management Solution is only a component of a good fraud detection and prevention strategy as we cannot always pinpoint every fraudulent transaction. You as the merchant are often in the best position to identify suspicious activity and you need to understand your detection and prevention responsibilities.

This fraud education material has been developed to increase your understanding of how fraud can occur, the risks you face and how you can best protect your business.

For further inquiries on fraud prevention or to arrange for a card acceptance training session, do contact your relationship manager.

Disclaimer: *Adopting some or all of these suggestions will not guarantee that you will not be exposed to card fraud. Your liability of card fraud is detailed in your merchant agreement.*

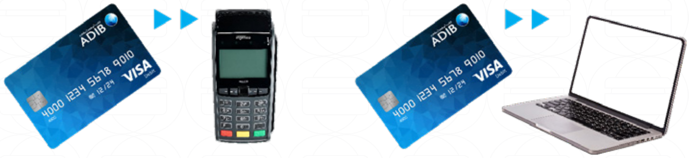
The Risks & Regulations on "Double Swiping"

"Double Swiping" is a term used in the industry to describe the act of a second swipe of a payment card at merchant ECR terminal after the first swipe to obtain initial authorization from the bank. This second swipe effectively exposes a payment card's magnetic stripe full track data to compromise.

Criminals are constantly attempting to access and compromise merchant ECRs that are not PCI-Compliant. The double swiping activity may result in track data being captured at these ECRs which are then used to make counterfeit cards.

Step 1: Merchant Dips or Swipes the Card for Authorisation

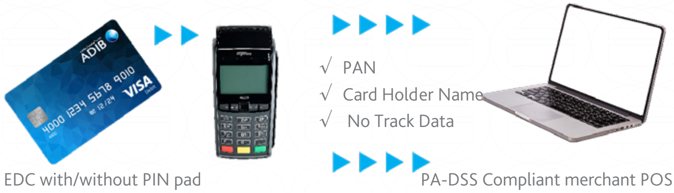
Step 2: Merchant "Double Swipes" on a non PA-DSS Terminal



EDC with/without PIN pad

Merchant POS system

"Single Dip" and use PA-DSS certified POS systems



√ PAN

√ Card Holder Name

√ No Track Data

EDC with/without PIN pad

PA-DSS Compliant merchant POS system

Merchant must NOT "Double Swipe" on unsecured PPOS systems. If card data is required, integrate and transmit only non – sensitive information to third party POS systems.

"Merchants that have been allegedly implicated in a potential account data compromised event may be subjected to fines and other recovery fees by ADIB. Merchants will also be required to conduct forensics investigations by a PCI Forensic Investigator (PFI).

VISA, MasterCard & Central Bank of UAE Mandate:

In line with the Central Bank of UAE notice number 242/2016, In order to enhance the data protection and prevent Payment Card related frauds, the POS merchants are hereby instructed to have suitable, operational & technological changes to their card acceptance practices so as to eliminate Double-swiping of payment cards through their EDC machines.

Merchants are not permitted to use or request Visa/Master account data for any purpose that is not related to payment for goods and services. Please call your relationship manager immediately and to report.

Glossary

American Express: American Express Travel Related Services Company, Inc.

Approval Code: An Authorization Code indicating that the Transaction is approved and the Card may be honored.

Authorization: A required procedure by which a Merchant requests of a Transaction from the Issuer. Authorization is initiated by accessing the authorization center by telephone or POS Devise.

Bank Identification Number (BIN): The identification number assigned to a Merchant that is used for Card issuing, Authorization, Clearing and Settlement processing.

Batch: The accumulated Card Transactions stored in the POS Devise or Host computer.

Bill Payment: PIN-less Debit Card payment Transactions resulting in funds transfer from Cardholders to Merchants in connection with payments for recurring services (excluding casual or occasional purchases) for which a corresponding invoice is periodically presented to the Cardholder by the Merchant and which Transaction is initiated via a telephone (Voice Recognition Unit, Interactive Voice Recognition) or Internet device.

Card: A plastic issued by a bank or other financial institution or by a Card company (e.g., Visa and MasterCard, Covered/Credit Cards and Debit Cards), that allows a Cardholder to pay for purchases by credit, charge, or debit.

Card Present: The processing environment where the Payment device is physically presented to the Merchant by the Cardholder as the form of payment at the time of Transaction.

Card Not Present: The processing environment where the Payment device is not physically presented to the Merchant by the Cardholder as the form of payment at the time of the Transaction. Card Not Present includes but is not limited to Mail Order (MO), Telephone Order (TO), and Electronic Commerce (EC).

Cardholder: (i) the individual in whose name a Payment Device has been issued; and (ii) any individual who possesses or uses a Payment Device and who purports to be the person in whose name the Payment Device was issued or who purports to be an authorized user of the Payment Device.

Card Identification Number (CID) or Card Validation Code (CVV2/CVC2): a number printed on a Card and used as additional verification for Card Not Present Transactions. For American Express this is a four-digit code printed above the Card account number. For Visa, MasterCard and Discover Network this is a three-digit card code value printed on the signature panel of the Card.

Card Rules: The Covered/Credit Card Rule, collectively.

Card Validation Code: Card Identification Number.

Cash Advance: A Transaction in which a Cardholder receives cash from a financial institution or an ATM.

Chargeback: A transaction dispute by a Cardholder or Issuer pursuant to the Payment Network Regulations.

Chip: A microchip that is embedded in a Card that contains cardholder data in an encrypted format.

Chip and PIN Technology: Any technology in whatever form introduced by any Payment Network which employs Chip embedded Cards and/or the use of a PIN in conjunction with or in replacement of a manual signature of Cardholder.

Chip Card: A Card embedded with a Chip that communicates information to a Chip-Reading Device.

Chip-Reading Device: A POS Device capable of reading, communicating and processing Transaction data from a Chip Card.

Code 10 Authorization: An Authorization or an "additional verification step" obtained for a suspicious or questionable Transaction, Card or Cardholder.

Complaint Chip Card: A chip Card that complies with all Payment Network Regulations.

Confidential Information: All information or items proprietary to any party to the Agreement of which the other party to the Agreement obtains knowledge or access as a result of the relationship formed as a result of the Agreement including, but not limited to the following types of information and other information of a similar nature (whether or not reduced to writing): scientific, technical or business information, product makeup lists, ideas, concepts, designs, drawing, techniques, plans calculations, system designs, formulae, algorithms, programs, software (source and object code), hardware, manuals, test procedures and results, identity and description of computerized records, identity and description of suppliers, customer lists, processes, procedures, trade secrets, "know-how", marketing techniques and materials, marketing and development plans, price lists, pricing policies, and all other financial information.

Contactless: A payment card or key fob equipped with a chip and antenna that securely communicates Cardholder account information via radio frequently to a POS Device.

Copy Request: Retrieval Request.

Covered/Credit Card: this includes any of the following cards or devices that are associated to the Person to whom the card or device is issued: (i) a Visa covered/credit card or device bearing the symbol(s) of Visa International; (ii) Master covered/ credit card or device bearing the symbol(s) of MasterCard International Incorporated.

Credit Card Associations: (i) Visa; (ii) MasterCard; (iii) American express; (iv) Diners; (v) UnionPay; and (viii) any other organization or association that hereafter contracts with Servicer and/or Member to authorize, capture, and/or settle Transactions effected with Covered/ Credit Cards or signature-based Debit Cards issued or sponsored by such organization and any successor organization or association to any of the foregoing.

Covered/Credit Card Rules: All applicable rules and operating regulations of the Credit Card Associations, and all rules, operating regulations, and guidelines for Covered/Credit Card Transactions issued Servicer from time to time, including, without limitation, all amendments, charges and revision made thereto from time to time.

Credit Transaction Receipt: A document in paper or electronic form evidencing a Merchant's refund or price adjustment to be credited to the Cardholder's account and debited from the

Merchant's DDA. This is also known as a credit slip or credit voucher.

CVV2/CVC2: Card Verification Value .

Customer: A client of Merchant who elects to conduct a payment Transaction with Merchant through presentation of a Payment Device (including a Cardholder).

Debit Card: A card or device bearing the symbol(s) of one or more EFT Network or Credit Card Associations, which may be used to purchase goods and services from Merchant or to pay an amount due to Merchant by an electronic debit to the Cardholder's designated deposit account. A "Debit-Card" includes (i) a card or device that bears the symbol of a Credit card Association and may be used to conduct signature-based, offline debit transactions, and (ii) a card or device that bears the symbol of an EFT Network and be used to conduct PIN based, online debit transactions.

Diners: Diners Club International Ltd.

Discount: A type of fee paid by Merchant to process its Card Transactions. Discount is calculated by multiplying the Discount rate by the volume of Card transactions.

Dynamic Currency Conversion (DCC): The conversion of the purchase price of goods or services from the currency in which the purchase price is displayed to another currency as agreed to by the Cardholder and Merchant. The currency becomes the Transaction currency, regardless of the Merchant's local currency.

EGC: Electronic Gift Card.

Electronic Commerce Transaction: A Transaction that occurs when the Cardholder uses the Internet to make a purchase from a Merchant or Merchant uses the Internet to submit the Transaction for processing.

Gift Card (EGC): A special card purchased by a Customer or provided by Merchant to a Customer that is redeemable for merchandise services or other Transactions. A program that allows a Merchant to sell Electronic Gift Cards redeemed for in-store merchandise or services.

Embossing: The process of printing data on a Card in the form of raised characters so that the Card may be used in the imprinting of Transaction receipts.

Encryption: A security or anti-fraud technique that scrambles data automatically in the POS Device before the data is transmitted. For example PIN's are encrypted when transmitted for Authorization.

High-Risk Payment Service Provider: A Payment service Provider that facilities Transactions on behalf of high-risk Sponsored Merchants.

Hologram: A three-dimensional image include on a Card to discourage counterfeiting.

Host: The central server we use to store Merchant information and to route information between the Merchant and the Issuers.

Issuer: The financial institution or other entity that issued and Covered/Credit Card or Debit Card to a Cardholder.

JCB: JCB International Co., Ltd.

Laws: All applicable local, state, and federal statues, regulations, ordinances, rules and other binding law in effect from time to time.

Magnetic Stripe: A stripe of magnetic material affixed to the back of a Card that contains Cardholder account information.

Mail Order/Telephone Order (MO/TO) Transaction: For MO, a Transaction that occurs when the Cardholder uses the mail to make a payment a Merchant and for TO, a Transaction that occurs when the Cardholder uses a telephone to make a payment to a Merchant.

Manual Entry Authorization: An Authorization request generated when the Merchant key-enters the Cardholder's Card number, expiry date and sales amount into the POS Device (e.g., when the POS Device is unable to read the Cardholder information from the Magnetic Stripe on the Card).The POS Device then dials out to the appropriate Authorization Center to obtain an Authorization Code.

MasterCard: MasterCard International Incorporated.

Member: A financial institution designated by us that is a principal, sponsoring affiliate or other member of Visa, MasterCard or other member of the applicable Payment Network. The Member may be changed by Servicer at any time and the Merchant will be provided notice of same.

Merchant: The business entity that provides goods and/or services to Customers.

Merchant Application: The Merchant Application and any additional document containing information regarding Merchant's business that is submitted to Servicer and Member in connection with Merchant's application for processing services, including documents submitted by Merchant as a part of the bid process, if applicable.

Merchant Category Code (MCC): The four-digit code and corresponding definition assigned to each Merchant that describes the type of business in which the Merchant is engaged.

Merchant Identification Number (MID): A unique identification number assigned to a Merchant to identify its business

Merchant Statement: A summary of activity in a Merchant account.

Payment Card Industry Data Security Standard (PCI DSS): The data security regulations including maintaining Cardholder account data in a secure environment and other data security best practices endorsed by the major card associations including Visa and MasterCard, as such may be amended from time to time.

Payment Device: Any device used for the purpose of obtaining credit or debiting a designated account including a Covered/Credit Card, Debit Card, and any other financial transaction device, including an electronic Gift Card, check (whether converted into electronic form or used as a source document for an electronic fund transfer), stored value card, "smart" card, or other device created to be used for the purpose of obtaining credit or debiting a designated account, that is now or hereafter affected through Transaction with Merchants.

Payment Network: Any Covered/Credit Card Association, EFT Network, governmental agency or authority and any other entity or association that issues or sponsors a Payment Device.

Payment Service Provider: A merchant that is registered by Acquirer and Member with the Payment Networks to facilitate Transactions on behalf of Sponsored Merchants.

Person: Any individual, firm, corporation, business trust, partnership, governmental agency or authority or other entity and shall include any successor (by merger or otherwise) of such entity.

Personal Identification Number (PIN): A number that must be entered by a Cardholder in order to complete certain types of Transactions (e.g., online debit,).

PIN Pad: A secure device with an alphanumeric keyboard which conforms with the Debit Card Rules and applicable standards administered by the Payment Card Industry Security Standards Council and requirements establish from time to time by servicer and through which a Cardholder may enter a PIN.

POS Device: A terminal, software, or other point-of-sale device at a Merchant location that conforms with the requirements established by Servicer and the applicable Payment Network.

Pre-authorized Order: A written or electronic authorization by a Cardholder allowing a Merchant to charge his or her Card at a future date.

Prepaid Card: A card having available funds paid for in advance by the Cardholder.

Program: The Payment Device processing services and other related products and services received by Merchant pursuant to the Agreement.

Retrieval Request: A request initiated by a Cardholder or Issuer that requires the Merchant to produce a legible copy of the Cardholder's signed Transaction Receipt within a specified within a specified period of time.

Services: The entity that processes Transactions on behalf of the Merchant.

Settlement: The process of submitting Transactions to the Servicer of processing.

Site Data Protection Program (SDP): MasterCard's data security regulations to protect Cardholder account data and other data security best practices. The exact requirements for SDP can be found at https://sdp.mastercardintl.com

Split Transaction: A prohibited process by which Merchants use multiple Transaction Receipts to avoid Authorization for a single Transaction.

Transaction: Any action by a Cardholder using a Payment Device and a Merchant that results in activity on the Cardholder's account (e.g. payment, purchase, refund, return, or debit).

Transaction Data: All information regarding the Transaction including without limitation the Cardholder account number, dirham amount of the Transaction and in information stored in the Card's Magnetic Stripe.

Transaction Date: The date that a Transaction occurs.

Transaction Receipt (Slip): The paper or electronic record evidencing the purchase of goods or services from or payment to a Merchant by a Cardholder using a Payment Device.

UnionPay (UPI): Union Pay International

Visa: Visa International.

PCI Industry

The payment card industry data security standard 'PCI DSS'

Visa and MasterCard have developed the Payment Card Industry Data Security Standard or 'PCI DSS' as a means of managing risk of external and internal data compromises. This is a set of industry-wide requirements and processes, supported by every major international payment card system through the PCI Security Standards Council or 'PCI Council'.

The PCI DSS has 12 basic requirements that focus on using secure systems. The standards include installing a firewall, changing default passwords, protecting stored data, using antivirus software and encrypting transmissions of cardholder data across public networks.

The way PCI DSS relates to your business and the way in which it should be implemented will depend on:

- The size and nature of your business.
- The configuration of your card acceptance system and processes.
- The service providers you work with and their respective roles.

The PCI DSS requirements

By following the PCI DSS requirements you can assess if your business protects cardholder data, has a secure network, maintains a security policy, maintains strong access control measures, regularly monitors and tests networks, utilises a third party and if so, if they are also meeting the PCI DSS requirements. The 12 PCI DSS requirements are as follows:

Build and maintain a secure network.

1. Install and maintain a firewall configuration to protect cardholder data.

2. Do not use vendor-supplied defaults for system passwords and other security parameters.

Protect cardholder data

3. Protect stored cardholder data.

4. Encrypt transmission of cardholder data across open public networks.

Maintain a vulnerability management program

5. Use and regularly update anti-virus software or programs.

6. Develop and maintain secure systems and applications.

Implement strong access control measures

7. Restrict access to cardholder data by business need-to-know.

8. Assign a unique ID to each person with computer access.

9. Restrict physical access to cardholder data.

Regularly monitor and test networks

10. Track and monitor all access to network resources and cardholder data.

11. Regularly test security systems and processes.

Maintain an information security policy

12. Maintain a policy that addresses information security for employees and contractors.

Further information can be obtained from www.pcisecuritystandards.org

The benefits to your business

By following the industry-wide requirements of the PCI DSS, businesses can:

- Protect customer data.
- Provide a complete ‘health check’ for any business that stores or transmits customer information.
- Lower exposure to financial losses and remediation costs.
- Maintain customer trust and safeguard the reputation of their brand.

Don’t put your customers or your business at risk

Protecting your customers’ account information from the growing threat posed by high-tech criminals is one of the biggest challenges facing businesses today. As technology used by merchants and their partners has evolved, card fraud has become more sophisticated.

Any business that processes, stores or transmits cardholder account data is a potential target. It is important for merchants to understand what measures need to be taken every day to ensure the security of highly sensitive personal financial information.

How do I get started?

Visa and MasterCard have created a set of tools and resources to make PCI DSS implementation simple and straightforward.

To learn what your specific compliance requirements are, check with your card brand compliance program:

- **American Express:** *www.americanexpress.com/datasecurity*
- **JCB International:** *http://partner.jcbcard.com/security/jcbprogram/index.html*
- **MasterCard Worldwide:** *http://www.mastercard.com/sdp*
- **Visa Inc:** *http://www.visa.com*

Frequently asked questions

Who needs to be compliant?

All entities that store, process and/or transmit cardholder data, such as merchants, service providers (e.g. payment gateways, SPSP, processors), must comply with the PCI DSS. The requirements apply to all acceptance channels including retail (brick-and-mortar), mail and telephone order 'MOTO,' and e-commerce. The obligation to comply may also arise under your Merchant Agreement.

How do I know if I meet the PCI DSS requirements?

To check that you have met the PCI DSS requirements, you will need to complete one or more of the following validation tasks (depending on the annual volumes you process).

These standards include:

- The Self-Assessment Questionnaire 'SAQ'
- Vulnerability Scan
- On-site Review.

Do I have to complete all the validation tasks?

Visa and MasterCard have defined four merchant levels to determine the requirements These are summarized in the table below:

Level	Visa/MasterCard	Validation Requirements
1	• Merchants processing over 6 million transactions annually (all channels), or global merchants identified as Level 1 by any card scheme	• Annual on-site assessment by QSA • Quarterly network scans by ASV • Attestation of compliance
2	• Merchants processing 1 million to 6 million transactions annually (all channels)	• Annual SAQ • Quarterly network scans by ASV • Attestation of compliance
3	• Merchants processing 20,000 to 1 million e-commerce transactions annually	• Annual SAQ • Quarterly network scans by ASV
4	• Merchants processing less than 20,000 e-commerce transactions annually, and all other merchants processing up to 1 million transactions annually	• Annual SAQ • Quarterly network scans by ASV

What is a vulnerability scan?

A vulnerability scan ensures that your systems are protected from external threats such as unauthorized access, hacking or malicious viruses. The scanning tools test all of your network equipment, hosts and applications for known vulnerabilities. Scans are intended to be non-intrusive and are conducted by an Approved Scanning Vendor (ASV).

Regular quarterly scans are necessary to ensure that your systems and applications continue to afford adequate levels of protection. For a list of ASVs that provide vulnerability scanning, please visit *www.pcissc.org*

What is the Self-Assessment Questionnaire?

The SAQ is a free, confidential tool that can be used to gauge your level of compliance with the PCI DSS. It is an online tool made up of a series of 'yes' and 'no' questions. Once it has been completed, you will have made a good assessment of your risk level. If the assessment indicates that remedial work is needed, you will need to undertake this work in order to comply with the PCI DSS. You can complete the process internally or work with a QSA to manage it on your behalf.

Once completed, the SAQ will provide you with an assessment of where potential risks may lie. The questionnaire will also point out if any remedial action is required. If this occurs, you must make sure that you act quickly to ensure compliance with the PCI DSS standards.

The appropriate SAQ can be downloaded from the PCI Council website and can be completed manually and submitted to the bank. Alternatively a number of Scan vendors support acquiring online completion of the SAQ on their websites.

You can visit the PCI Council website at: *www.pcisecuritystandards.org/*

What do I do once I acknowledge my validation to PCI DSS compliance?

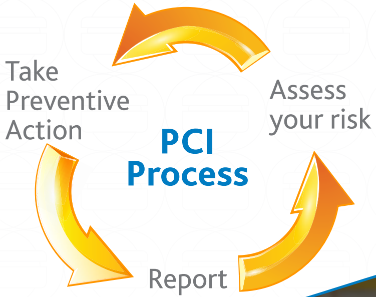
All information relating to PCI DSS certification should be stored in a safe location on your merchant premises and your certificate of compliance must be emailed to

What if I choose not to be involved in the program?

Merchants must adhere to PCI DSS requirements, failure to do so may give rise to a breach of the Merchant Agreement and/or lead to your merchant facilities being suspended or terminated.

If you are at fault for a security breach, business fallout can be severe:

- Fines and penalties
- Termination of ability to accept payment cards
- Lost confidence, so customers go to other merchants
- Lost sales
- Cost of reissuing new payment cards
- Legal costs, settlements and judgments
- Fraud losses
- Higher subsequent costs of compliance
- Going out of business



Payment Application Data Security Standard

The PCI Payment Application Data Security Standard (PA-DSS) Requirements and Security Assessment Procedures define security requirements and assessment procedures for software used by merchants to process Payment Card transactions.

The PA-DSS requirements are derived from the Payment Card Industry Data Security Standard (PCI DSS) Requirements and Security Assessment Procedures. The merchants are required to ensure the Payment Applications used to process Payment card transactions are secure and comply with PA-DSS standards.

Secure Payment Applications, when implemented in a PCI DSS-compliant environment, will minimize the potential for security breaches leading to compromises of primary account number (PAN), full track data, card verification codes and values (CAV2, CID, CVC2, CVV2), PINs and PIN blocks, and the damaging fraud resulting from these breaches.

The PA DSS requirements

The merchant must ensure the software used for Payment card transactions includes the following 12 protections

1. Do not retain full magnetic stripe, card validation code or value, or PIN block data.
2. Protect stored cardholder data.
3. Provide secure authentication features.
4. Log payment application activity.
5. Develop secure payment applications.
6. Protect wireless transmissions.
7. Test payment applications to address vulnerabilities and maintain payment application updates.
8. Facilitate secure network implementation.
9. Cardholder data must never be stored on a server connected to The Internet.
10. Facilitate secure remote access to payment application.
11. Encrypt sensitive traffic over public networks.
12. Encrypt all non-console administrative access.

Further information can be obtained from

www.pcisecuritystandards.org