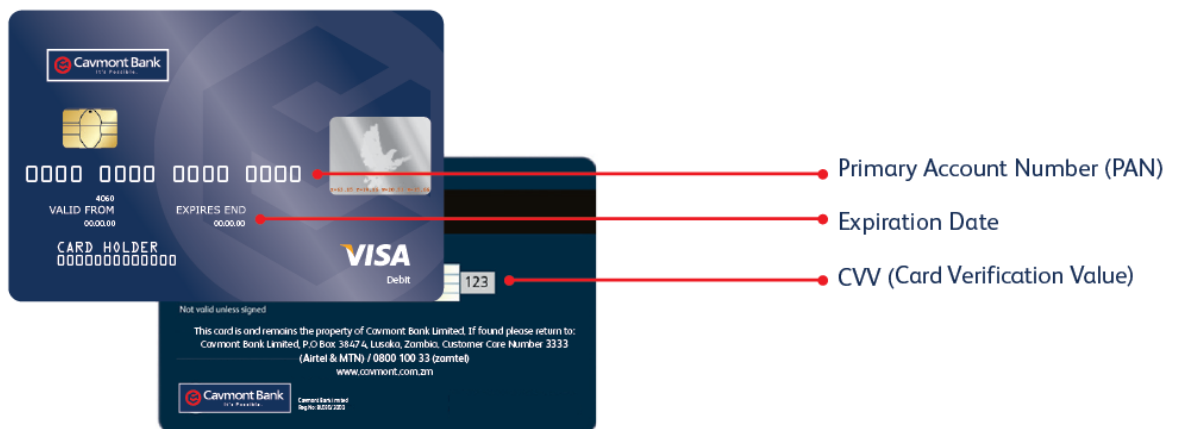


# PCI DSS\* Awareness

(\*Payment Card Industry Data Security Standards)

## Protect Customer Payment Card Data

Consider that when you handle a customer's payment card (debit or credit cards) directly or indirectly, there is always a risk of data being compromised. In your daily work and responsibilities, always keep in mind the following guidelines to promote security awareness for Card Holder Data (CHD).



### DO

1. Restrict physical access to new or existing customer cards, PINs or card data
2. Restrict access to card data information based on business need-to-know
3. Report / Query any unprotected card data
4. Question business processes violating card data confidentiality
5. Write down / enter / store only the first 6 and last 4 numbers of a PAN and only if needed
6. Dispose of expired or faulty cards / documents containing card data by cross-shredding

### DO NOT

1. Store or write down the full PAN of the card
2. Store the card expiration date
3. Store the CVV (Card Verification Value)
4. Store any payment card data longer than is necessary to fulfill a duty, business process or transaction
5. Make a copy of a customer payment card (front and / or back) for any reason
6. Scan, Copy, Fax or Email any information containing the full PAN
7. Ask or expect a customer to complete any form with the full card number
8. Dispose of an expired card or document containing card data in a waste basket or general trash