RAKBANK pay | RAKBANK Simply Better

www.rakbank.ae

RAKBANK

Merchant Best Practices & Guidelines

RAKBANK pay | RAKBANK Simply Better

TABLE OF CONTENTS

INTRODUCTION 1

GUIDELINES TO REDUCE MERCHANT RISKS 2
CARD PRESENT TRANSACTIONS 2.1
CARD NOT PRESENT TRANSACTIONS 2.2

GOODS DELIVERY 3

REFUNDS 4

THIRD PARTY PROCESSING 5

CHARGEBACK 6

IMPORTANT INFORMATION TO REMEMBER 7

SECURE THE TERMINAL 8

PCI INDUSTRY 9

FREQUENTLY ASKED QUESTIONS 10

GLOSSARY 11

1. INTRODUCTION:

With countless incidents of fraud occurring every day, fraud prevention is the top most priority for individuals and companies alike. The purpose of this guide is to provide merchants and their back-office sales staff with accurate, up-to-date information and best practices to help merchants process all kinds of card transactions while minimizing the risk of loss from fraud.

RAKBANK is committed 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 Merchant Best Practices Guide. The more you know about the potential risks the more you'll be able to protect your business against chargebacks and fraud.

2. GUIDELINES TO REDUCE MERCHANT RISKS

2.1 CARD PRESENT TRANSACTIONS

Card-present transactions are those in which both the card and cardholder are present at the point of sale. Once the Cardholder presents the card for payment, 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.

CHECK CARD DETAILS

- 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 colour 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 CARD

- Never manually enter the credit card number. Take extra caution if the customer requests you to manually key a transaction.
- 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 amounts and/or suspicious transaction ask for ID proof (copy of original passport or any other photo ID which matches details with card details).

BE WARY IN SITUATIONS 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.
- 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.
- 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 RAKBANK 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 your Relationship Manager.
- Do not handover the RAKBANK POS terminal to the cardholder in order to conduct the transaction, the POS terminal should be operated by the Merchant or Merchant authorized staff only at all times.

Visa Brand Mark Card Security Features

Embossed/ Unembossed or Printed Account Number on valid card begins with "4". All digits must be even, straight and the same size.

Chip may appear on the card front

Dove hologram may appear on the front or back of the card

Visa Brand mark may be placed in the upper left, upper right, or lower right corner of the card

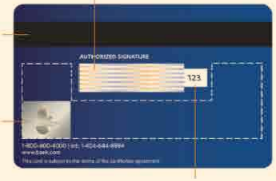
Ultraviolet V is visible over the Visa logo when the card is placed under an ultraviolet light

Four to six Digit Bank Identification Number (BIN) must be printed directly below the account number and must match exactly with the first four digits of the account number

Expiration or "Good Thru" dates should appear below the account number

The Signature Panel must appear on the back of the card and be signed

Magnetic stripe is encoded with the Card's identifying information



The Mini-Dove Design Hologram may appear on the back anywhere within the outlined areas shown here. The three-dimensional dove hologram should appear to move as you tilt the Card.

Card Verification Value (CVV)* is a unique three-digit

Mastercard Brand Mark Card Security Features

FRONT

Card Feature	Description
1	The first 4 digits of the account number must match the 4 digit preprinted BIN. Remember that all Mastercard account numbers start with the number 5
2	The last 4 digits of the account number must match the 4 digits that appear on the cardholder receipt
3	The global hologram is three dimensional with a repeat 'Mastercard' printed in the background. When rotated the hologram will reflect light and appear to move
4	The stylized 'MC' security feature has been discontinued but may continue to appear on cards through 1 June 2010.

CARD BACK

Card Feature	Description
1	The signature panel is tamper-evident with the word 'Mastercard' printed in multiple colors at a 45 degree angle. For magnetic swiped transactions, remember to compare the signature on the back of the card with the cardholder's signature on the receipt
2	The 4 digits printed on the signature panel must match the last 4 digits of the account number, followed by the 3-digit CVC 2 number

2.2 HOW TO REDUCE THE RISK OF CARD NOT PRESENT FRAUD

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:

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 especially for large and/or suspicious orders 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.
- If you take payments via a website, contact your gateway provider and see if they have any fraud prevention software which you can utilise.
- Keep all copies of correspondence including invoices, emails, quotations, faxes, proof of delivery, etc.
- Always obtain authorisation for all card not present transactions, regardless of value, and for the full amount of the transaction.

Remember, an authorisation 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.

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.

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.

Secure your customers' data

At RAKBANK, we are committed to providing our merchants assistance to help protect their business, and their customers, from the growing threat posed by online fraudsters. 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.

RAKBANK 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, Mercury, Diners & Discovery, Union Pay International 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 RAKBANK immediately.

Risk mitigation for Online Merchants

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

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

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, trade license number, and address.
- Telephone number and fax number where available.
- A clear explanation of shipping practices and delivery policy/timeframe.
- Transaction currency: RAKBANK merchants can process AED amount only, unless enrolled for dynamic currency services 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.

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, which 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.

For further information on data security standards please refer to following website https://pcisecuritystandards.org/merchants/

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.

3. GOODS DELIVERY

A common point of fraudulent transactions is allowing someone, particularly a third party, to pick up the goods from your store after a telephone order has been placed without the credit card being presented, a card imprint taken or signature obtained. Deliveries should always be made by your carrier or by a reputable courier engaged by you, not by your customer.

For deliveries the following procedures are recommended:

- Ensure the person making the delivery delivers the goods to a person inside the premises, not someone waiting outside.
- The deliverer should always obtain the signature of the person taking the delivery.
- Never deliver to car parks or parks.
- Try to deliver only to physical addresses, take extra caution when delivering to hotels and PO BOX addresses.
- Be wary of orders going overseas, recent fraud trends have indicated Africa and Asia fraudsters targeting UAE merchants with stolen credit card numbers.
- Site the card wherever possible upon delivery of the goods.
- Check internet maps and street views to verify business.

4. REFUNDS

You are not permitted to:

- Refund a transaction back to a card other than the one used to make the original purchase.
- Send the refunded amount to the customer via cash, the Internet, money order or international money transfer.
- It is also beneficial to monitor all refunds processed. An increasingly common form of fraud involves employees using your EFTPOS solution to process refunds to their own cards. Ensure only authorized staff have access to process refunds and be aware of your refund limits.
- Regularly change your refund password. Do not use a generic password such as 9999.

5. THIRD PARTY PROCESSING

Third party processing is forbidden. Third party processing is where you process a transaction on behalf of another company or person. If any transactions are deemed as fraudulent, you will be responsible for the chargeback of that transaction. Here are some typical scenarios of third party processing:

'If you process these transactions I will give you 15% of the total sales'.
'My terminal is broken and the bank can't fix it till later this week, can you please process this transaction for me as I will lose the sale?'

6. CHARGEBACK

A chargeback is a reversal of a credit card transaction and usually occurs when a customer raises a dispute with their financial institution (also known as the Issuer) in relation to a purchase made on their credit card. A chargeback may cause the amount of the original sale and a commission / discount amount to be deducted from the merchant's account.

The reasons why chargebacks arise vary greatly but are generally the result of a customer or issuer bank being dissatisfied with their purchase or due to illegal or fraudulent activity/use of their card.

Common chargeback:

- Transaction not recognized by the cardholder
- Transaction not authorized by the cardholder
- Duplicated transactions
- Cancelled recurring/direct debit transactions
- Goods/services not received or faulty
- Goods/services not as described
- Declined Authorization
- Fraudulent multiple transactions
- Legal proceedings
- Point-of-Sale errors
- Delayed Charges
- Invalid / Incorrect Card / Account number used
- Late Presentment / Expired Card

The Chargeback process:

a. Transaction is disputed. Cardholder raises problem with their financial institution (known as the Issuer) or the Issuer discovers a breach of the card scheme rules.
b. Issuer advises RAKBANK via schemes.
c. RAKBANK may request documentation from the merchant to verify the transaction. The merchant has a set timeframe to respond to retrieval requests, usually 10 days.
d. If the dispute is invalid, RAKBANK will decline the chargeback and return it to the Issuer.
e. If the chargeback is valid, the chargeback amount is debited from the merchant's account and written notification is provided to the merchant. A commission / discount amount may also be charged to the merchants account.

7. IMPORTANT INFORMATION TO REMEMBER

- If you are suspicious, contact RAKBANK - Risk & Fraud team prior to the processing and dispatching of the goods.
- Always obtain authorization, especially for online transactions, regardless of value and for the full transaction amount.
- Look at the decline codes on the POS terminal when a transaction rejects, does the code indicate the card is lost or stolen? If so retain the card. Is the card number valid? If not do not proceed with the transaction or accept another card.
- Do not lower the amounts, split sales or accept card after card.
- Be mindful of overseas orders.
- Never conduct third party processing.
- Store your customer's information securely. Ensure all your computer systems are password protected and data maintained on databases should be encrypted. Ensure all paper records are securely stored with restricted access. Never store the CVV2/CVC2 or full card track data. Report all security incidents.
- Train your staff. Ensure your staffs are aware and vigilant of potential fraudsters.
- Be aware of what your staffs are processing. Staff has been found to be involved in fraudulent activity. Look out for staff refunding to their own credit cards or storing unnecessary customer information.
- Be extra cautious on high risk transactions including: card not present, manually keyed, no authorization obtained or fallback transactions.

Adopting these suggestions may help reduce fraud but will not guarantee that you will not be a victim of credit card fraud. It is your responsibility to confirm that the purchaser is the genuine cardholder, as you may be liable for the transaction in the case of a chargeback under your merchant agreement terms and conditions. Merchants should be aware of their responsibilities under their RAKBANK Merchant Terms & Conditions.

8. SECURE THE TERMINAL

Fraud and misuse of credit or debit card information is a growing problem for many merchants globally. The loss of customer card data and subsequent misuse may undermine customer confidence and potentially reduce card usage at your business. As part of RAKBANK's ongoing commitment to providing the most up to date information on terminal and cardholder data security, we have outlined a list of best practices for protecting your terminals and your customer's information.

Your RAKBANK merchant terminal is equipped with a number of in-built security features which are designed to protect your customers' information. By implementing the recommended best practices below, you can protect your business, your customers and your reputation from credit and debit card fraud or misuse.

Recommended best practices

- Always ensure that terminals are secure and under supervision during operating hours (including any spare or replacement terminals you have)
- Secure your equipment – do not leave terminals unattended.
- Ensure that only authorized employees have access to your terminals and are fully trained on their use when closing your store or kiosk, always ensure that your terminals are securely locked and not exposed to unauthorized access.
- Never allow your terminal to be maintained, swapped or removed without advance notice from RAKBANK or our partner Etisalat. Be aware of unannounced terminal service visits.
- Only allow authorized RAKBANK or our partner Etisalat personnel to maintain, swap or remove your terminal, and always ensure that security identification is provided.
- Inspect your terminals on a regular basis, to ensure that the terminal casing is whole with external security stickers remaining unbroken and of a high print quality.
- Ensure that there are no additional cables running from your terminal .
- Make sure that any CCTV or other security cameras located near your terminal(s) can't observe Cardholders entering details.
- The site manager reviews the CCTV recording each day to check or signs of criminal activity.
- Note should be taken of:
  - Time stamps – in case the camera was switched off for a period of time
  - Any blackouts
  - Any period when the image is blocked
  - Any incidence when the camera is moved
  - Any other suspicious footage
- You immediately examine all of your terminals if a camera has been moved, damaged, or if images have been blocked. This may be an indicator that criminals have targeted your merchant location.

It is important to notify RAKBANK immediately if:

a. Your terminal is missing
b. You, or any member of your staff, is approached to perform maintenance, swap or remove your terminal without prior notification from RAKBANK or our partner Etisalat and/or security identification is not provided
c. Your terminal prints incorrect receipts or has incorrect details
d. Your terminal is damaged or appears to be tampered with.

HINTS

- Trust your instincts! If a sale seems too good to be true, it probably is.
- All too often what a merchant might think is a great sale will turn out to involve some type of fraud.
- Take the time to properly investigate overseas orders from customers with whom you have never done business. That bit of extra work may well prevent you from becoming the victim of a fraud scheme and having to bare any associated chargebacks.

9. PCI INDUSTRY

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/

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:
- MasterCard Worldwide: http://www.mastercard.com/sdp
- Visa Inc: http://www.visa.com

10. FREQUENTLY ASKED QUESTIONS

1) 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.

2) 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.

3) 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 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 20,000 e-commerce transactions annually, and all other merchants processing up to 1 million transactions annually	• Annual SAQ • Quarterly network scans by ASV

4) 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

5) 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/

6) 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 rakbankpay@rakbank.ae

7) 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

11. GLOSSARY

American Express: American Express Travel Related Services Company, Inc.
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 Bank that is used for Card issuing, Authorization, Clearing and Settlement processing.
Batch: The accumulated Card Transactions stored in the POS Devise or Host computer.
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.
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.
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.
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 .
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.
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.
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.
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.
High-Risk Payment Service Provider: A Payment service Provider that facilitates 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.
Interchange: The incentive paid by the Acquirer Bank to the Card Issuer Bank for promoting payment through cards.
JCB: JCB International Co., Ltd.
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 Discount Rate (MDR): The commission charged by the acquirer (RAKBANK) to the Merchant (Trader/Service Provider). It is also termed as Merchant Service Fee (MSF).
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.
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.
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.
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.