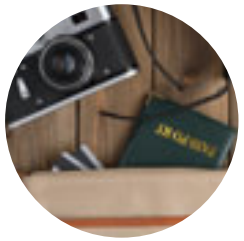

FOR THOSE TRAVELLING

Before You Go Abroad

- Take note of our Emergency Helpline numbers usually written on the back of your card. It is also advisable to store these numbers in your mobile phone contact list so you can contact us if your card is lost or stolen immediately.
- Our **Emergency Helpline** numbers are **+673 244 9666** (for enquiries) and **+673 245 4222** (for lost or stolen cards).
- Only bring along cards that you intend to use. This reduces the risk of losing any of your cards.

During Your Trip Abroad

- **Cover the PIN pad.**
  When you are withdrawing money or making purchases where it requires you to key in your PIN, cover the PIN pad with either your other hand or an object.
- **Never disclose your PIN to anyone.**
  Only you and you alone should know your PIN.
- **Always have your card readily accessible when required**.
  Avoid having to go through your wallet or purse for money or cards, especially at the ATM. Being in this situation makes you more vulnerable to oncoming perpetrators.
- **Don't let your card out of your sight.**
  It is advisable for you to be present at a card terminal when your credit or debit card is used to complete a purchase.
- **Retain your transaction receipts.**
  This will be useful in reconciling your statement.

EMERGENCY HELPLINE

For enquiries (7am to Midnight daily)	**+673 244 9666**
For lost or stolen cards (24-Hour Hotline)	**+673 245 4222**

CAUTIONARY TIPS ON USING YOUR CREDIT OR DEBIT CARDS

FRAUD PREVENTION AND PROTECTION

BAIDURI BANK

TIPS FOR CARDHOLDERS

Card Protection

- In the event that your card is either lost or stolen; retained in an ATM; or suspicious and unusual activities are noticed, contact our **24-Hour Hotline** at **+673 245 4222** immediately.
- Please ensure that your contact details are updated especially when you are travelling abroad. This would allow us to notify you of any suspicious transactions made on your card(s) via SMS notification.
- Always sign on the Signature Panel as soon as you receive your card for validation.
- Do not leave your card unattended in public or even in personal places.
- Ensure that you get your card back after purchases are made.

PIN Protection

- It is advisable NOT to write down your Personal Identification Number (PIN) where it is readily available. Best practice would be to memorize your PIN.
- It is NEVER required to provide your PIN to anyone including members of financial institutions, enforcement agencies or merchants.
- Avoid using your personal information such as date of birth, telephone number or a combination of the two when selecting a PIN.
- Where card purchases require a PIN to be keyed in, cover the PIN pad with either your hand or an object as an added security measure.

Best Practices for Card Usage

- It is good practice to keep copies of your receipts from card purchases and ATM transactions.
- It is advisable not to provide your full credit or debit card details over the phone, unless you are positive that you are dealing with a reputable company or if you have initiated the call at your own accord.
- It is good practice to check your monthly card statements against your receipt purchases especially after travelling abroad. Specifically look for transactions that are not familiar to you.
- Other than proof of identification, do not reveal other personal information such as phone numbers or occupation to validate usage of credit or debit cards.

FOR THOSE WHO SHOP ONLINE

- Only shop at credible internet merchant sites that you know and trust.
- Be wary of unsolicited e-mails from internet merchants. Website links embedded in such e-mails could potentially lead to phishing sites or viruses.
- It is good practice to check an internet merchant's refund policies; some merchants set specific timeframes for returns or charge a fee in accepting returned products.
- Never share passwords with anyone.
- Use different passwords for different websites.
- Ensure that your computer has the latest firewall, spam filter, anti-virus and anti-spyware installed before entering your credit card and personal details into any online shopping portal.
- Activate your browser's pop-up blocker.
- Most merchants implement a "3D secured facility" which requires you to key in a One-Time Passcode (OTP) to complete your online purchase as an added security feature. The OTP will be automatically sent to the mobile phone number you have registered with us.
- It is advisable to print and save the Confirmation Page or e-mails for every successful online purchase.
- It is good practice to review your card statements and bank account statements for any suspicious or unusual activity by logging into your Personal i-Banking account or calling our Emergency Helpline numbers.