belize bank
Our Country. Your Bank

Merchant Guide
to Card Acceptance

2023/2024 Edition

Contents

Introduction

The Card Acceptance Guidelines for merchants is a comprehensive manual for all businesses that accept card transactions in the card-present and/or card-absent environment. The purpose of this guide is to provide merchants and their support staff with accurate, up-to-date information and best acceptance practices to help merchants process transactions, understand the rules, and protect cardholder data while minimizing the risk of loss from fraud.

What is Card Acceptance?

It is the ability to process electronic payments such as debit, prepaid and credit cards via a Point-of-Sale terminal or Ecommerce facility (Website) for the exchange of goods and services.

Type of Merchant Services offered by Belize Bank

1. Point of Sale Terminal

- Acceptance of 3 major card brands (American Express, MasterCard, and Visa)
- Process transactions using dual interface (Chip or Contactless)
- The terminal supports Wifi, Ethernet Cable or 4G/Sim Card with a backup host capability.

2. Ecommerce

- Acceptance of two major card brands (MasterCard and Visa)
    - Acceptance of American Express cards in 2024.
- Quick, easy and secure integration to our Ecommerce service.
- API integration is readily available.
- The hosted payment page can be branded.
- No additional agreement needs to be signed. If you are a Belize Bank merchant already, there is no need to sign any additional documentation.
- PCI DSS compliance - merchants do not need to comply with PCI DSS and therefore can save costs. Bank complies with a standard and covers all costs related to it. In case of any fraud/scam attack, the merchant doesn't hold sensitive financial information of its customers. However, regardless of the extent of outsourcing to third parties, the merchant retains responsibility for ensuring that payment card data is protected. Connections and redirections between the merchant and the third party can be compromised, and the merchant should monitor its systems to ensure that no unexpected changes have occurred and that the integrity of the connection/redirection is maintained.
- Extra layer of security against fraud with 3D Secure.
    - What 3DSecure? Verified by Visa or 3D Secure provides merchants with cardholder authentication on eCommerce transactions. This added layer of security assists to reduce eCommerce fraud by helping to ensure that the transaction is being initiated by the rightful owner of the card account. This gives merchants greater protection on Ecommerce transactions.

3. E-Kyash

- Acceptance of digital payment from both banked and unbanked clients
- Lower merchant discount rate (effective 1% per transaction)
- Funds credited to your merchants wallet in real-time.
- After several years of working with merchants we see that merchants accepting E-kyash managed to increase their revenue by an average of 20% annually.
- Possibility to offer digital gift certificates and gain customers countrywide
- Direct API integration available
  - QR Code placed below will take you to the most recent API documentation, so you could start your integration and offer all cashless transactions available in Belize powered by the Belize Bank Limited.

SCAN ME!

E-Kyash API Docs

View Now

Point of Sale (POS) & E-Commerce Overview

Who is involved?

The processing of transactions consists of other parties beside the merchant and the cardholder.

- A cardholder is an authorized user of payment cards or other card payment products.
- A merchant is any business entity that is authorized to accept cards for the payment of goods and services.
- An acquirer is a financial institution that contracts with merchants to accept cards for payment of goods and services.
- A card issuer is a financial institution that maintains the cardholder relationship. It issues credit cards and contracts with its cardholders for billing and payment of transactions.
- Card Association or Card Networks - is an organization that facilitates payment card transactions. It regulates who, where, and how cards are used. Examples of card networks include, American Express®, Mastercard® and Visa®
    - It is a collection of systems that includes:
        - An authorization service through which card issuers can approve or decline individual card transactions.
        - A clearing and settlement service that processes transactions electronically between acquirers and card issuers to ensure that:
            - Transaction information moves from acquirers to card issuers for posting to cardholders' accounts.
            - Payment for card transactions moves from card issuers to acquirers to be credited to the merchant accounts.

Transaction Flow for Point of Sale (POS) Merchants

At the POS terminals, merchants can accept the following payment types and these are known as Card Present Transactions:

- Contactless (Tap or Wave card or mobile device)
  - Clients that have added their international issued cards (American Express, Mastercard, and Visa) to their Google Pay or Apple Pay wallet will be able to use their mobile device to make payment on our POS terminals.
- Contact (Insert Chip in chip reader)
- Magstripe (Swiping Magnetic stripe on card reader)

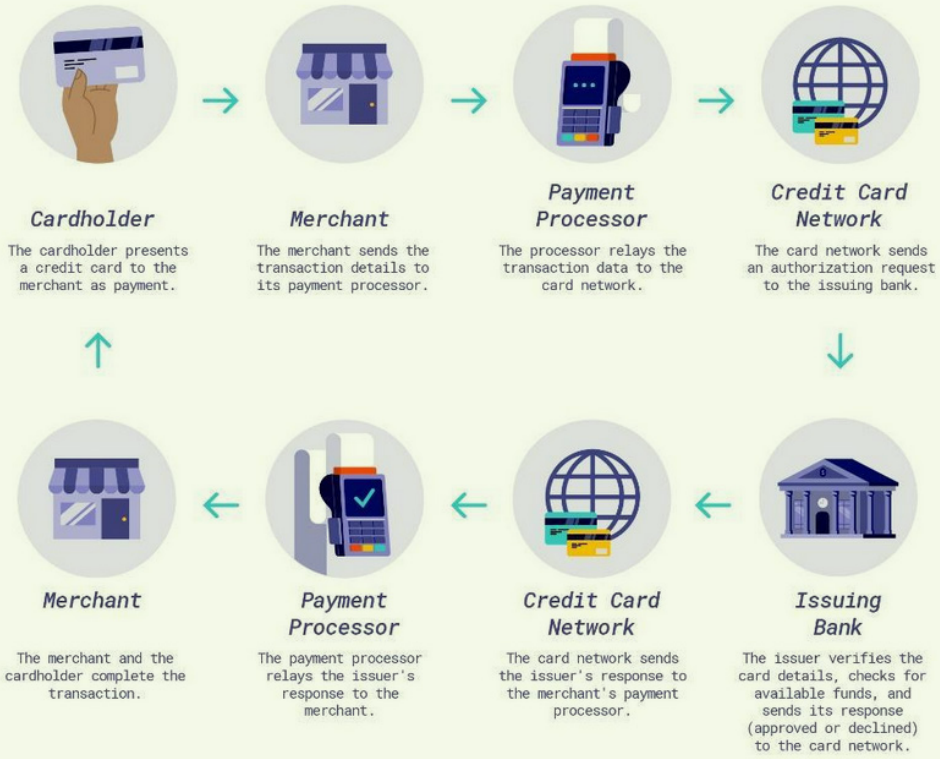
Transaction Life Cycles

The following illustrations show the life cycle of card-present (POS) transactions. Processing events and activities may vary for any merchant, acquirer, or card issuer, depending on card and transaction type, and the processing system used.

Online Authorization Process for Credit, Prep or Debit Transactions

During the authorization process, card transactions are approved or declined by the issuer, or by the card association on the issuer's behalf.

POS Transaction Cycle



Cardholder

The cardholder presents a credit card to the merchant as payment.

Merchant

The merchant sends the transaction details to its payment processor.

Payment Processor

The processor relays the transaction data to the card network.

Credit Card Network

The card network sends an authorization request to the issuing bank.

Issuing Bank

The issuer verifies the card details, checks for available funds, and sends its response (approved or declined) to the card network.

Credit Card Network

The card network sends the issuer's response to the merchant's payment processor.

Payment Processor

The payment processor relays the issuer's response to the merchant.

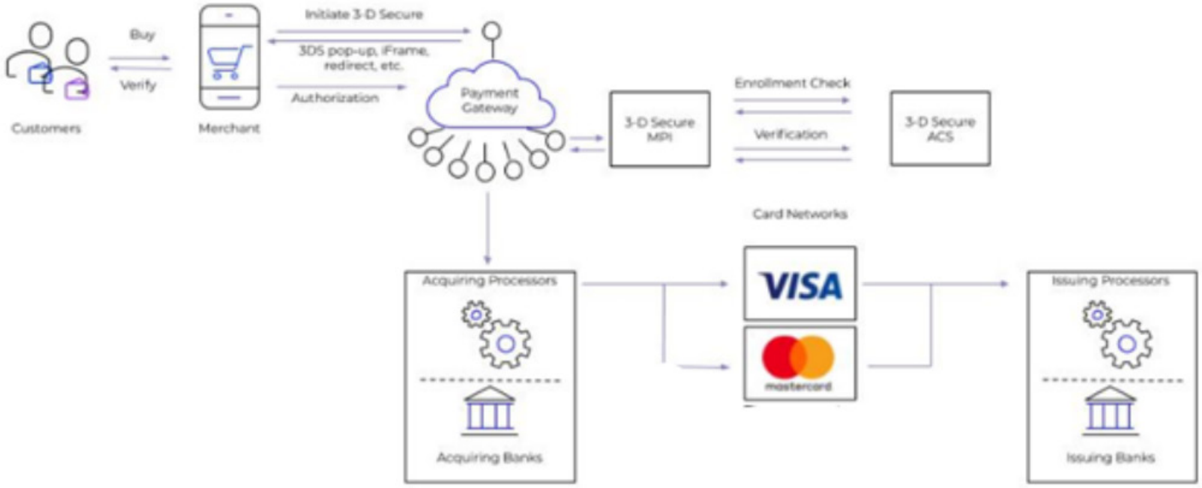
Merchant

The merchant and the cardholder complete the transaction.

Step 1	Merchant or cardholder waves or taps the card in front of the POS contactless reader, inserts the card into a chip-reading device, or swipes the card through a magnetic-stripe card reader. Transactions BZD$500.00/USD$250.00 or below, you should process as contactless Transactions above BZD$500.00/USD$250.00, process as contact Magnetic Stripe is only used when the card does not have a chip or contactless logo or if the POS prompts that chip cannot be read.
Step 2	Merchant enters the transaction amount and sends an authorization request to the acquirer (Belize Bank). Some transactions may require the cardholder to insert their PIN prior to processing the authorization. This is based on the chip profile of the issuing bank.
Step 3	Acquirer electronically sends the authorization request to the processor and then to the card association: American Express, MasterCard and Visa.
Step 4	The Card Association passes the request to the card issuer.
Step 5	Card issuer provides an online response.
Step 6	Card Association forwards the card issuer's authorization response to the acquirer.
Step 7	Acquirer forwards the response to the merchant.
Step 8	Merchant receives the authorization response and completes the transaction accordingly.

Step 9	Message to terminal and signature request, if required. Note: Transactions that require a PIN do not require a signature on the sales draft. Contactless transactions above BZ$100/US$50 will require a signature on the sales draft.

Transaction Flow for E-commerce Merchants



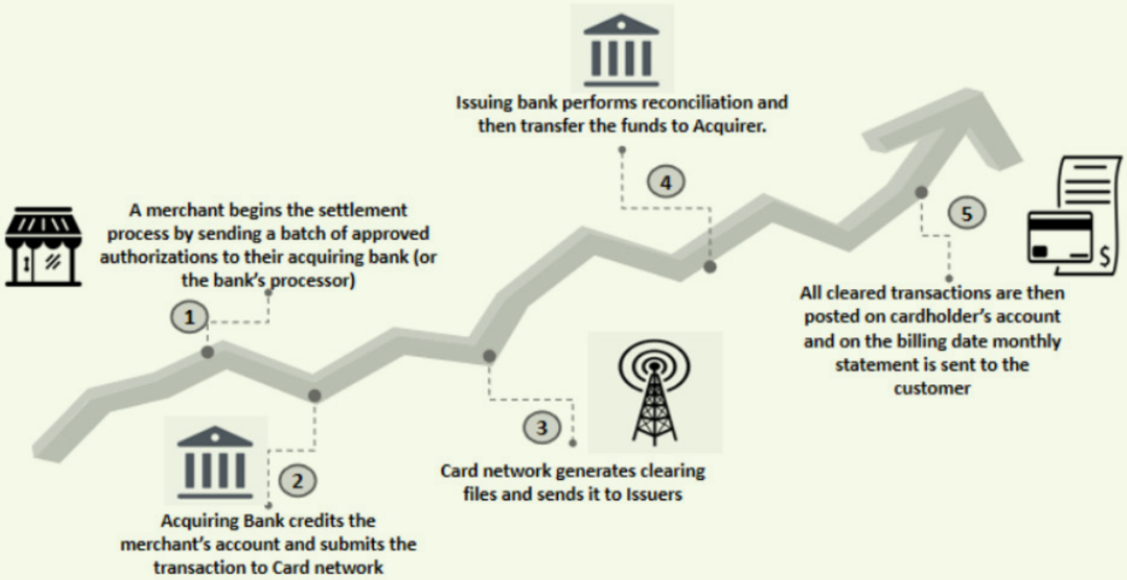
Step 1	Cardholder initiates transaction at ecommerce website on checkout page
Step 2	The transaction is routed to Payment Gateway for 3DS validation. Once a card is enabled with 3D secure, a 3Ds request will be initiated with the cardholder's bank via the payment gateway.
Step 3	Once authentication completed, payment gateway submits transaction for authorization to Acquiring Bank If the authentication is successful, the cardholder will be prompted to enter either a one-time password, PIN code, or respond to a security question to verify that they are the actual cardholder.
Step 4	Acquiring bank submits authorization request to Card Network (Mastercard or Visa, Amex in 2024)
Step 5	Card Network submits to Issuing Bank
Step 6	Issuing Bank responds to Card Network
Step 7	Card Network responds to Acquirer (Belize Bank)
Step 8	Acquirer (Belize Bank) submits responds to Ecommerce Merchant

Note: Customers won't always be subject to 3D secure measures and may not be asked to provide any details at all. This could be the case for transactions that are seen as 'low-risk', like payments under a certain amount or regularly recurring payments. After entering the correct information and once the card provider approves the payment, they will automatically be sent back to the merchant website with an order confirmation message. It's a quick and simple process.

Process of Clearing and Settlement of a Transaction for POS and E-commerce Merchants

During the clearing and settlement of a transaction, the transaction information moves from acquirers to card issuers for posting to cardholders' accounts. The Card Associations facilitate the payments to the acquirer for a transaction and the debit to the card issuer.

POS & Ecommerce Transaction Settlement Cycle


Issuing bank performs reconciliation and then transfer the funds to Acquirer.
4
A merchant begins the settlement process by sending a batch of approved authorizations to their acquiring bank (or the bank's processor)
1
5
All cleared transactions are then posted on cardholder's account and on the billing date monthly statement is sent to the customer
$
3
2
Card network generates clearing files and sends it to Issuers
Acquiring Bank credits the merchant's account and submits the transaction to Card network

Step 1	The merchant submits the transaction to the acquirer (Belize Bank Limited) Important Note: POS terminals should be settled daily. Effective October 1st, 2023, it is required for the bank to present all transactions to the card association within 3 calendar days. To ensure that Belize Bank Limited is in compliance with this new rule, we have enabled the Auto Settlement feature on our terminals. The auto settlement feature will automatically settle the POS batch at a specified time. The default time is 11:00 P.M.; however, this time can be adjusted to suit your business opening hours. Ecommerce Merchant website will automatically perform the closure of the batch at 4:00 PM
Step 2	The acquirer/processor credits the merchant's account and electronically submits the transaction to the card association for settlement.
Step 3	Card Association facilitates settlement and pays the acquirer and debits the card issuer account. They then send the transaction to the card issuer.
Step 4	Card Issuer posts the transaction to the cardholder's account and sends the monthly statement to the cardholder.
Step 5	Cardholder receives the statement.

Card Present Transactions

Card-present transactions are those in which both the card and cardholder are present at the point of sale. Merchants are required to take all reasonable steps to assure that the card, cardholder, and transaction are legitimate. Proper card acceptance begins and ends with sales staff and is critical to customer satisfaction and profitability.

A chip card is a plastic payment card with a microchip that is extraordinarily difficult to copy and re-use. Migrations to EMV[1] chip have proven the value of chip cards at reducing counterfeit fraud.

Doing it right at the Point-of-Sale (POS) Terminal

- Wave or tap the card (or mobile device) in front of the contactless point-of-sale terminal
- Insert the card into the chip-reading device
- Or swipe the magstripe through a magnetic card reader to request the transaction authorization.

Tap or Wave Card on Contactless Reader

Merchants are encouraged to:

- Tap the contactless card unto the POS contactless reader for transactions up to BZ$500/USD$250.
- If a card is tapped on contactless which exceeds the above mentioned limit, the POS will display Contactless Limit Exceeded and will prompt for the chip to be inserted.

[1] EMV is a payment method based on a technical standard for smart payment cards and for payment terminals and automated teller machines which can accept them. EMV stands for "Europay, Mastercard, and Visa", the three companies that created the standard.
EMV cards are smart cards, also called chip cards, integrated circuit cards, or IC cards, which store their data on integrated circuit chips, in addition to magnetic stripes for backward compatibility. These include cards that must be physically inserted or "dipped" into a reader, as well as contactless cards that can be read over a short distance using near-field communication technology. Payment cards which comply with the EMV standard are often called chip and PIN or chip and signature cards, depending on the authentication methods employed by the card issuer, such as a personal identification number (PIN) or digital signature.

- Follow the picture or diagram displayed on the terminal screen that shows which way the chip should face.
- Once the transaction is approved signature will be required for transactions greater than BZ$100/US$50.

Insert Chip Card into Chip Reader

Merchants are encouraged to:

- Insert the card into the chip-reading device. If the card is swiped first, the terminal will read the service code and display a prompt to insert the card into the chip-reading device.

- Follow the picture or diagram displayed on the terminal screen that shows which way the chip should face.
- Make sure the card is inserted in the chip-reading device until instructed to remove the card by the chip-reading device.
- The card should not be swiped unless instructed to do so on the terminal screen (!!)
- Follow the instructions on the terminal screen. The chip-reading device compares the applications it supports to the applications available on the card, then displays instructions on how to proceed.

If the Terminal Cannot Read the Chip

If the chip-reading device cannot read the chip on the card, you should follow "fallback" acceptance procedures. If the chip cannot be read, the terminal should first fallback to magnetic stripe, only if the magnetic stripe cannot be read should key entered take place. Key entered transactions should be the last option. Because the fallback transaction is swiped or key entered, a signature will be required as the option to capture PIN will be bypassed. Ensure that all staff are trained to follow the prompts on the terminal to avoid higher levels of key-entered transactions. The liability shift does not impact key entered rules as the counterfeit liability remains with the party that has not invested in chip technology.

Swiping the Stripe for Magstripe Cards Only

On the back of every card, you'll find a magnetic stripe. It contains the cardholder's name, card account number, and expiration date, as well as special security information designed to help detect counterfeit cards. When the magnetic stripe is swiped through the terminal, this information is electronically read and relayed to the card issuer, who then uses it as crucial input for the authorization decision.

If a Card Won't Read When Swiped for Magstripe Cards Only

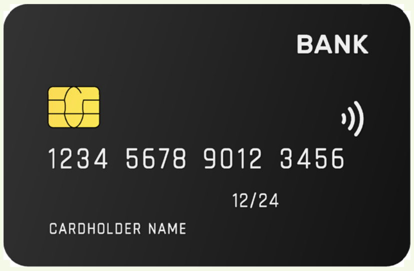
In some instances, when you swipe a card, the terminal will not be able to read the magnetic-stripe or perform an authorization. When this occurs, it usually means one of four things:

- The terminal's magnetic-stripe reader is not working properly, or there is a power outage.
- The card is not being swiped through the reader correctly.
- You may have a counterfeit or altered payment card.

- The magnetic stripe on the card has been damaged or demagnetized. Damage to the card may happen accidentally, but it may also be a sign that the card is counterfeit or has been altered.
- If a card won't read when swiped, you should:
- Check the terminal to make sure that it is working properly and that you are swiping the card correctly.
- If the terminal is okay, look at the card's security features (Annex A) to make sure the card is not a counterfeit or has not been altered in any way.
- If the problem appears to be with the magnetic stripe, follow your merchant store procedures.
- For key-entered transactions, make an imprint of the front of the card (embossed cards ONLY). The imprint proves the card was present at the point-of-sale and can protect your business from potential disputes if the transaction turns out to be fraudulent. The imprint can be made either on the sales receipt generated by the terminal or on a separate manual sales receipt form signed by the customer.
  - Embossed Cards - The cardholder name, card number and expiration date are printed or stamped on the face of the card creating a high rise impression on the face of the card.

0000 0001 2345 6789
00 00/00 00/00
MR.GENERIC CARDHOLDER

- If an unembossed card contactless feature does not work, the chip cannot be read, and the magstripe will not swipe, you should ask for another form of payment. Do not manually key enter unembossed cards or write the account number on a paper draft. A marked paper draft will not protect a merchant against disputes.
  - Unembossed Cards - The cardholder name, card number, expiration date, Card Verification Value (3-digit code) are thermal or laser printed on the card creating a smooth and flat surface.



Obtain an Authorization

The authorization process allows the card issuer to approve or decline a transaction. In most cases, authorizations are processed electronically in a matter of moments. However, to protect against fraud, the card issuer may request additional information about the transaction.

- An approved transaction does not guarantee payment; it simply means that the card has not been reported lost or stolen and that there are sufficient funds available at the time of the authorized transaction.
- Never accept a card when the POS displays "Declined or Do Not Honor"

Messages displayed on POS Authorization Responses

During the authorization process, your sales associates should receive one of the following responses.

Response	Meaning
Approved	Card issuer approves the transaction. This is the most common response.
Declined or Do Not Honor	Card issuer does not approve the transaction. The transaction should not be completed. Return the card and instruct the cardholder to call the card issuer for more information on the status of the account.
Pick Up	Card issuer wants to recover the card. Do not complete the transaction. Inform the customer that you have been instructed to keep the card and ask for an alternative form of payment. If you feel uncomfortable, simply return the card to the cardholder.
Insufficient Funds	Card does not have sufficient funds to cover the transaction.

While the transaction is being processed, check the card's features and security elements, if possible. Make sure the card is valid and has not been altered in any way. Refer to Card Security Features on Annex A.

Print a copy or transmit an electronic receipt to the cardholder.

- The final step in the card acceptance process for transactions is to verify the PIN, cardholder's signature once the signature panel feature is on the card, or other methods as required in the Card Association Rules. The card brands support a range of cardholder verification methods including signature and PIN.

Signature – Verify that the signature on the card signature panel matches the signature on the Transaction Receipt and on any identification requested and presented. For suspicious or non-matching signatures, adhere to your merchant store procedures. Match the name and last four digits of the account number on the card to those printed on the receipt.

- Note: The card brands are updating their card designs and the signature panel on the card is now optional.
- Signature will only be required if the card does not request for pin validation.
- Signature will not be required for contactless transactions that is BZ$100/US$50 or less. (This limit is the current card brand mandated limit for our country)

PIN – Verification using an acceptance device with electronic capability accepts a cardholder's PIN rather than a signature. The merchant must not ask the cardholder to reveal the PIN.

- Note: A signature is not required for PIN verified transactions. The sales draft will not contain a signature line and merchants should not request a signature from the cardholder.

When a Signature is Not Present

When a transaction is PIN verified, the card brand best practice is not to print a signature line on the receipt. Merchants need to be aware that they should not request a signature from the cardholder when a signature line is not present on the receipt.

Unsigned Cards

When a transaction is PIN verified, the card brand best practice is not to print a signature line on the receipt. Merchants need to be aware that they should not request a signature from the cardholder when a signature line is not present on the receipt.

Cards with a Signature Panel

While verifying the card security features, you should also ensure that the card is signed if the card contains a signature panel. An unsigned card is considered invalid and should not be accepted. If a customer gives you an unsigned card, The following steps must be taken if a customer presents an unsigned card:

- Check the cardholder's ID. Ask the cardholder for some form of official government identification, such as a driver's license or passport.
- Ask the customer to sign the card. The card should be signed within your full view, and the signature checked against the customer's signature on the ID. A refusal to sign means the card is still invalid and cannot be accepted.

Cards without a Signature Panel

While reviewing the card security features of a card, it will be noted that newer card designs may no longer contain a signature panel on the card. The cardbrands have made this an optional card feature mandate. Merchants should proceed to verify all other card security features on the card.

- "See ID" - Some customers write "See ID" or "Ask for ID" in the signature panel, thinking that this is a deterrent against fraud or forgery; that is, if their signature is not on the card, a fraudster will not be able to forge it.
- Criminals often don't take the time to practice signatures. They use cards as quickly as possible after a theft and prior to the accounts being blocked. They are counting on you not to look at the back of the card and compare signatures; they may even have access to counterfeit identification with a signature in their own handwriting.

In this situation, follow recommended steps listed above under Unsigned Cards.

Requesting Cardholder ID

A merchant may request cardholder identification as a condition of purchase. It is important that merchants understand that the requesting of a cardholder ID does not change the merchant's liability for disputes.

❗ If you suspect fraud, adhere to your merchant store procedures, and respond accordingly.

Card Not Present Transactions

A card not present transaction is when a credit card isn't physically presented to the merchant at the time of check out. The card magnetic stripe wasn't swiped, a chip card wasn't inserted into the card reader, and the card wasn't tapped for contactless payment on a point-of-sale terminal.

Recommendations for Card Not Present Transaction On POS Terminal

- Obtain complete and signed Credit Card Authorization Form. It should include the following:
  - Cardholder Name
  - Card Number
  - Expiration Date
  - Address
  - Issuing Bank Name
  - Description Of Service/Good sold.
  - Amount in processing currency of POS terminal
  - Merchant refund and or cancellation policy (cardholder should sign acknowledging terms)
  - Cardholder signature

- Obtain an authorization/approval code.
- Look for general warning signs of fraud.
  - Contact our Merchant Development Officer to report suspicious activity (please refer to Annex B for details).
- For embossed cards, obtain a manual card imprint of the card when card is presented (Hotels, Car Rentals, Tour Operators)at the time of check-in to support the original key entered transaction.
  - This will provide support that the cardholder and card was present at the merchant location.
- For unembossed cards, do not manually key enter unembossed cards or write the account number on a paper draft.

Recommendations for Card Not Present Transaction for MO/TO and Ecommerce Processing

The growth of the mail order, telephone order (MO/TO), and Internet markets means increasing numbers of merchants are now processing transactions in situations where the card and cardholder are not present, and fraud may be more difficult to detect. MO/ TO and E-commerce merchants should strongly consider developing in-house fraud control policies and providing appropriate training for their employees.

- The card acceptance procedures for these transactions are different from procedures for card-present transactions but must still allow merchants to verify—to the greatest extent possible—the cardholder's identity and the validity of the purchase.
- For card not present transactions, SECURITY should be top priority.
- Authorization is required on ALL card-not present transactions and should occur before any merchandise is shipped or service performed.
- Ecommerce Merchants should ask for:
  - Cardholder Name
  - Card Number
  - Expiration Date
  - Billing Address

- Contact information
- Card Verification Value 2 (CVV). The CVV2 is a 3-digit security number printed on the back of the card to help validate that a customer is in possession of a legitimate card at the time of an order.

POS & Ecommerce

Best Acceptance Practices

Merchants must follow basic card acceptance rules for all card transactions. Careful and consistent adherence to the Card Rules outlined in this section will help you to enhance customer satisfaction and operate your business efficiently.

- Accept all Valid branded cards (Amex, MasterCard, Visa) presented for use.
    - Do not discriminate against or discourage the use of any card in favor of a competing card brand.
- Authorization Code/Number should be obtained for all card and card not present transactions.
- Verify the security features of the card brand presented for payment. Annex A
- If the POS terminal requires a PIN, ensure that the cardholder enters the PIN.
    - Do not key enter card present transaction if cardholder cannot remember PIN or PIN cannot be validated.
- If the POS receipt requires a signature, ensure that the cardholder signs the slip.
- Do not slip or double charge the customer's card.
    - Merchants should only process transactions once on their POS terminals for the entire amount of the charge. Do not encourage split transactions especially for manual key entered transactions.
        - Fraudsters would instruct merchants to split transactions in small amounts and for the merchant not to charge the entire transaction amount at once so as to avoid any parameter rule that may be in place by the cardholder's bank..
    - Only process split transactions when prompted by the POS terminal.

    - Partial authorization will support only card present transactions and on multiple cards if the cardholder has another card to present. The cardholder may also make the difference in owning via another payment method.
    - The Partial Authorization feature will be available to all terminals by March 2024. Partial Authorization is explained below in section”POS changes for 2023/2024”.
- Do not re-attempt transactions once a Declined or Do Not Honor message is received on POS terminals.
    - The merchant should ask for another form of payment.
- Never Honor a card when:
    - The cardholder does not have the actual bankcard at the time of the transaction.
    - The card appears to have been altered or tampered with.
    - The card does not belong to the person conducting the transaction.
    - The transaction is declined, or the terminal indicates that cards are lost/stolen.
    - When signature line is present and the signatures on the card do not match.
- **Do Not impose minimum or maximum dollar amounts as a condition of honoring a card transaction.**
- **Do Not impose a Surcharge.**
    - Surcharges are not permitted in our Latin and Caribbean (LAC) region.
    - Transactions can be disputed.
- **Merchants should Not take pictures of or scan a cardholder’s card for record retention.**
- Never use a card for illegal purposes. In addition, merchants must never use a card account number to refinance existing debts or as a payment for a debt deemed as uncollectible (i.e., recover funds for a dishonored check).
- Merchants should only process transactions for your own business. Merchants owning multiple businesses should have a merchant facility for each registered business.
    - Processing transactions on behalf of another merchant is called laundering or factoring and this is not allowed.
    - Merchants will need to accept any chargeback dispute once a transaction is processed on behalf of another business.
- Do Not list cardholder’s personal information on the sales slip.

- Notify the cardholder how the transaction will be reflected on their bank statement (if the merchant's name differs from the Doing Business Name of the merchant location).
- Provide cardholders with a direct contact (customer service phone number and/or email addresses) to proactively resolve billing disputes/inquiries.
- Disclosure of Refund Policy
    - As a merchant, you are responsible for establishing your merchandise return and policies. Clear disclosure of these policies can help you avoid misunderstandings and potential cardholder disputes. The card brands will support your policies, provided they are clearly disclosed to cardholders. (Merchants should ensure not set unreasonable expectations)
    - If your merchant business has a refund policy, it should be disclosed to the cardholder at the time of the transaction. It should be pre-printed near the signature line of the transaction receipt. We can include the refund policy on the POS receipt.
    - **Refunds are to be issued to the same card that was used in the original transaction.**
    - Do not give cash refunds for returned goods. Refunds should be always processed to the same payment method which was used for the original transaction.
    - Do not do refunds via wire transfers
    - If the disclosure is on the back of the transaction receipt or in a separate contract, it must be accompanied by a space for the cardholder's signature or initials.
- Disclosure of Cancellation Policy (Hotels, Tour Operators, Car Rentals)
- As a merchant, you are responsible for establishing your cancellation policies. Clear disclosure of these policies can help you avoid misunderstandings and potential cardholder disputes. The card brands will support your policies, provided they are clearly disclosed to cardholders. (Merchants should ensure not set unreasonable expectations)
    - The merchant should disclose their cancellation policy at the time of the transaction. If the cardholder is required to complete an authorization form, the cardholder should initial or sign agreeing to the merchant cancellation policy.
    - For MO/TO or Ecommerce transactions, policies may be mailed, emailed, or texted to the cardholder but the merchant must prove that the cardholder received or acknowledged the policy for the disclosure to be proper.
        - Recommendation is for merchants to have a click to accept or acknowledgment button,

checkbox, or location for an electronic signature and have the data saved for record keeping. Terms can also be sent to the cardholder.

  - The disclosure must not be solely on a link to a separate web page.
- Delivery of Good and Services
  - Deliver the merchandise or services to the cardholder at the time of the transaction. For card-absent transactions, cardholders should be informed of delivery methods and tentative delivery date. **Transactions cannot be settled/deposited until goods have been shipped or services received.**
- Daily POS Settlement
  - Transactions should be settled daily. The card association's new mandate effective October 1, 2023 will be that a transaction should be settled with the card association in 3 business days.
  - Transactions not settled within the mandated business days by the card brands can be disputed for late presentment.
  - Merchant accounts are credited the following business day once transactions are settled prior to the end of the day processing cut-off time.
    - Monday to Friday cutoff time is 4:00 PM
    - Sundays or holidays cutoff time is midday.
    - Daily merchant statements can be viewed from the Belize Bank Limited online banking via www.belizebank.com or mobile app for easy reconciliation.
- Record Retention
  - All merchant slips should be kept for a minimum of 18 months.
  - Slips are to be kept safe in a cool location (some merchants take scan them to ensure that they remain legible in the digital format)
  - All customer account information should be kept confidential and should only be provided to your bank officer or merchant officer in the event of a query or dispute.
  - All records should be destroyed when they are no longer needed for business or legal reasons.

Useful Tips to Protect Your Business

- Beware of persons posing as processors, American Express, MasterCard or Visa representatives.
- Do not divulge cardholder account information over the telephone or to someone you are not familiar with.
- If you receive a suspicious call, ask the caller for information such as name, telephone number, or email. Tell the caller that you do not have the information readily available and will get it back to them.
- Report the call to the Bank immediately.
- Keep your POS terminal and imprinter in a secure place.
- Only your staff members that perform transactions should have access to the POS terminal and card imprinter.
- Only Belize Bank Limited Merchant Development Officers (Annex B)should perform servicing to Belize Bank Limited equipment.
- Advise the bank if you close or sell your business and return any equipment, imprinter and stationery to the Bank.

Ecommerce Merchant Website Requirements

As your bank, we recommend that you include certain content or features on your website. These elements may be intended to promote ease of use for online shoppers and reduce cardholder disputes and potential disputes.

1. Complete description of goods and services.
    a. The global market increases opportunities for unintended misunderstandings or miscommunications. For example, if you sell electrical goods, be sure to state voltage requirements, which vary around the world.
2. Complete description of goods and services.
    a. The global market increases opportunities for unintended misunderstandings or miscommunications. For example, if you sell electrical goods, be sure to state voltage requirements, which vary around the world.
3. Customer service contact information includes an email address and/or phone number.
    a. Online communication may not always be the most time-efficient or user-friendly communication method for some customers. Including a customer service telephone number as well as an email address and more and more popular chatbots, promotes customer satisfaction.
4. Full Disclosure of Return, refund, and cancellation policy.
    a. Merchants should have a check box or a button where all cardholders have to agree to the terms and conditions prior to proceeding with the transaction.
    b. The merchant's back end should register/log the date and time stamp when the cardholder agrees to the terms and conditions.

[2] Merchant Development Officer (MDO) - Belize Bank Limited has personnel assigned to your area to provide merchant terminal support and servicing. Contact information for the assigned MDO can be found in the **Contact Information** section of this training manual guide.

5. Delivery policy
    a. Merchants set their own policies about delivery of goods, that is, if they have any geographic or other restrictions on where or under what circumstances they provide delivery. Any restrictions on delivery must be clearly stated on the website.
        i. Country of origin. The merchant must prominently display the merchant location country on the checkout page or a page leading up to it. You must also disclose the address for cardholder correspondence.
        ii. Export restrictions (if known)
6. Confirmation Email of Goods or Services
    a. Merchant websites should send cardholders a confirmation email of goods or services bought along with their business disclosure.

Best Practices for Websites

Suggested best practices for merchant website information include:

1. Privacy statements.
2. Information on when cards are charged. The merchant should not bill the customer until merchandise has been shipped.
3. Order fulfillment information. Indicate time frames for order processing and send an email confirmation and order summary within one business day of the original order. Provide up-to-date stock information if an item is backordered.
4. A statement on a website regarding security controls used to protect customer's personal information or data.
5. A statement encouraging cardholders to retain a copy of the transaction receipt.

Additional Fraud Prevention for Belize Bank Ecommerce Facility

The Belize Bank Limited E-commerce Facility now has an extra layer of security. The bank has added the Verified by Visa/3D secure authentication protocol, which gives our merchants greater protection on E-commerce transactions.

Benefits of Verified by Visa/3D Secure Authentication for Merchants

- **Lower Risk of Fraud:** By requesting additional customer information, merchants can reduce the risk of fraudulent transactions.
- **Liability Shift:** As mentioned, some card issuers may offer liability shifts if a fraudulent transaction occurs while using 3D Secure Authentication. This means the card issuer would be responsible for any losses instead of the merchant.
- **Improved Customer Experience:** With improved security measures, customers will feel more secure making purchases from your business. This can result in increased customer satisfaction and loyalty.
- **Improved Brand Reputation:** As customers become savvier to online security measures, they're more likely to do business with companies that use 3D Secure Authentication.

Integration of Belize Bank Limited E-commerce

Digital Transactions Processing

Full API Integration **Recommended**

Via this feature, we will allow our merchants to be similar to Amazon and other websites around the world, where a cardholder can browse on a merchant's website, find a product or service they wish to purchase, and immediately perform payment via their credit or debit card.

The Bank is making this feature be available via the hosted payment page concept. This means the merchant will never need to concern itself with being PCI DSS compliant, storing any sensitive card information, or processing the card transaction at any time. The merchant's website or app will simply need to direct the customer to our system when they are ready to perform payment, and we will in turn direct the customer back to the merchant's system when payment has been processed.

Pay by link

Via this feature the merchant can email or share a payment link to a customer, the payment link will be just like any other link to any website. The cardholder upon receiving this link, will click on the link, and they will be directed to a page, where they will enter their card details and click pay and immediate payment would have been performed. The merchant can use this option immediately after signup, and does not need to have his system connected to ours to use this feature.

Card acceptance via Customer Support

Via this feature, the merchant will be able to obtain the card details of their customer over the phone and process the payment using a portal that will be available to the merchant. The merchant can use this option immediately after signup, and does not need to have his system connected to ours to use this feature.

E-commerce Docs

SCAN ME!

View Now

Account Information Security

Because of media reports of hacker incidents, stolen cards and identity theft, consumers are increasingly concerned about information security. Due to this the Card Associations implemented Payment Card Industry (PCI) Data Security Standard (PCI DSS). PCI DSS ensures that merchants and their service providers maintain a high information security standard. It offers a baseline approach to safeguarding sensitive data for all card brands.

What is the PCI DSS?

PCI DSS is a comprehensive set of international security requirements to help protect cardholder data. The PCI DSS was developed by the card brands of the PCI Security Standards Council to help facilitate the broad adoption of consistent data security measures on a global basis.

All acquirers and card issuers must comply and must also ensure the compliance of their merchants and service providers who store, process, or transmit card account numbers. This program applies to all payment channels including card-present, mail/telephone order, and eCommerce.
Separate from the mandate to comply with PCI DSS is the validation of compliance which identifies vulnerabilities and helps ensure that appropriate levels of cardholder information security are maintained.

We highlight below the 12 PCI DSS requirements:

Build and Maintain a secure network

1. Requirement 1: Install and maintain a firewall configuration to protect data
2. Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

3. Requirement 3: Protect stored data
4. Requirement 4: Encrypt transmission of cardholder data and sensitive information across public networks

Maintain a Vulnerability Management Program

5. Requirement 5: Use and regularly update anti-virus software
6. Requirement 6: Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7. Requirement 7: Restrict access to data by business need-to-know
8. Requirement 8: Assign a unique ID to each person with computer access
9. Requirement 9: Restrict physical access to cardholder data

Regularly monitor and Test Networks

10. Requirement 10: Track and monitor all access to network resources and cardholder data
11. Requirement 11: Regularly test security systems and processes.

Maintain an Information Security Policy

12. Requirement 12: Maintain a policy that addresses information security.

What your Bank does for you to secure your business and customers

- Build Consumer Trust in the Security of Sensitive Information. Customers seek out merchants that they feel are "safe." Confident consumers are loyal customers. They come back again and again, as well as share their experience with others.
- Minimize Direct Losses and Associated Operating Expenses.
- Appropriate data security helps protect cardholders, limit risk exposure, and minimize the losses and operational expenses that stem from compromised cardholder information.
- Maintaining Positive Image Information security is on everyone's mind…including the media. Data loss or compromise not only hurts customers, it can seriously damage a business's reputation.

E-kyash

Physical & Digital Processing

E-kyash Overview

Our E-kyash digital wallet solution, launched in 2021, brings new levels of payment efficiency to all Belizeans business owners and their consumers. It revolutionizes payment processing by offering a faster, more secure, and technologically advanced means of conducting transactions compared to traditional physical methods. As at the end of September 2023, there were 33.5K individual users and almost 2,000 merchants enrolled countrywide.

Some of the benefits and features of E-kyash includes:

- Convenient, fast and efficient purchases using QR (Quick Response) codes
- Secure payment option for merchants with significantly lower costs
- Safe cashless transactions reducing the risk of robbery
- Electronic Gift Certification for a special occasion
- Instant transactions with minimum cost to customers

- Seamless Bill payments
- Real Time processing of Temporary work permits application fees
- Innovation phone top ups (SMART)
- Instant salary payment directly to E-kyash wallet

E-kyash has a dedicated website (www.e-kyash.com) with detailed information about the convenience of E-kyash and how to use it.

Tutorials for your individual customers can be found at:
https://www.e-kyash.com/how-to-use-e-kyash/

While tutorials for our Business customers can be found at:
https://www.e-kyash.com/tutorials-business/

E-kyash for Business

We want you to be successful and grow your revenue stream and be safe in doing so. With our digital wallet solution, safety is our priority.

Merchant Wallet

Compliments the Individual wallet by allowing consumers to purchase goods and services using electronic funds. Customers can pay you digitally by scanning a QR code or via a link that you can send at any time from your device.

Money collected on your digital wallet can then be transferred daily to your bank account so that you can avoid standing in the long lines to deposit your daily turnover.

Retail Operator

Merchants also have the option of being a Retail Operator. For each top-up and cash-out processed for individual users, we will pay you a commission. In the application, you can easily view the number of processed top-ups, cash-outs, and commission earned at any point in time.

- Cash-in - the business is able to transfer digital funds to a customer's E-Kyash wallet in exchange for physical cash. (Top-UP the E-Kyash wallet)
- Cash-out – the business is able to take out digital funds from the customer's E-Kyash wallet and pay out physical cash to the customer. (Withdraw from the E-Kyash wallet)

Commission

Cash In - Per Transaction (Commission earned by RO) - 0.25

Cash Out - Per Transaction (Commission earned by RO) - 1.00

E-kyash API Integration

E-kyash's newest feature is its third party merchant API integration which offers a modern and streamlined alternative to traditional physical payment processing methods. Unlike physical processing, which often requires physical cards or cash, E-kyash APIs enable seamless, contactless transactions through smartphones or other digital devices. This not only enhances convenience for our customers but also provides businesses with real-time transaction data, simplifying accounting and reducing the risk of errors associated with manual handling. Moreover, E-kaysh APIs have robust security features incorporated, making it more secure than traditional physical transactions.

Benefits of the E-kyash API integration include:

1. The creation of a seamless user experience because the integrators can now offer E-kyash as a form of payment whenever their clients want to make payments for goods or services
2. The APIs are flexible and allow for integration with both Websites and Mobile Apps.
3. The APIs and the data being exchanged is secure
4. The APIs offer extensive capabilities such as voidances, refunds and robust reconciliation capabilities

Getting Started

1. Sign E-kyash merchant agreement
2. Download the business app from your app store
3. Register and sign into business app using OTP that was sent via SMS
4. In the app, invite your staff members. All members will be given a staff role
5. Go to the business portal to assign roles to accepted staff members
6. Open branches if you operate more than one locations
7. If you wish to start issuing digital gift certificates, provide the following information to your SME Officer or Sales and Business Development Officer:
8. For Retail Operators only: Transfer funds to your wallet and be ready to transact with your customers

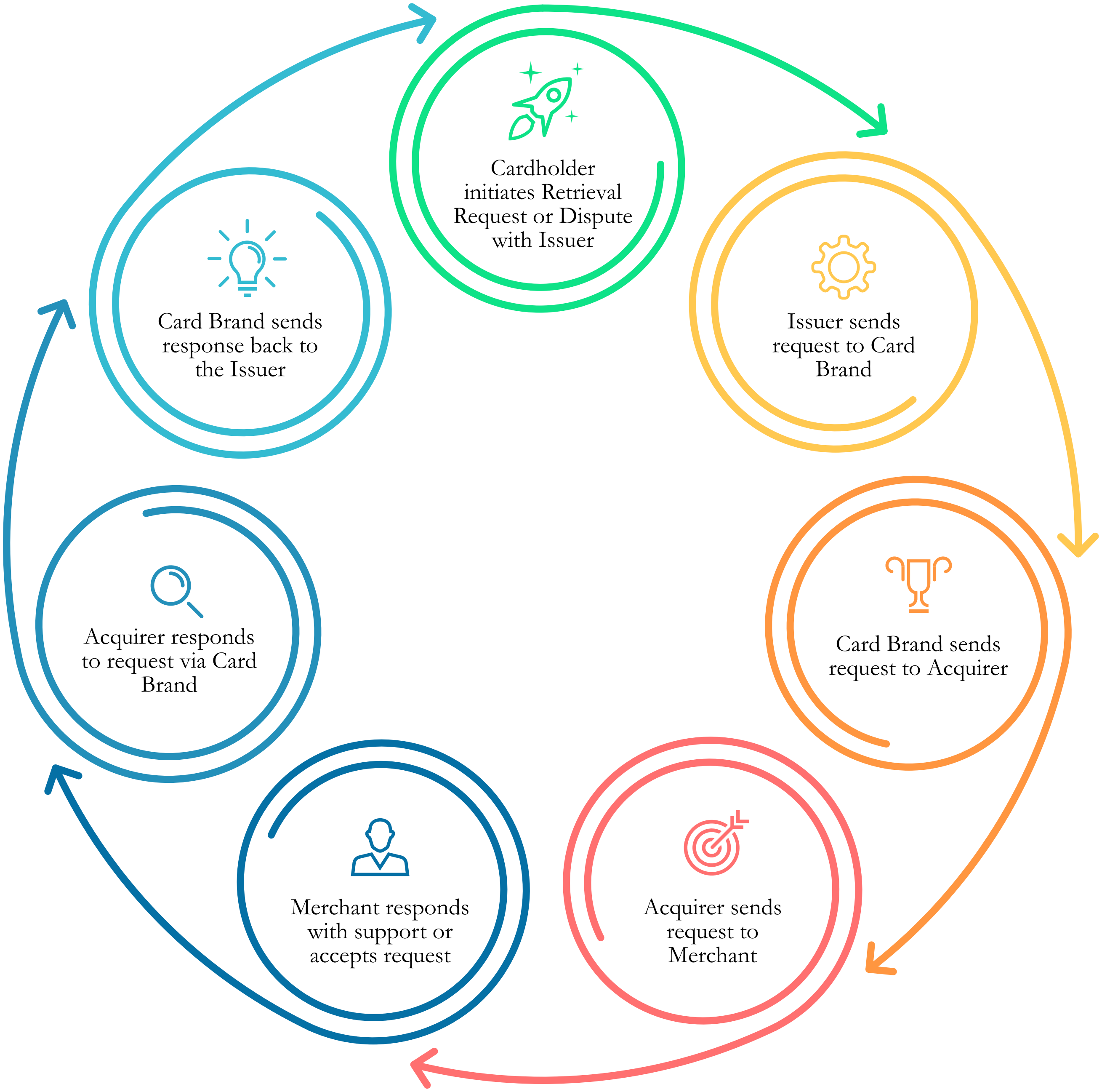
You can also let us know if you would like to register for E-kyash gift certificates or partner with us for any special promotion your business may have. We would be happy to include your promotion in the promo section of the E-kyash App and promote it on our social media platforms FREE of charge.

When posting the promotions on your social media platforms please tag E-kyash and Belize Bank on Tiktok: @belizebank, Instagram: @belize_bank, Facebook: @TheBelizeBankLimited

Disputes

What is a Dispute?

A dispute is a settled transaction or transactions that are returned by the Issuer (Cardholder) to the Acquirer (Merchant). The return may be for the entire settlement or partial settlement.


Cardholder initiates Retrieval Request or Dispute with Issuer
Issuer sends request to Card Brand
Card Brand sends request to Acquirer
Acquirer sends request to Merchant
Merchant responds with support or accepts request
Acquirer responds to request via Card Brand
Card Brand sends response back to the Issuer

Stages of the Dispute Process and the meaning

Retrieval Request	The request for original sales slip and invoice.
Chargeback	The Issuer initiates to move financial liability from itself to an Acquirer on a previously submitted transaction
Representment	This is the process by which the Merchant can respond to the chargeback. The goal of representment is to prove that the charge in question is legitimate and therefore should not be reversed.
Pre Arbitration	This stage occurs when a Cardholder disputes a transaction for a second time with new evidence after the chargeback is reversed.
Arbitration	This is the last stage of the dispute process. It means the parties involved—the Banks, Cardholder, and the Merchant, cannot resolve the dispute. The Card Brand's Arbitration Committee will review the evidence and make a final decision on who is financially responsible. This decision is final and can't be appealed.
Pre-compliance	The process through which the Issuer challenges a case involving a rule violation, and specific reason code be used to initiate a dispute.
Compliance	The Card Brand's Compliance Committee will review the evidence and make a final decision on who is financially responsible. This decision is final and can't be appealed.
Good Faith	An exchange between the Cardholder and the Merchant, where one participant contacts the other requesting the exchange of full or partial funds. This is normally initiated when no chargeback rights are available.

Dispute Reason Codes

What is a Reason Code?

A reason code is a 2-to-4-digit alphanumeric code provided by the issuing bank involved in a chargeback, which is meant to identify the reason for the dispute. Each of the major card brands has their own system of reason codes. Reason codes are important to help merchants address recurring chargeback triggers, as well as identify frivolous chargebacks, against which the merchant will need to fight back.

Reason Codes by Card Brand

American Express	Mastercard	Visa
• Incorrect Transaction Amount or Primary Account Number • Multiple Processing • Credit Not Presented • Paid Through Other Means • Request for Support Not Fulfilled • Request for Support Illegible/Incomplete • Invalid Authorization • Missing Imprint • Currency Discrepancy • Multiple ROCs • Late Presentment • Card Not Presentment • Cancellation of Recurring Goods/Services • Not as Described or Defective Merchandise • Good and Services Not Received • Car Rental Charge Non-Qualified or Unsubstantiated • No Valid Authorization	• Required Authorization Not Obtained • Multiple Authorization Requests • Goods or Services were Not as Described or Defective • Goods or Services Not Provided • Credit Not Processed • Counterfeit Goods • Cardholder Dispute of a Recurring Transaction • Addendum Dispute ◦ "No Show" Hotel Charge ◦ Transaction Did Not Complete ◦ Timeshares • No Cardholder Authorization • Cardholder Debited More than Once for the Same Goods or Services • Transaction Amount Differs • Charges for Loss, Theft or Damages • Late Presentment • Currency Errors*	• Other Fraud Card Present Environment • Other Fraud Card Present Environment • Declined Authorization • No Authorization • Late Presentment • Incorrect Account Number • Incorrect Amount • Duplicate Processing • Paid By Other Means • Merchandise/Services Not Received • Cancelled Recurring Transaction • Not as Described or Defective Merchandise/Service • Counterfeit Merchandise • Misrepresentation • Credit not Processed • Cancelled Merchandise/ Services

Timeframes to respond to a dispute

A Cardholder has 120 calendar days from the transaction date to initiate a dispute. If the goods or services are future dated the dispute time starts on the day the goods or services would have been issued.

The Merchant has 7 business days to respond to the case. There may be times when the response period is less than 7 business days. This is dependent on the stage of dispute.
Cardholders have 45 calendar days to respond and initiate the next stage of the dispute

Arbitration cases don't have a timeframe on when the final decision is made. This is solely dependent on when the Arbitration Committee issues its decision.

Best Practices on handling and responding to disputes

Retrieval Request

A. Common reasons for a Retrieval Request

i. The customer doesn't recognize or remember making a purchase

ii. The amount on the statement doesn't match the agreed-upon transaction amount.

iii. The customer doesn't recognize transaction details appearing on the statement.

B. Responding to Retrieval Request

i. Respond within the given timeframe

ii. Provide legible documents (Sales Slips/Invoice/Refund Slip)

C. Minimizing Retrieval Request

i. Make Sure Customers Can Recognize Your Name on Their Bills

ii. Make Sure Your Business Name Is Legible on Receipts

iii. Train Sales Staff

iv. Avoid Illegible Transaction Receipt

Disputes

A. Common reasons for a Dispute

i. Merchant didn't provide goods/services in a timely fashion

ii. The goods were damaged, defective, or missing parts

iii. The cardholder was charged an incorrect amount

iv. The buyer used stolen cardholder information

v. The customer regrets their purchase

vi. The cardholder's family member made the purchase

vii. The buyer wants to end a subscription

viii. The product description was inaccurate

ix. The buyer is trying to get something for free

B. Best Acceptance Practices for Responding to most common Disputes

i. Fraud – Card Present

- Provide a copy of the sales slips as proof the card was chip read or tapped at the POS.
- A manual imprint was obtained at the time of sale.
- A refund has been processed
- Cardholder no longer disputes the transaction (provide an email or letter form customer)

ii. Fraud – Card Absent

- Proof a refund has been processed
- Proof Cardholder no longer disputes the transaction (provide an email or letter form customer)
- Provide evidence, such as photographs or emails, to prove a link between the person receiving the merchandise or services and the Cardholder.
- Provide evidence to prove that the Cardholder disputing the transactions in possession of the merchandise and/or is using the merchandise or services.
- If the merchandise was picked up from merchant location provide proof of the Cardholder signature on the pickup form, copy of identification presented or details of the identification presented by the Cardholder
- Evidence that the Transaction was completed by a member of the Cardholder's household or Family

- Evidence of one or more non-disputed payments for merchandise or service
- T&E Transaction, evidence that the services were provided and either:
    - Details of loyalty program rewards earned and/or redeemed
    - Address and telephone number that establish a link to the Cardholder
    - Evidence that an additional Transaction or Transactions related to the original Transaction, such as the purchase of upgrades or subsequent purchases not disputed

iii. No Authorization

- Evidence an authorization was obtained
- Proof a refund has been processed
- Proof Cardholder no longer disputes the transaction (provide an email or letter form customer)

iv. Late Presentment

- Provide evidence transaction was processed within the required timeframe
- Proof a refund has been processed
- Proof Cardholder no longer disputes the transaction (provide an email or letter form customer)

v. Incorrect Transaction Amount

- Provide a copy of the sales slip and itemized invoice
- Proof a refund has been processed
- Proof Cardholder no longer disputes the transaction (provide an email or letter form customer)

vi. Duplicate Processing

- Provide two sales slip and matching invoices
- Proof a refund has been processed
- Proof Cardholder no longer disputes the transaction (provide an email or letter form customer)

vii. Paid by Other Means

- Provide the sales records or other documentation that shows no other form of payment was used.
- Proof a refund has been processed

- Proof Cardholder no longer disputes the transaction (provide an email or letter form customer)

viii. Merchandise/Services not received

- Proof
  - Merchandise was delivered or made available on the agreed upon date
  - Specifies delivery has not passed
  - Cardholder cancelled prior to delivery date
  - Transaction represents a partial payment with balance due
- Proof a refund has been processed
- Proof Cardholder no longer disputes the transaction (provide an email or letter form customer)

ix. Merchandise/Services not received

- Provide specific information (invoice, contract, etc.) to refute the cardholder's claims.
- Proof returned merchandise was not received or services were not cancelled.
- Merchandise was replaced or repaired.
  - The cardholder agreed to repair or replacement
  - Repair or replacement was received
  - The repair replacement has not since been disputed
- Proof a refund has been processed
- Proof Cardholder no longer disputes the transaction (provide an email or letter form customer)

x. Counterfeit Merchandise

- Provide specific information and invoices to refute the cardholder's claims.
- Proof a refund has been processed
- Proof Cardholder no longer disputes the transaction (provide an email or letter form customer)

xi. Credit Not Processed

- Provide evidence sale is valid and Cardholder is not due a credit
- Proof a refund has been processed
- Proof Cardholder no longer disputes the transaction (provide an email or letter form

customer)

xii. Canceled Merchandise/Services

- You never received, or accepted, the returned merchandise.
- Proof policies were properly disclosed.
- Proof cardholder did not cancel according to your disclosed policy
- Proof Cardholder continued to use services
- Proof a refund has been processed
- Proof Cardholder no longer disputes the transaction (provide an email or letter form customer)

C. Best Acceptance Practises for Minimizing Disputes

i. Do not complete a transaction without obtaining an authorization.

ii. Do not complete a transaction if the authorization request was declined.

iii. Do not accept a card after its "Good Thru" or "Valid Thru" date.

iv. Key entered transactions - make an imprint of the front of the card on the transaction receipt, using a manual imprinter.

v. Ensure that the transaction information on the transaction receipt is complete, accurate, and legible before completing the sale.

vi. Card Present Transaction – Do not accept the transaction if the physical card is not present.

vii. Ensure that transactions are entered into point-of-sale terminals only once.

viii. Ensure that incorrect or duplicate transaction receipts are voided.

ix. Clear disclosure of refund/cancellation policies

x. Electronic refund/ cancellation policy must have a "click to accept" button, checkbox, or location for an electronic signature.

Physical refund/cancellation policy must have the customer's signature. If the policy has several pages, have the customer initial each page.

Card Fraud Prevention

Fraud is a real problem in any business. It's an additional risk for merchants who support card-not-present transactions.

- It's important to start fraud prevention early
- Make it a major part of new employee training because they are in the best position to have a significant effect on your company's fraud losses.
- Reinforce training (including your seasonal temporary employees), especially as holidays approach and fraud potential is at its peak.

POS Terminal CardFraud Prevention

A dispute is a settled transaction or transactions that are returned by the Issuer (Cardholder) to the Acquirer (Merchant). The return may be for the entire settlement or partial settlement.

We have two very sound fraud-fighting resources: **Technology & People.**

Technology - terminals have proven to be very effective in obtaining authorizations quickly and easily.

A terminal can tell you:

- whether a cardholder has the balance available
- whether their account has been blocked by the issuer.

A terminal cannot tell you:

- whether the card security features are irregular or missing
- whether the signatures match for cards that carry a signature panel
- terminals won't ever notice a customer acting suspicious.

People

- We've come to rely more on technology than on people to fight fraud.
- Criminals know this and are taking advantage of our reliance on these terminals.
- The reality is YOU are the first line of defense against fraud.
    - Staff are able to detect phishing or suspicious emails.

You can **STOP FRAUD** on cards that are not yet blocked in the authorization system.

Everyone who accepts cards from customers can make a tremendous difference in fighting fraud by following proper acceptance procedures and examining card security features.

YOUR staff is the front-line defense against card fraud. Alongside fraud prevention technologies. YOUR staff are incredibly important in the fight against card criminals. Your vigilance in Spotting and Stopping card fraud is essential.

Ecommerce CardFraud Prevention

A dispute is a settled transaction or transactions that are returned by the Issuer (Cardholder) to the Acquirer (Merchant). The return may be for the entire settlement or partial settlement.

Methods for Ecommerce Fraud Prevention

- **Detecting fraud patterns with Artificial intelligence (AI)/ machine learning (ML)** - helps merchants set baselines, track abnormal activity, and understand seasonal differences.
- **Integrate multiple data sources** - Integrating data from multiple sources can help merchants spot emerging issues earlier.
- **Monitor Security Posture** - Having a robust security posture can help mitigate risks. Some best practices for establishing and monitoring security include:
    - Checking your SSL certificate
    - Monitoring for malware
    - Maintaining backups
    - Scanning for vulnerabilities

- **Identify Risks** - certain IP addresses or geographic locations may be riskier than others because fraudsters use them more often. Merchants should have controls and monitoring to identify and mitigate these risks.
- **Install Updates in a Timely Manner** - Cybercriminals exploit known software and application vulnerabilities to steal data. Merchants should make sure to update the following as soon as possible:
  - CMS
  - Shopping-cart plugins
  - Website themes
- **Authenticate Users** - Since merchants can't see their customers, you need to use digital means, which includes multi-factor authentication (MFA). With MFA, merchants can mitigate account takeover risks because the person needs to answer a challenge question, like entering a security code before logging into the account.
- **Engage in Manual Review** - Even if merchants don't review every single order before fulfillment, merchants should make sure to do spot checks. Merchants may also want to review suspicious orders manually.
- **Use Hypertext Transfer Protocol Secure (HTTPS) for Data-in-Transit** - HTTPS is the protocol that sends data between a merchant online store and the customer's browser. With HTTPS, the merchant encrypts the data-in-transit to protect customer information like name, address, and payment card number.
- **Minimize Data Collection** - Preventing fraud is more than just protecting yourself. Merchants also need to ensure that cybercriminals can't use their website to steal data. Collecting only the data needed to complete the transaction will mitigate risk.
- **Set Purchase Limits** - Setting purchase limits mitigates risks associated with bots and card testing.

Fraud Warning Signs

Warning Signs of Fraud

Watch out for customers who:

1. Purchase a large amount of merchandise without regard to size, style, color, or price.
2. Ask no questions on major purchases.
3. Try to distract or rush you during the sale.
4. Make purchases and leave the store, but then return to make more purchases.
5. Make large purchases just after the store's opening, or as the store is closing.
6. Refuse free delivery for large items or are hesitant when requesting personal information.

If You See Signs That Make You Suspicious:

- Hold on to the customer's card if you think you can do so safely.
- Follow your company's procedures and notify your supervisor.
- Certain customer behavior could point to bankcard fraud.
- It doesn't necessarily indicate criminal activity—you know your customers, so let your instincts steer you in the right direction. Never risk your own safety or the safety of others in the vicinity.

If the Card is NOT There — You Need to be MORE Aware:

Report all suspicious activity to your bank.

To stay ahead of the crooks and reduce your fraud exposure:

- Ask the customer for the card's expiration date and include it in your authorization request. An invalid or missing expiration date can be an indicator that the person on the other end does not have the actual card in hand.

- Be on the lookout for questionable transaction data or other signs indicating "out of pattern" orders.
- Develop, introduce, and perform fraud screen program to suspend processing of E-commerce and MO/TO transactions if:
    - Matches data stored in your internal negative files.
    - Exceeds velocity limits and controls.
    - Generates a mismatch or no match for Card Verification Value 2 (CVV2) Code. The Code helps add an extra layer of security to online transactions, helping to prevent fraudulent transactions and protect cardholders.
    - Matches other high-risk attributes. For example, transactions associated with anonymous email addresses, high-risk shipping addresses or cards issued outside the country.

Card Network	Appearance	Number of Digits
American Express	Front of the card	4
Mastercard	Back of the card within the signature panel	3
Visa	Back of the card within the signature panel	3

Keep in mind. None of these by itself means you're being scammed—but several of them together might result in fraud.

Hotel, Tour Operators and Travel Agency Scams

Tips to identify Scam Emails:

- Often the scammer will be acting in an urgent manner and will be making bookings with short notice dates.
- They will also want long stays, a lot of rooms, or tours for a large number group. The scammer may be very vague about the actual number of guests. The reason is they want to get the booking charge high.
- They will show little or no regard for rates.

- They will be flexible on dates of arrival/ departure and the number of nights booked.
- They don't care about your location. They will express little or no interest in area attractions, nearby airports, or other facilities.
- The first e-mail you receive will likely not address your hotel specifically. It will be a general e-mail and may not even mention your town or city.
- The scammer's grammar, spelling and use of punctuation will be off.
- In some cases, the scammer will pretend to be a travel agency. Take note if the e-mail comes from a free e-mail service like Yahoo! or Hotmail. Legitimate travel agents rarely use free e-mail accounts.
- They will offer you a commission.
- They want you to send them cash, usually by wire and take note that they will ask for wire to be done via Western Union. This should be the Ultimate tip off!
- Scammers do not use their own real name. For the most part they use made up names and made up or wrong addresses. In some cases, they may assume the identity of another real legitimate person. They may also claim associations with well-known organizations.

Actions to Take:

- If you get one of these and it appears too good to be true, it probably is. If you feel it is a legit booking request, make sure you chat with them and ask about the attractions they plan to see in Belize. Ask them what airport they are flying to and who they are flying with.
- Check if they will be renting a car. However, it is probably best to just ignore them.
- Contact the bank to verify the authenticity of the transaction.

What to do if you are suspicious:

- Call your Merchant Development Officer or Relationship Banker. We can attempt to contact Issuing Bank to validate the transaction.

Be alert for transactions with several of these characteristics:

- First time customer – The risk of fraud is less when dealing with repeat customers.
- Orders that are larger than is normal for the Merchant.

- Orders consisting of several purchases of the same item.
- Orders consisting of high value purchases, such as jewelry or electronics goods.
- Transactions are made with cards that have similar account numbers.
- Orders are shipped to a single address but purchased with various cards.
- Multiple transactions on a single card over a very short period
- Multiple transactions are made with several cards with a single billing address, but multiple shipping addresses.
- Expedited shipping and lack of concern over color, size, etc. of the merchandise.

Benefits of Accepting Cards

- A merchant account is inexpensive, quick, and easy to set up. Reduces the risk and problems of bounced checks and robbery.
- A merchant account improves cash flow. Prompt payments into your bank account, reduce the cost of your financial arrangements.
- Increase in sales as it allows cardholders to spend more money at your business.
- Benefit of competition that does not accept cards as a medium of payment.
- Fast and seamless (automated) reconciliation.

Benefits of Displaying Decals

- The display of card brand decals helps customers identify the types of cards accepted at the merchant establishment.
- Provides a sense of trust and confidence to customers that they are able to use their card for payment.

- Customers prefer to pay with their cards rather than carrying cash.
- Increase customer buying power and can attract customers who prefer a specific card payment method.

Benefits of using Belize Bank POS Terminal

- Only bank that accepts the 3 major card brands (American Express, MasterCard, and Visa).
    - Payments for transactions available the next business day once POS transactions are settled prior to 4:00 P.M on weekdays and by midday on weekends or holidays.
- Merchant statements available via online banking for easy reconciliation
- Training on equipment use and card acceptance procedures.
- 24-hour merchant support

Benefits of Merchant Training

Cardholders expect and depend on accurate, efficient card processing when shopping at any location .

Your sales staff and customer service associates play a critical role in ensuring proper transaction processing. Ensuring that they receive regular and ongoing training in Card acceptance policies and procedures benefits everybody.

- Sales staff and customer service associates benefit because they are given the skills and knowledge they need to do their jobs accurately and confidently.
- You benefit because:
    - Customer service is enhanced, leading to increased sales.
    - You may have fewer fraudulent transactions, which reduces related losses.

    - You may have fewer transaction receipt copy requests and disputes, which reduces related expenses.
- It is important that your sales staff and customer service associates understand the proper card acceptance procedures, which are easy to learn and Belize Bank is here to help you.

POS Changes For 2023/2024

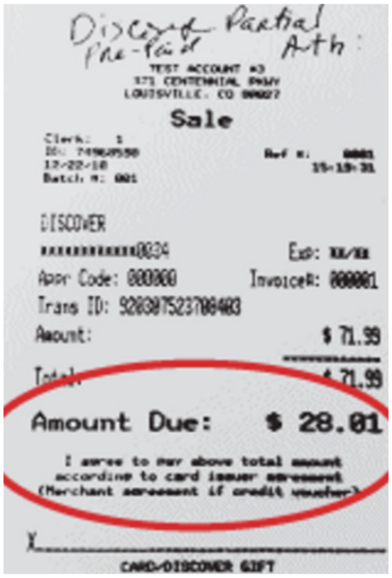
Partial Authorizations

What is a Partial Authorization?

A Partial Authorization enables participating merchants to receive an approval for a partial amount of a transaction (i.e., the amount available on the card) when the amount in the original authorization request exceeds the available card balance. The merchant may then request another form of payment (another card or cash) to cover the remaining transaction amount.

Benefits of Partial Authorization

- The issuer will not decline the transaction when the card account does not have sufficient funds to approve a transaction in full. The issuer will return an authorization response with an approval code for a portion of the original amount requested.
    - The Point-of-Sale terminal will prompt if they would like to proceed with another card transaction for the difference of the transaction.
        - If the cardholder presents cash the option chosen on the terminal should be **NO**.
        - If the cardholder presents another card, the option chosen



Discover Pre-Paid Partial Ath:

```
TEST ACCOUNT #3
371 CENTENNIAL PKWY
LOUISVILLE, CO 80027
Sale
Clerk:   1
ID: 749620550                    Ref #:   0001
12-22-10                               15:13:31
Batch #: 001

DISCOVER
************0034                 Exp: XX/XX
Appr Code: 000000            Invoice#: 000001
Trans ID: 920307523700403
Amount:                               $ 71.99
                                 ------------
Total:                                $ 71.99
Amount Due:                           $ 28.01
      I agree to pay above total amount
      according to card issuer agreement
    (Merchant agreement if credit voucher)

X____________________________________________
          CARD-DISCOVER GIFT
```

on the terminal should be **YES**.

- This feature will reduce the decline rate for insufficient funds.

Requirements undertaken by Belize Bank

- Belize Bank Limited's team is diligently working with its processors to perform test transactions and will be seeking certification with the card associations by the end of October 2023.
- Belize Bank Limited will enable this feature for all merchants.
- All terminals will require a configuration update.

Requirements for Merchants

- Partial authorization is only applicable to card present transactions.
- Merchants should ensure that they verify and collect the remaining balance from cardholders for partially approved transactions. The cardholder either pays via cash or another card medium.
    - For example, if a cardholder is unable to make payment for the difference of the partially approved transaction via cash or another card when purchasing a cell phone, the merchant should void the transaction.
- Merchants need to have a clear understanding of this process to maintain accurate records of all transactions.

Implementation Date

- Certification is to be completed by December 2023.
- All Belize Bank terminals will be updated by March 2024.

Online PIN Verification

What is Online PIN Verification?

Online PIN verification is when the PIN-encrypted data entered by the cardholder on the Point-of-Sale terminal is verified online by the card issuer. This means that when the POS terminal prompts for a PIN Number and the cardholder inserts his/her unique PIN on the POS terminal, the POS terminal will send that encrypted data to the card issuer. The card issuer will authenticate that the

PIN number corresponds to that in their system.

- Currently, all Belize Bank terminals authenticate PIN-requested transactions using the offline PIN validation method. This means that when the POS prompts the cardholder to enter his/ her PIN, the pin number is validated between the POS terminal and the chip on the card.

Benefits of Pin Online

- Convenient for both cardholders and merchants. Cardholders will no longer need to sign sales drafts after successful PIN authentication.
- Each transaction is heavily encrypted, as cardholders are required to enter their unique personal identification number (PIN) prior to completing the transaction.
- Reduction in counterfeit card fraud transactions.
- Extra security for cards that are lost or stolen, as chip and pin protection makes it harder for thieves to perform card-present transactions.

Requirements Undertaken by Belize Bank

- Belize Bank Limited's team is diligently working with its processors to perform test transactions and will be seeking certification with the card associations by the end of October 2023.
- Belize Bank Limited will be reprogramming all POS terminals with unique encrypted keys to adhere to the new protocols.

Requirements for Merchants

- Merchants should allow the cardholder to enter his/her unique PIN number on the terminal.
    - A merchant should not enter the PIN number on behalf of the cardholder.
- If the cardholder's PIN is inaccurate, the merchant should request another medium of payment.
- The merchant should report any suspicious PIN activity when processing a transaction.

Implementation Date

- Certification is to be completed by December 2023.
- All Belize Bank terminals will be updated by March 2024.

Reconciliation

Merchant statements are an essential tool for every business to keep track of card transactions processed via the Belize Bank Limited Point-of Sale terminal. These statements provide a detailed summary of all transactions (date of transaction, card number and amount) by brand. It also indicates the gross totals by card present and card not present transactions., the merchant discount rate and the net amount.

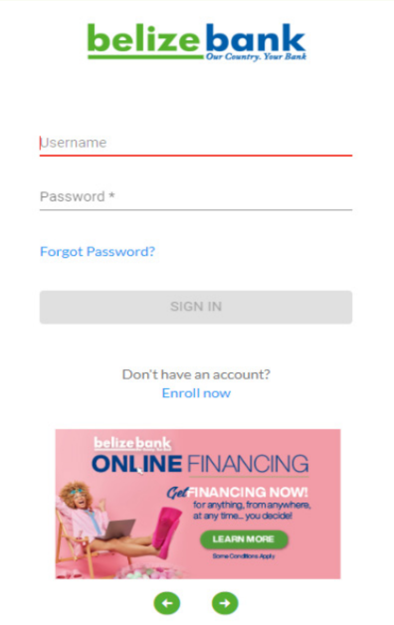
These statements play a crucial role in assisting businesses to reconcile daily which can also identify any payment discrepancies.. It also helps businesses to keep track of their revenue earned via this medium.

How to Access Merchant Statements

Merchant statements are uploaded daily and can be accessed via our Belize Bank Limited website user access. Merchant statements provide a listing of all batches settled by the merchant.

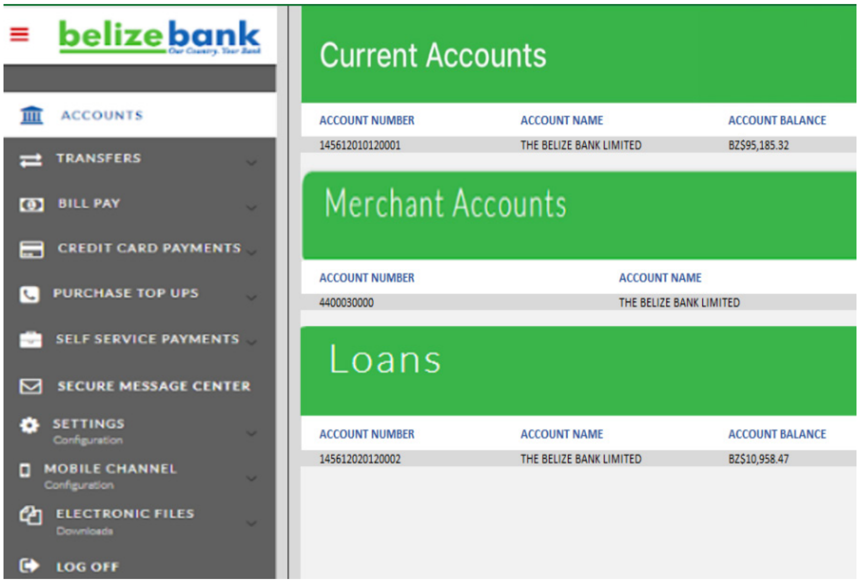
- A business merchant id must be linked to every online user credential that requires access which will enable the specific merchant to view those statements.

Step 1: Login to Belize Bank Online Banking



Step 2: A listing of all accounts linked to your user credential will be displayed.

- Merchant statements are uploaded daily and can be accessed via our Belize Bank Limited website user access. Merchant statements provide a listing of all batches settled by the merchant.



Current Accounts

ACCOUNT NUMBER	ACCOUNT NAME	ACCOUNT BALANCE
145612010120001	THE BELIZE BANK LIMITED	BZ$95,185.32

Merchant Accounts

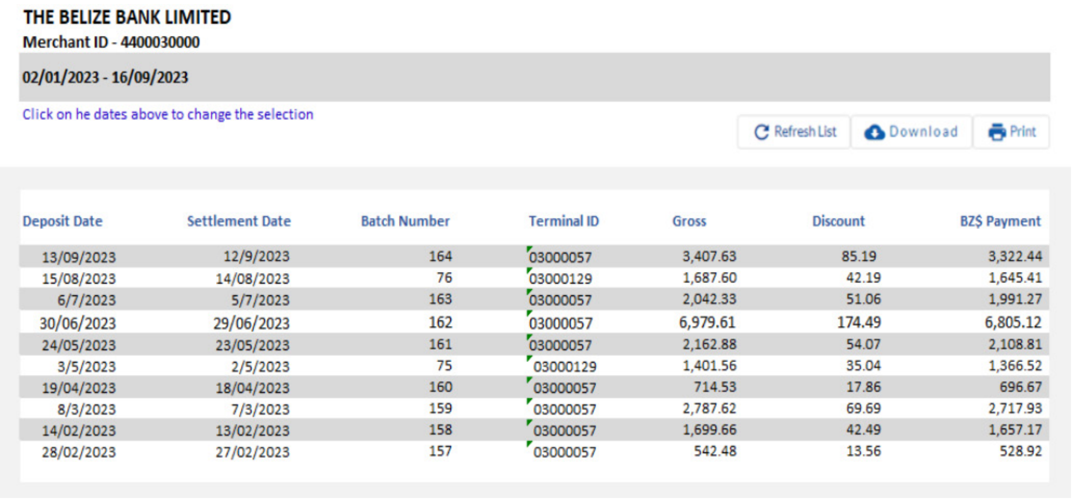
ACCOUNT NUMBER	ACCOUNT NAME
4400030000	THE BELIZE BANK LIMITED

Loans

ACCOUNT NUMBER	ACCOUNT NAME	ACCOUNT BALANCE
145612020120002	THE BELIZE BANK LIMITED	BZ$10,958.47

Step 3: Select the date range that you would like to inquire about. A listing of all settled batches that have been paid to the merchant will be displayed.

- Each batch number corresponds to the batch that was closed.
- Each batch contains a listing of transactions that corresponds to the deposit to your merchant account.
- Choose the deposit you would like to inquire about and click on the Download button.



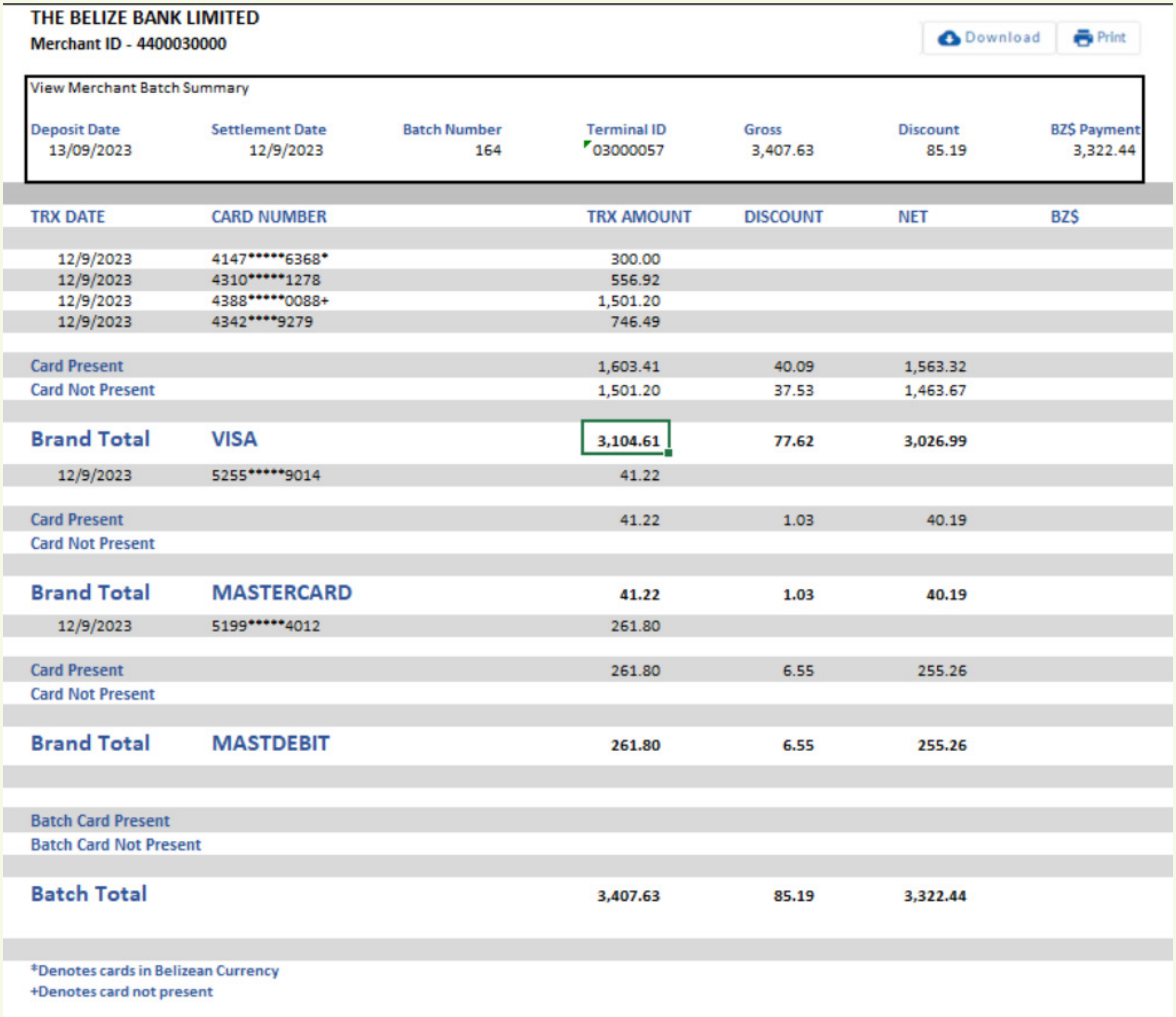
THE BELIZE BANK LIMITED
Merchant ID - 4400030000

02/01/2023 - 16/09/2023

Click on he dates above to change the selection

Deposit Date	Settlement Date	Batch Number	Terminal ID	Gross	Discount	BZ$ Payment
13/09/2023	12/9/2023	164	03000057	3,407.63	85.19	3,322.44
15/08/2023	14/08/2023	76	03000129	1,687.60	42.19	1,645.41
6/7/2023	5/7/2023	163	03000057	2,042.33	51.06	1,991.27
30/06/2023	29/06/2023	162	03000057	6,979.61	174.49	6,805.12
24/05/2023	23/05/2023	161	03000057	2,162.88	54.07	2,108.81
3/5/2023	2/5/2023	75	03000129	1,401.56	35.04	1,366.52
19/04/2023	18/04/2023	160	03000057	714.53	17.86	696.67
8/3/2023	7/3/2023	159	03000057	2,787.62	69.69	2,717.93
14/02/2023	13/02/2023	158	03000057	1,699.66	42.49	1,657.17
28/02/2023	27/02/2023	157	03000057	542.48	13.56	528.92

Step 4: After choosing the batch being reconciled, a detail of all transactions will be displayed by card brand. The transaction indicates what card was present and card not present transactions.



THE BELIZE BANK LIMITED
Merchant ID - 4400030000

View Merchant Batch Summary

Deposit Date	Settlement Date	Batch Number	Terminal ID	Gross	Discount	BZ$ Payment
13/09/2023	12/9/2023	164	03000057	3,407.63	85.19	3,322.44

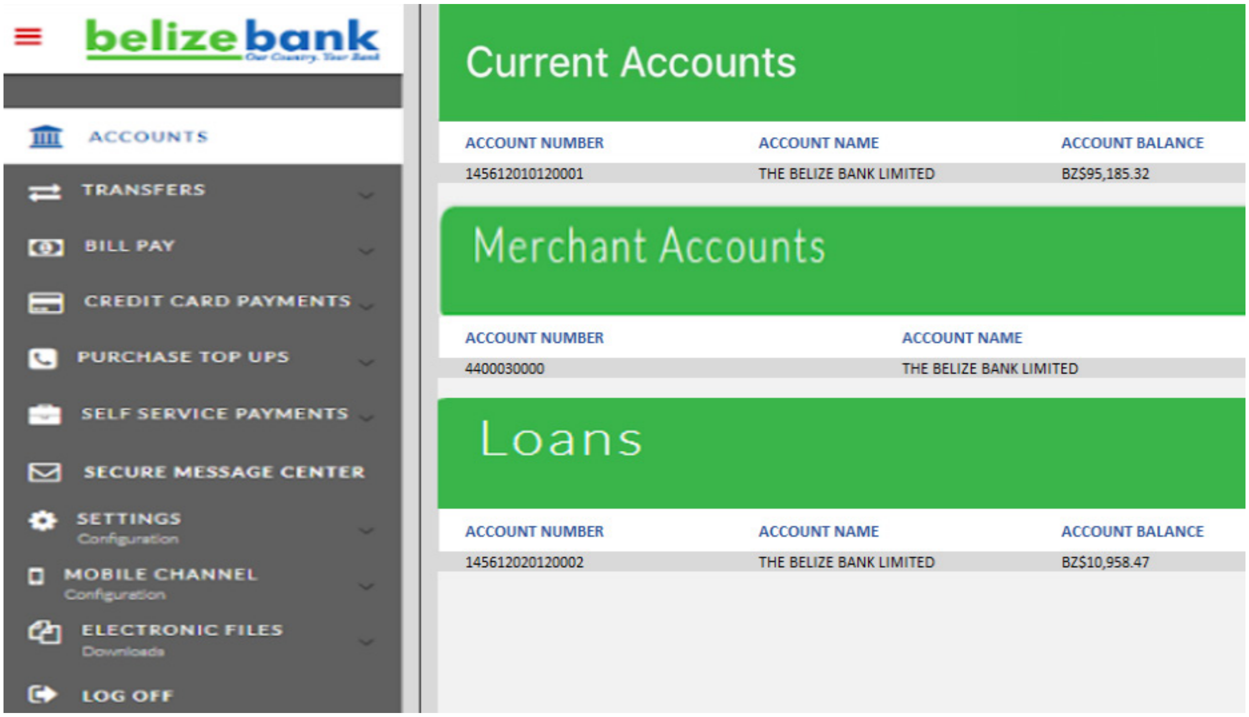
TRX DATE	CARD NUMBER	TRX AMOUNT	DISCOUNT	NET	BZ$
12/9/2023	4147*****6368*	300.00			
12/9/2023	4310*****1278	556.92			
12/9/2023	4388*****0088+	1,501.20			
12/9/2023	4342****9279	746.49			
Card Present		1,603.41	40.09	1,563.32	
Card Not Present		1,501.20	37.53	1,463.67	
Brand Total	**VISA**	**3,104.61**	**77.62**	**3,026.99**	
12/9/2023	5255*****9014	41.22			
Card Present		41.22	1.03	40.19	
Card Not Present					
Brand Total	**MASTERCARD**	**41.22**	**1.03**	**40.19**	
12/9/2023	5199*****4012	261.80			
Card Present		261.80	6.55	255.26	
Card Not Present					
Brand Total	**MASTDEBIT**	**261.80**	**6.55**	**255.26**	
Batch Card Present					
Batch Card Not Present					
Batch Total		**3,407.63**	**85.19**	**3,322.44**	

*Denotes cards in Belizean Currency
+Denotes card not present

Reconciling Merchant Statements Gross and Discount Amounts to Deposit Account

All merchant deposits are credited to the merchant accounts with the same date of the merchant statements.

Step 1: Click on the merchant deposit account where merchant deposits are deposited to for each settled transaction batch.



Current Accounts

ACCOUNT NUMBER	ACCOUNT NAME	ACCOUNT BALANCE
145612010120001	THE BELIZE BANK LIMITED	BZ$95,185.32

Merchant Accounts

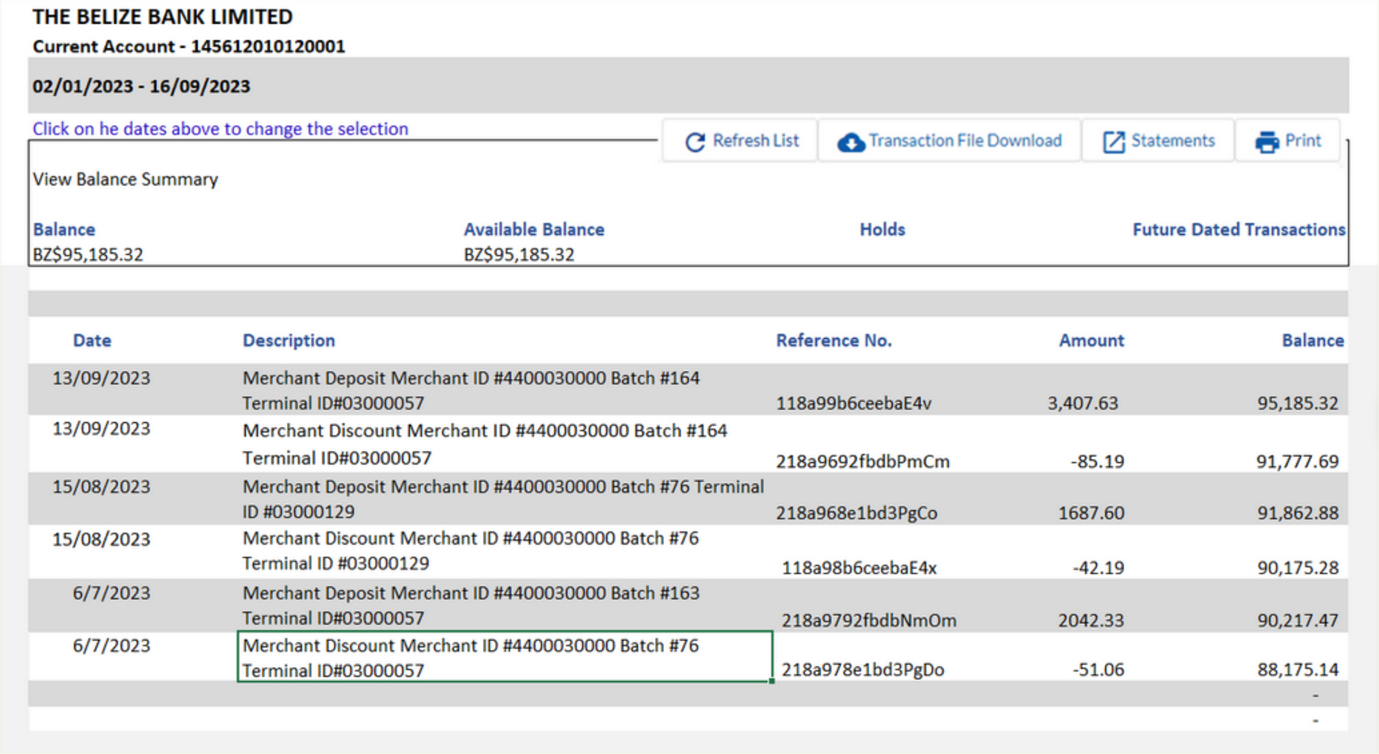
ACCOUNT NUMBER	ACCOUNT NAME
4400030000	THE BELIZE BANK LIMITED

Loans

ACCOUNT NUMBER	ACCOUNT NAME	ACCOUNT BALANCE
145612020120002	THE BELIZE BANK LIMITED	BZ$10,958.47

Step 2: Select the date range that you would like to inquire about. A listing of all deposits and withdrawals that have been processed to the deposit account will be displayed.

- Merchant account is credited for the Gross with description “Merchant Deposit” for Sale transactions.
- Merchant account is debited for the Discount with description “Merchant Discount” for Sale transactions. This is the Gross Deposit multiplied by the Merchant Discount Rate.



THE BELIZE BANK LIMITED
Current Account - 145612010120001

02/01/2023 - 16/09/2023

Click on he dates above to change the selection

View Balance Summary

Balance	Available Balance	Holds	Future Dated Transactions
BZ$95,185.32	BZ$95,185.32		

Date	Description	Reference No.	Amount	Balance
13/09/2023	Merchant Deposit Merchant ID #4400030000 Batch #164 Terminal ID#03000057	118a99b6ceebaE4v	3,407.63	95,185.32
13/09/2023	Merchant Discount Merchant ID #4400030000 Batch #164 Terminal ID#03000057	218a9692fbdbPmCm	-85.19	91,777.69
15/08/2023	Merchant Deposit Merchant ID #4400030000 Batch #76 Terminal ID #03000129	218a968e1bd3PgCo	1687.60	91,862.88
15/08/2023	Merchant Discount Merchant ID #4400030000 Batch #76 Terminal ID #03000129	118a98b6ceebaE4x	-42.19	90,175.28
6/7/2023	Merchant Deposit Merchant ID #4400030000 Batch #163 Terminal ID#03000057	218a9792fbdbNmOm	2042.33	90,217.47
6/7/2023	Merchant Discount Merchant ID #4400030000 Batch #76 Terminal ID#03000057	218a978e1bd3PgDo	-51.06	88,175.14
				-
				-

Benefits & Features

Of Belize Bank Credit Products

SCAN ME!

Credit Card Products

View Now

Glossary

Account Number An issuer-assigned number that identifies an account in order to post a transaction.

Acquirer An Acquirer is a financial institution that enters into agreement with merchants to accept cards as means of payment for goods and services. The acquirer is commonly referred to as the merchant bank.

Address Verification Service(AVS) An optional service through which a merchant can verify a cardholder's billing address before completing a transaction in a card-absent environment.

Altered Card A legitimately issued card which has been lost/stolen and re-embossed, re-encoded and/or otherwise modified to reflect a different name, account number, expiration date and/or signature other than the valid cardholder's account information.

Authorization This is a process by which a transaction for a specified amount is approved by a Card Issuer, an authorizing Processor, or a Stand-In-Processor for a merchant.

Bank Card A card issued by a bank or financial institution.

Call Referral A call referral indicates that the acquiring bank or merchant must contact the card issuer for further instructions. The card issuer uses the call referral as a fraud prevention tool when it suspects or is attempting to prevent fraud at the point of sale.

Card Acceptance Procedures The procedures a merchant or merchant employees must follow during the point-of-sale transaction to ensure that a card and cardholder are valid.

Card Association Visa, MasterCard, and American Express

Card Expiration Date "Good Thru" date.

Cardholder This is the person or entity whose name is embossed on the face of a card or encoded on the magnetic stripe.

Card Absent Environment An environment where a transaction is completed and either the cardholder or the card is not present.

Card Issuer A financial institution that issues cards.

Card Present Environment An environment that comprises of a face-to-face transaction.

Card Security Features An alphanumeric, pictorial, and other design and functional elements on bankcards.

Card Verification Value (CVV) A unique three-digit check value or "check number" encoded on the magnetic stripe of all valid cards to validate card information during the authorization process. CVV is calculated from the data encoded on the magnetic stripe using a secure cryptographic process. The number is verified on-line at the same time a transaction is authorized.

Chargeback A chargeback is a transaction that has been disputed by the cardholder or issuer and must be resolved by the acquirer or the merchant.

Chip An electronic designed to perform process or memory functions.

Chip Card A card embedded with a chip that communicates information to a point-of-sale terminal.

Chip-initiated transaction An EMV chip card transaction that is processed at a chip-reading device using full-chip data.

Chip-reading device a point-of-sale terminal capable of reading, communicating, and processing transaction data from a chip card.

Contactless Payment Terminal A point-of-sale terminal that reads the chip data on a contactless payment chip through an approved wireless interface, and that includes chip reading capabilities.

Copy Request A retrieval request that is processed through an electronic documentation transfer method.

Counterfeit Card
A payment device, which has been fraudulently printed, embossed and/or encoded to be used as a valid card.

Credit A merchant's refund or price adjustment to be credited to a cardholder account.

Disclosure Merchants are required to inform cardholders about their policies for merchandise returns, service cancellations, and refunds. How this information is conveyed or disclosed varies for card present and card absent merchants but in general, disclosure must occur before a cardholder completes the transaction.

Electronic Commerce (E-commerce) E-commerce (electronic commerce or EC) is the buying and selling of goods and services on the Internet.

Expired Card A card on which the expiration date is embossed and/or encoded by the Issuer has expired.

Face-to-Face Transactions These transactions occur when the card holder is present at a retail establishment and uses his credit card to complete a purchase. Face-to-face transactions are the easiest, simplest, most secure transactions for both the merchant and the card holder.

Fallback Transaction An EMV chip card transaction initially attempted at a chip reading device where the device's inability to read the chip prevents the transaction from being completed using the chip card data, and the transaction is instead completed using an alternate mean of data capture and transmission.

Floor Limit
The currency amount established for a merchant location that requires an authorization for any transaction that exceeds the merchant's floor limit. Transactions over this amount require authorization by the merchant from its authorizing Member.

Hologram
Visa
The three-dimensional holographic image of a dove that is part of legitimate Visa cards. The dove should appear to have depth when the card is tilted back and forth. The hologram should have a multi-image appearance not a flat appearance.

MasterCard
MasterCard's hologram is one with interlocking globes showing the continents appears three dimensional and move when the card is tilted. The word "MasterCard" will appear in the background of the hologram. The letters "MC" are micro-engraved around the two rings.

American Express
On American Express cards, the letters "Amex" and a phosphorescence in the Centurion portrait are visible when the card is examined under ultraviolet light.

Issuer A financial institution that issues Visa, MasterCard, American Express and/or Discover cards.

Key-Entry The use of the manual features of a point-of-sale or EDC terminal to enter account information at the point of sale, as opposed to swiping the card through the terminal's magnetic stripe reader.

Magnetic Stripe (Mag Stripe) A strip of magnetic tape on the back of all bankcards. On a valid card, the account information on the magnetic stripe matches similar embossed information on the front of the card.

Magnetic Stripe Reader The component of a point-of-sale device that electronically reads the information on a payment card's magnetic stripe.

Mail Order/Telephone Order (MO/TO) Transaction A transaction between a merchant and a cardholder that is conducted by telephone, mail, or another means of telecommunications in which the cardholder and the card are not physically present at the merchant during the transaction.

Merchant A principal or entity entering into a card acceptance agreement with a member bank (Acquirer).

Payment Card Industry Data Security Standard (PCI DSS) A set of comprehensive requirements that define the standard of due care for protecting sensitive cardholder information.

Personal Identification Number (PIN) A personal identification number code that identifies a cardholder in an authorization request.

Point of Sale (POS) Terminal Point of Sale Terminals are used for the processing of credit cards and/or debit cards in a traditional retail environment. The terminals are used in "face-to-face" transactions. The merchant will swipe the customers' card through the terminal or key-in payment information and the terminal does the rest.

Processor A client that provides authorization, clearing, and/or settlement services for merchants and/or members.

Recurring Transaction A transaction that a cardholder grants written permission for a merchant to periodically charge its account number for recurring goods or services.

Representment A clearing record that an acquirer presents to an issuer through interchange after a dispute/chargeback.

Sales Draft or Draft A paper or electronic record of a sale, rental or service which the merchant presents to the bank for processing. The cardholder's card account can then be debited and the merchant account may be credited.

Signature Panel The signature panel is a tamper-evident panel on the back of the card on which a cardholder signs his or her name.

Skimming A counterfeiting technique in which the account information encoded on the magnetic stripe of a valid card is copied onto the magnetic stripe of a counterfeit card.

Transaction The act between the cardholder and a merchant or cardholder and financial institution which results in the sale of goods or services.

Transaction Receipt An electronic or paper record of a transaction (or a copy), generated at the point of transaction, either manually or by a point-of-sale or EDC terminal.

Unsigned Card A seemingly valid card that has not been duly signed by the legitimate cardholder. Merchants cannot accept an unsigned card until the cardholder has signed it and the signature has been checked against valid government identification, such as a driver's license or passport .

Verified by Visa An approved authentication method based on the 3D secure specification.

Annex B - Contact Information

SCAN ME!

Contact Information

View Now