**SyndicateBank**
**Card Centre:: Corporate Office:: Bangalore**

# Safety tips for using SyndicateBank Global Credit Cards / Debit Cards

- Sign on the signature panel at the back of your Card immediately on its receipt.
- Treat the Card just like you would keep cash, cheques etc. and always protect it. No one should have access to the Card except you. Please notify us immediately, if it is lost / stolen / copied.
- Do not bend or scratch the Card, particularly the magnetic stripe on the back of the Card.
- Do not place two cards with magnetic strips together.
- Do not expose the Card to electronic devices and gadgets or heat / direct sunlight.
- Keep your PIN (Personal Identification Number) or VbV Password or OTP (one Time Password) secret and do not record it anywhere in writing.
- Do not disclose the PIN or VbV Password or OTP to anyone, not even to the Bank staff.
- Use your body to shield ATM keyboard while entering PIN at ATM to ensure that no one can see you entering your PIN.
- Avoid using an ATM if you sense any abnormal / suspicious behavior by person(s) near the ATM or notice anything strange or suspicious about ATM machine or in its vicinity including sign of tampering or attachment of additional fixtures like skimming device, transparent overlays on ATM keypads, tiny cameras overlooking the keypad etc.
- Don't take help from strangers in carrying out an ATM transaction.
- Enter your PIN or VbV Password or OTP carefully without mistake. Please note that in order to prevent fraudulent use, only three attempts to re-enter the PIN or VbV Password or OTP are provided. Thereafter, the ATM will disallow any transactions and the ATM may capture (swallow) your Card and Block the card for further operation for online transactions.
- There is a time out for response to any request in an ATM. So, please respond to the request displayed on the screen of ATM quickly.
- Quote your 16 digits Debit/ Credit Card number in every correspondence/ payment.
- Ensure that the Merchant swipes the Card only once and in your presence. In case of any doubts, immediately call our help line and confirm the transaction authorization.
- Once Card is swiped and authorized by the system, payments towards such transactions cannot be stopped later.
- In case of any cancellation of a transaction already done through your card at any merchant establishment, insist and obtain a VOID Transaction slip generated by the POS terminal.
- Keep a record of your payment transactions and periodically verify the transaction history / billing statement to ensure its correctness. Any unauthorized Card transaction in the account, if observed, should be immediately reported to the bank.
- Check all transactions, even the small ones, because criminals 'test' stolen card by buying inexpensive items first.
- Never send Card details via e-mail.
- Cardholders may receive "phishing e-mails" which is also known as "carding" / "brand spoofing", asking them to visit certain internet sites, which resemble existing legitimate sites of Cardholders' bank to trick customers in to divulging personal financial information such as bank or card account numbers, ATM PIN or or VbV Password or OTP or other personal identifiers. Such stolen information from successful "phishing" activities is then used to commit fraud.
- Cardholders are requested to be aware of phishing e-mails and should neither respond to them nor access fraudulent websites mentioned in the email.
- Cardholders, who receive such emails and phony request should immediately report the incidents to VISA for action at phishing@visa.com
- If Cardholders suspect that they have disclosed confidential information to a fraudulent website, they should contact 24 Hour Toll Free Help Line to get the Card hot listed.
- Neither VISA nor Bank would initiate contact with cardholders by e-mail or phone seeking their personal or confidential information.
- Promptly notify Card Centre / 24 Hour Help Line of any suspicious transaction or email.

--o0o--